Course Contents

Module No.	Topics	Hrs.
1.0	**Cybercrime and Ethical Hacking**	06
	Introduction to Cybercrime, Types of Cybercrime, Classification of Cybercriminals, Role of computer in Cybercrime, Prevention of Cybercrime. Ethical Hacking, Goals of Ethical Hacking, Phases of Ethical Hacking, Difference between Hackers, Crackers and Phreakers, Rules of Ethical Hacking. **Self Learning Topics :** Exploring various online hacking tools for Reconnaissance and scanning Phase.	
2.0	**Digital Forensics Fundamentals**	06
	Introduction to Digital Forensics, Need and Objectives of Digital Forensics, Types of Digital Forensics, Process of Digital Forensics, Benefits of Digital Forensics, Chain of Custody, Anti Forensics. Digital Evidence and its Types, Rules of Digital Evidences. Incident Response, Methodology of Incident Response, Roles of CSIRT in handling incident. **Self Learning Topics :** Pre Incident preparation and Incident Response process.	
3.0	**Computer Forensics**	08
	Introduction to Computer Forensics, Evidence collection (Disk, Memory, Registry, Logs etc), Evidence Acquisition, Analysis and Examination (Window, Linux, Email, Web, Malware) , Challenges in Computer Forensics, Tools used in Computer Forensics. **Self Learning Topics :** Open source tool for Data collection & analysis in windows or Unix.	
4.0	**Network Forensics**	08
	Introduction, Evidence Collection and Acquisition (Wired and Wireless), Analysis of network evidences (IDS, Router,), Challenges in network forensics, Tools used in network forensics. **Self Learning Topics :** IDS types and role of IDS in attack prevention.	

Module No.	Topics	Hrs.
5.0	**Mobile Forensics**	04
	Introduction, Evidence Collection and Acquisition, Analysis of Evidences, Challenges in mobile forensics, Tools used in mobile forensics **Self Learning Topics :** Tools / Techniques used in mobile forensics.	
6.0	**Report Generation**	04
	Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a forensic report. **Self Learning Topics :** For an incident write a forensic report.	
	Total	28

UNIT - I

Chapter 1 : Cybercrime and Ethical Hacking 1-1 to 1-22

Syllabus :

Introduction to Cybercrime, Types of Cybercrime, Classification of Cybercriminals, Role of computer in Cybercrime, Prevention of Cybercrime.

Ethical Hacking, Goals of Ethical Hacking, Phases of Ethical Hacking, Difference between Hackers, Crackers and Phreakers, Rules of Ethical Hacking.

Self Learning Topics : Exploring various online hacking tools for Reconnaissance and scanning Phase.

1.1 **Introduction to Cybercrime** 1-2

1.1.1 Types of Cybercrime 1-2

1.1.2 Classification of Cybercriminals 1-5

1.2 **Role of Computer in Cybercrime** 1-6

1.3 **Prevention of Cybercrime** 1-7

1.4 **Ethical Hacking** 1-9

1.4.1 Goals of Ethical Hacking 1-10

1.5 **Phases of Ethical Hacking** 1-11

1.6 **Difference between Hackers, Crackers and Phreakers** 1-13

1.7 **Rules of Ethical Hacking** 1-15

1.8 **Self Learning Topics : Exploring Various Online Hacking Tools for Reconnaissance and Scanning Phase** 1-16

1.8.1 Tools used for Reconnaissance 1-16

1.8.2 Tools used for Scanning Network Vulnerabilities 1-20

UNIT II

Chapter 2 : Digital Forensics Fundamentals 2-1 to 2-31

Syllabus :

Introduction to Digital Forensics, Need and Objectives of Digital Forensics, Types of Digital Forensics, Process of Digital Forensics, Benefits of Digital Forensics, Chain of Custody, Anti Forensics.

Digital Evidence and its Types, Rules of Digital Evidences.

Incident Response, Methodology of Incident Response, Roles of CSIRT in handling incident.

Self Learning Topics : Pre Incident preparation and Incident Response process.

2.1 **Introduction to Digital Forensics** 2-2

2.1.1 Need and Objectives of Digital Forensics 2-3

2.2 **Types of Digital Forensics** 2-4

2.3 **Process of Digital Forensics** 2-6

2.4 **Benefits of Digital Forensics** 2-9

2.5 **Chain of Custody** 2-9

2.6 **Anti Forensics** 2-11

2.6.1 Anti-Forensic Techniques 2-11

2.7 **Digital Evidence and its Types** 2-13

2.7.1 Rules of Digital Evidences 2-14

2.8 **Incident Response** 2-15

2.8.1 Computer Security Incident 2-15

2.8.2 Goals of Incident Response 2-15

2.8.3 Methodology of Incident Response 2-16

2.9 **Roles of CSIRT in Handling Incident** 2-17

2.9.1 The CSIRT Core Team 2-18

2.9.2 Technical Support Personnel 2-20

2.9.3 Organizational Support Personnel 2-21

2.10 **Self Learning Topics : Pre-Incident Preparation and Incident Response Process** 2-23

UNIT III

Chapter 3 : Computer Forensics 3-1 to 3-56

Syllabus :

Introduction to Computer Forensics, Evidence collection (Disk, Memory, Registry, Logs etc), Evidence Acquisition, Analysis and Examination (Window, Linux, Email, Web, Malware), Challenges in Computer Forensics, Tools used in Computer Forensics.

Self Learning Topics : Open source tool for Data collection & analysis in windows or Unix.

3.1 **Introduction to Computer Forensics** 3-2

3.1.1 Advantages of Computer Forensics 3-2

3.1.2 Disadvantages of Computer Forensics 3-2

3.2 **Evidence Collection (Disk, Memory, Registry, Logs etc.)** 3-3

3.2.1 Disk 3-3

3.2.2 Memory 3-6

3.2.3 Registry 3-8

3.2.4 Logs 3-12

3.3 **Evidence Acquisition** 3-14

3.4 **Analysis and Examination (Window, Linux, Email, Web, Malware)** 3-18

3.4.1 Investigating Live Systems Windows 3-18

3.4.2 Investigating Live Linux System 3-28

3.4.3 Email Analysis 3-35

3.4.4 Analysis of Web 3-40

3.4.4(A) Cookie Storage and Analysis 3-42
3.4.4(B) Analyzing Cache and Temporary Internet Files 3-42
3.4.5 Analysis of Malware 3-44
3.5 Challenges in Computer Forensics 3-46
3.5.1 Technical Challenges 3-46
3.5.2 Legal Challenges 3-47
3.5.3 Resource Challenges 3-48
3.6 Tools used in Computer Forensics 3-48
3.7 Self Learning Topics : Open-Source Tool for Data Collection & Analysis in Windows or Unix 3-54

UNIT -IV

Chapter 4 : Network Forensics 4-1 to 4-29

Syllabus :

Introduction, Evidence Collection and Acquisition (Wired and Wireless), Analysis of network evidences (IDS, Router), Challenges in network forensics, Tools used in network forensics.

Self Learning Topics : IDS types and role of IDS in attack prevention.

4.1 Network Forensics Introduction 4-2
4.2 Evidence Collection and Acquisition (Wired and Wireless) 4-3
4.2.1 What is Network based Evidence? 4-4
4.2.2 What are the Goals of Network Monitoring? 4-4
4.2.3 Types of Network Monitoring 4-4
4.2.4 Setting up a Network Monitoring System 4-5
4.2.5 Performing a Trap-and-Trace 4-9
4.2.6 Using TCPDUMP for Full Content Monitoring 4-10
4.2.7 Collecting Network-based Log Files 4-10
4.3 Analysis of Network Evidences (IDS, Router) 4-11
4.3.1 Obtaining Volatile Data Prior to Powering Down 4-12
4.3.2 Finding the Proof 4-13
4.3.2(A) Direct Compromise 4-13
4.3.2(B) Handling Routing Table Manipulation Incidents 4-15
4.3.2(C) Handling Theft of Information Incidents 4-15
4.3.2(D) Handling Denial-of-Service (DoS) Attacks 4-15
4.3.3 Using Routers as Response Tools 4-16
4.4 Challenges in Network Forensics 4-19

4.5 **Tools used in Network Forensics** 4-22
4.6 **Self-Learning Topics : IDS Types and Role of IDS in Attack Prevention** 4-26
4.6.1 Intrusion Detection System 4-26
4.6.1(A) Types of IDS 4-27
4.6.1(B) IDS Advantages and Disadvantages 4-28
4.6.2 Role of IDS in Attack Prevention 4-29

UNIT V

Chapter 5 : Mobile Forensics 5-1 to 5-17

Syllabus :

Introduction, Evidence Collection and Acquisition, Analysis of Evidences, Challenges in mobile forensics, Tools used in mobile forensics

Self Learning Topics : Tools / Techniques used in mobile forensics.

5.1 **Introduction** 5-2
5.1.1 Mobile Phone Basics 5-3
5.1.2 Inside Mobile Devices 5-5
5.2 **Evidence Collection and Acquisition** 5-7
5.2.1 Evidence Acquisition 5-10
5.3 **Analysis of Evidences** 5-11
5.4 **Challenges in Mobile Forensics** 5-12
5.5 **Tools used in Mobile Forensics** 5-14
5.6 **Self-Learning Topics : Tools / Techniques used in Mobile Forensics** 5-15

UNIT -VI

Chapter 6 : Report Generation 6-1 to 6-16

Syllabus :

Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a forensic report.

Self Learning Topics : For an incident write a forensic report.

6.1 **Goals of Report** 6-2
6.2 **Layout of an Investigative Report** 6-2
6.3 **Guidelines for Writing a Report** 6-6
6.4 **Sample for Writing a Forensic Report** 6-11
6.5 **Self-Learning Topics : For an Incident Write a Forensic Report** 6-12

□□□

Cybercrime and Ethical Hacking

Syllabus

Introduction to Cybercrime, Types of Cybercrime, Classification of Cybercriminals, Role of computer in Cybercrime, Prevention of Cybercrime.

Ethical Hacking, Goals of Ethical Hacking, Phases of Ethical Hacking, Difference between Hackers, Crackers and Phreakers, Rules of Ethical Hacking.

Self Learning Topics : Exploring various online hacking tools for Reconnaissance and scanning Phase.

Topics

1.1 Introduction to Cybercrime

1.2 Role of Computer in Cybercrime

1.3 Prevention of Cybercrime

1.4 Ethical Hacking

1.5 Phases of Ethical Hacking

1.6 Difference between Hackers, Crackers and Phreakers

1.7 Rules of Ethical Hacking

1.8 Self Learning Topics : Exploring Various Online Hacking Tools for Reconnaissance and Scanning Phase

1.1 Introduction to Cybercrime

- Cybercrime encompasses any criminal act handling computer systems and networks. Cybercrime additionally includes conventional crimes performed via the internet.
- A major attack vector of Cyber Crime is to exploit broken software. The crimes are either cybercrime or cyber related crimes.

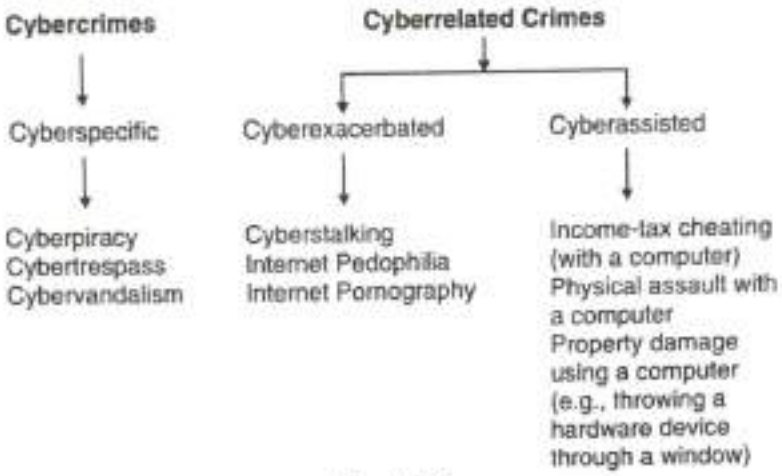


Fig. 1.1.1

1.1.1 Types of Cybercrime

There are following two types of Cybercrimes :

1. Violent or potentially violent cybercrime
2. Nonviolent crimes

1. Violent or Potentially Violent Cybercrime Categories

These crimes pose a physical risk to some character or persons. Kinds of violent or probably violent cybercrime include :

a. Cyber terrorism
b. Assault by threat
c. Cyberstalking
d. Child pornography

a. Cyber terrorism

Cyber terrorism is committed and planned activity in cyberspace via computer networks. It consists of the usage of e-mail for communications among co-conspirators to communicate records for use in violent activities as well as recruiting terrorist institution individuals through internet sites.

It also includes :

1. Air visitors control computer systems which reason the planes to collide or crash.
2. Infiltrating water treatment plant computer structures to reason infection of water supplies.
3. Hacking into medical institution databases and changing or deleting facts that could result in incorrect, risky remedy of a patient or sufferers.
4. Disrupting the electric power grid, this will motive lack of air conditioning in summer and warmth in iciness or result in the dying of folks.

b. Assault by Threat

It is used to give life threat via email to people and their loved one. This may also consist of e-mailed bomb threats sent to businesses or governmental agencies.

c. Cyberstalking

Cyberstalking is when someone uses electronic or digital means to harass or stalk a victim, such as social media, email, Instant Messaging (IM), or messages posted to a discussion group or forum. Cyberstalkers take advantage of the internet's anonymity to stalk or harass their victims without being caught, punished, or even detected.

d. Child pornography

Child pornography includes creating pornographic materials of minor children and distributes these materials as well as accesses this material. It becomes a cybercrime when computers and networks are used for any of these activities.

2. Nonviolent Cybercrime Categories

Nonviolent cybercrimes are divided into following sub-categories :

a. Cybertheft
b. Cybertrespass
c. Cyberfraud
d. Destructive cybercrimes
e. Other cybercrimes

a. Cybertheft

Theft is one of the maximum popular cybercrimes. Cybertheft crimes consist of :

1. **Embezzlement :** Which includes misusing money or belongings on your personal use that has been entrusted to you with the aid of a person else.

2. **Unlawful appropriation :** In this the criminal is not entrusted with the valuables but gains get access to the information from the outside of the organization. The funds can be transferred, documents can be get modified and gives the title to the document which is not owned by him/her.
3. **Company/business espionage :** Wherein men and women inside or outside a business enterprise use the network to scouse borrow exchange secrets, financial records, exclusive purchaser lists, advertising strategies, or different information that may be used to sabotage the commercial enterprise or advantage an aggressive gain.
4. **Plagiarism :** It is the theft of someone else's original writing with the intention of transferring it one's own name.
5. **Piracy :** Piracy means copying of copyrighted software in illegal manner. For example, music, movies, art, books etc. This act will result in loss of revenue to the legitimate owner of the copyright.
6. **Identity theft :** In this the attacker collects the victim's personal information, such as PAN card no, driver's license numbers, to commit the crime or to obtain the property or money which belongs to the victim.
7. **DNS cache poisoning :** It is a form of unauthorized interception. The intruders manipulate the contents of a computer's DNS cache to redirect network transmissions data to their own servers.

b. Cybertrespass

In cybertrespass crimes, the criminal have unauthorized accesses to a computer's or network's resources but does not misuse or damage the data there. The Cybertrespassers read your personal e-mail and documents and noting what programs you have on the system.

c. Cyberfraud

Cyberfraud means selling fake things for the benefit. It can be also named as theft. In the cyberfraud the victim knowingly and voluntarily offers the money to the criminal. Examples of cyberfraud are click and work from home fraud. Cyberfraud can take other forms; any modification of network data to obtain a benefit can constitute fraud.

d. Destructive Cybercrimes

The Destructive cybercrimes damage the network services. Because of this the data is damaged, destroyed and stolen for misuse. These crimes consist of Hacking into a network and deleting data or program files. The destructive cybercrimes are :

1. Web server hacking and "vandalizing" Web pages.
2. Introduce viruses, worms, and other malicious code in the computer network.

3. Planning a DoS attack that brings down the server. It also prevents legitimate users from accessing network resources.

Cybervandalism

Cybervandalism means damaging or destroying data rather than stealing (erasing all the files of business competitor) and transmitting virus through email.

e. **Other Nonviolent Cybercrimes**

Other nonviolent cybercrimes includes :

1. To do the Advertising/soliciting of prostitution services over the Internet
2. To do Internet gambling.
3. Sell the illegal drugs on the internet.
4. To do the Cyber laundering, where electronic transfers of funds is done illegally to obtained money.
5. Cyber contraband or transferring illegal items, like encryption technology that is banned in some jurisdictions, over the Internet.

1.1.2 Classification of Cybercriminals

A cybercriminal is someone who engages in illegal activity through the use of computers or the Internet. These cyber criminals commit cybercrime by utilising their knowledge of computer, network, and human behaviour, as well as a variety of tools. Cybercrime can be classified into the following categories :

1. **Hackers :** Hackers investigate other people's computer systems for a variety of reasons, depending on their needs. There are three types of hackers :
   - **White hat hackers** : A white hat hacker is an ethical hacker who opposes computer system and network abuse. A white hat is typically concerned with the security of IT systems.
   - **Black hat hackers :** A black hat hacker is a malicious hacker who compromises or breaches the security of a computer system or network without the permission of an authorised party.
   - **Grey hat hackers :** A grey hat hacker is someone who hacks both legally and illegally. They are a mixture of white and black hat hackers. They usually do not hack for personal gain or malicious intent, but they may or may not commit crimes on occasion.
2. **Crackers :** These people purposefully cause harm to others in order to satisfy antisocial motives or for fun. This category includes a lot of computer virus creators and distributors.
3. **Pranksters :** Pranksters are people who play practical jokes on others. They usually have no intention of causing any immediate or long-term harm.
4. **Career criminals :** Criminals who make a living from crime. These people make a living from crime. They may collaborate with others or work for organised gangs such as the Mafia. Russia, Italy, and Asia pose the greatest threat from organised crime.

5. **Cyber terrorists :** Cyber terrorists come in a variety of shapes and sizes. A hacker may gain access to a government website in order to steal information or make a threat. Up until May 2019, it was discovered that approximately 25 Indian government websites had been hacked.
6. **Cyber bulls :** Name calling in chat rooms, creating fake profiles on websites, and sending mean or cruel emails or messages are all examples of cyberbullying, which cyber bulls engage in.
7. **Salami attackers :** Attackers who use salami : These attacks are used to commit financial crimes. The key is to make the change so minor that it would go completely unnoticed in a single case, such as when a bank employee inserts a programme into the bank's servers that deducts a small amount from each customer's account.
8. **Drops :** These people exchange 'virtual money,' or cryptocurrency, for real money.
9. **Kids :** Because of their young age, they are referred to as "kids" (most are under 18). They purchase and resell the basic components of successful cyber-scams, such as spam lists, proxies, credit card numbers, hacked hosts, and scam pages.
10. **Coders :** They create ready-to-use tools for cyber criminals, such as trojans, mailers, custom bots, viruses, and other services, and sell them to them.

1.2 Role of Computer in Cybercrime

Computer Crime

Computer crime is any criminal offense, activity or issue that involves computers. Computer is used in illegal activities : child pornography, threatening letters, e-mail spam or harassment, extortion, fraud and theft of intellectual property, embezzlement.

Categorizing computer-related crime

A single category cannot accommodate the wide divergence of conduct, perpetrators, victims, and motives found in examining computer crimes. Adding to this confusion is the fact that computer crimes also can vary depending upon the jurisdiction criminalizing the conduct. Computers serve in several different roles related to criminal activity. The three generally accepted categories speak in terms of computers as communication tools, as targets, and as storage devices.

1. The computer as a communication tool presents the computer as the object used to commit the crime. This category includes traditional offenses such as fraud committed through the use of a computer. For example, the purchase of counterfeit artwork at an auction held on the Internet uses the computer as the tool for committing the crime. While the activity could easily occur offline at an auction house, the fact that a computer is used for the purchase of this artwork may cause a delay in the detection of it being a fraud. The use of the Internet may also make it difficult to find the perpetrator of the crime.

2. A computer can also be the target of criminal activity, as seen when hackers obtain unauthorized access to Department of Defense sites. Theft of information stored on a computer also falls within this category. The unauthorized procuring of trade secrets for economic gain from a computer system places the computer in the role of being a target of the criminal activity.
3. A computer can also be tangential to crime when, for example, it is used as a storage place for criminal records. For example, a business engaged in illegal activity may be using a computer to store its records. The seizure of computer hard drives by law enforcement demonstrates the importance of this function to the evidence gathering process.
4. In some instances, computers serve in a dual capacity, as both the tool and target of criminal conduct. For example, a computer is the object or tool of the criminal conduct when an individual uses it to insert a computer virus into the Internet. In this same scenario, computers also serve in the role of targets in that the computer virus may be intended to cripple the computers of businesses throughout the world.

1.3 Prevention of Cybercrime

The Fig. 1.3.1 is showing the five mantras for the prevention.

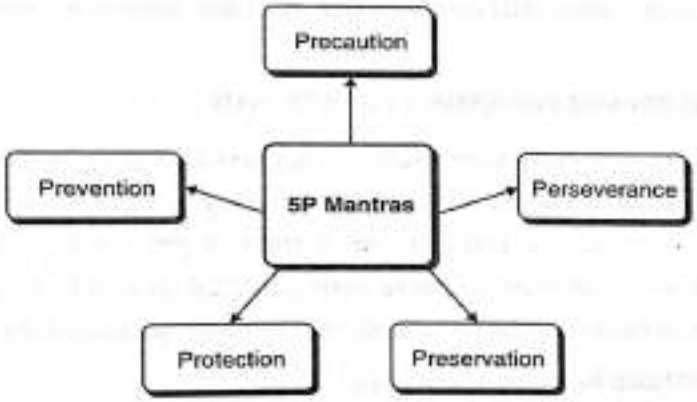


Fig. 1.3.1 : Prevention Methods

The following steps should be taken for preventing the cybercrime :

1. **Use a full-service internet security suite**

Use full-service internet security suite against existing and emerging malware including ransom ware and viruses, and helps protect your private and financial information for online transaction.

2. **Use strong passwords**

Do not use simple passwords. Use complex passwords that are combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

3. **Keep your software updated**

Cybercriminals often uses well-known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you will become a cybercrime target.

4. **Manage your social media settings**

Keep your personal and private information locked down. Cyber criminals often get your personal information through social engineering. So, the less you share personal information publicly, the better.

5. **Make stronger your home network**

Use strong encryption password as well as a virtual private network. A VPN encrypts all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data.

6. **Keep up to date on major security breaches**

If you do business with a merchant or have an account on a website, then that has been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

7. **Take measures to help protect you against identity theft**

A person's Identity can be obtained wrongfully using personal data in a way that involves fraud or deception, usually for economic gain. It can be done by tricking a person into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. Due to this it is important to guard your personal data. A VPN help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

8. **Know that identity theft can happen anywhere**

It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.

9. **Know what to do if you become a victim**

If you believe that you have become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future. If you think cybercriminals have stolen your identity

These are among the steps you should consider.

- Contact the companies and banks where you know fraud occurred.
- Place fraud alerts and get your credit reports.
- Report identity theft to the FTC.

10. Train the organization staff

Organizations must have to educate their employees about the attacks and the identification of the exposure.

11. Turn on your spam blocker

Most Internet providers provide a spam blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to your inbox.

1.4 Ethical Hacking

- **Ethical Hacking** is deployed as a tool across the globe to deal with cyber criminals and protect sensitive data. Ethical Hackers help develop the security system of a framework in a business or organization to prevent potential threats. They are referred to as White Hats, who end up provide protection from the Black Hats who are the unethical hackers. Ethical hacking is adopted by many almost every organization.
- Ethical hacking involves using the same hacking tools and techniques to identify the vulnerabilities in a system and address them before they can be exploited. Organizations are now hiring ethical hackers to prevent malicious practices and reduce incidents happening related to technology.
- Ethical hackers must examine and analyze each and every potential error and flaws present into the system and prepare a document which covers different aspects such as errors encountered, the vulnerability of the system due to errors, measures to be undertaken for protection and impact level of the error. After this it is the organizations responsibility to prioritize, analyze and strengthen security policies, network infrastructure, and end-user practices to safeguard the organization from cyber threats.

Hacking Types

Depending on what is hacked, we can divide hacking into different categories. These are the following :

1. Website Hacking
2. Computer Hacking
3. Network Hacking
4. Email Hacking
5. Password Hacking

1. **Website hacking :** Website hacking entails gaining unauthorised access to a web server or database and altering the information.
2. **Computer hacking :** Computer hacking refers to unauthorised access to a computer and the theft of information from the computer, such as the computer ID and password, through the use of hacking methods.
3. **Network hacking :** It is the gathering of information about a network with the intent of harming the network system and interfering with its operations using various tools such as Telnet, NS lookup, Ping, Tracert, and so on.
4. **Email hacking :** Unauthorized access to and use of an email account without the owner's permission is referred to as email hacking.
5. **Password hacking :** It is the process of recovering secret passwords from data that has already been stored in a computer system.

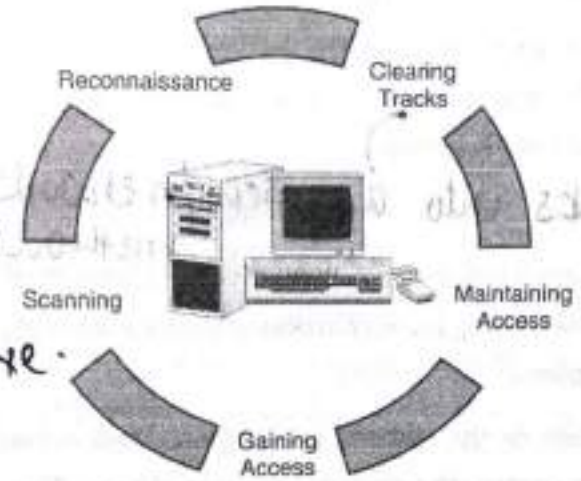
1.4.1 Goals of Ethical Hacking

The following are the goals of ethical hacking :

1. Uncover as much vulnerability as possible. They should also be able to count them and report back to the owner of the hacked system. It is also their responsibility to demonstrate each vulnerability they find. This could include a demonstration or any other type of evidence they have.
2. Ethical hackers frequently report to the system's owner, or at the very least to the part of a company's management in charge of system security. They collaborate with the company to ensure that the integrity of their computer systems and data is maintained. Their ultimate goal is to implement the results of their efforts and improve the system's security.
3. The goal of an ethical hacker is to test the security of an organization's information systems in order to improve security. Given the importance of ethical hacking, especially in light of the damage that successful malicious hacking can cause, there is growing interest in using ethical hackers to combat today's cyber threats.
4. By preventing cyber-terrorism and terrorist attacks, ethical hacking can ensure the nation's safety.
5. Learn new skills and apply it to a variety of jobs, including software development, risk management, quality assurance testing, and network defence.
6. The main strength of a company is trained ethical hackers. Ethical hackers should perform quick security tests under extreme and standard conditions to ensure that software functions properly.
7. Develop many tools and methods and quality assurance tester to eliminate all the system's vulnerabilities.
8. Before any attacks, ethical hackers should think like an attacker and find potential entry points and fix them.

1.5 Phases of Ethical Hacking / steps.

Phases involved in ethical hacking are as explained, generally these phases are used by a hacker to break into a network while ethical hackers use this to protect the system.



Direct interact - nmap tool. Active
collecting info. Passive.

Fig. 1.5.1 : Phases of ethical hacking

1. **Reconnaissance :** (foot printing & info gathering).
   - Reconnaissance (investigation or inspection) is the preliminary phase in which the hacker gathers information about the target before planning to launch an attack and is completed in phases before exploring system vulnerabilities.
   - One of the phases is dumpster diving. During this phase the hackers find important information such as old passwords, names of important employees (such as head of network department) and performs an active investigation on how the information flows through the organization and how the organization performs the functions.) usually collects info about n/w, host & people involved.
   - Subsequently, the hacker completes the process called foot printing in which the hacker collects data on security policies and focuses on the specific IP addresses and protocols used by the network, identifies the vulnerabilities in the target system and draws a network map to know how the network infrastructure works to break into it easily.
   - Foot printing also provides information about the domain names, system names, active TCP and UDP services and passwords. The hacker can also use a search engine to extract information about the organization and use the information of current employees for impersonation.
2. **Scanning :** Tools – dialers, n/w mappers, etc).
   - Scanning involves taking the information gathered during reconnaissance phase and examining the network. There are three methods for scanning pre-attack, port sniffing/scanning and information extraction. open port, live system.

- Each phase gives a specific set of vulnerabilities that the attacker can then use to understand the weaknesses and violate security policies.
- In the pre-attack method, the attacker scans the network based on the data discovered during the reconnaissance phase. In the port scanning method, scanning is performed to search for vulnerability scanners, dialers, port scanners and other data-gathering equipments.
- In the information extraction method the hacker collects information about the ports made available during establishing the connection, live machines present to service the requests for the clients and the operating system used.

3. **Gaining Access :** Breaks into a system/network using tools/or methods

- After the scanning is completed, the hacker designs the blueprint of the network of the target with the help of data collected during the reconnaissance and scanning phase. This is the phase where the real hacking takes place.
- The hacker gains access to the system, applications, and network, and escalates their user privileges available to control the systems connected to it. The method of connection that a hacker uses can be LAN (wired or wireless), local access to a computer, the internet, or offline mode of access.
- Some examples include Denial of Services (DoS) and session hijacking. Gaining control over a system in hacker world is known as owning the system.

4. **Maintaining Access :**

- Once a hacker has gained access they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits and Trojans.
- Once the hacker has taken a control over a base system it can use it for launching further attacks and information intercepting. In this case, the owned system is sometimes referred to as zombie systems.

5. **Covering tracks :** Clearing tracks.

- The hackers which have gained and maintained access, they cover their tracks or activities to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action.
- Hackers try to remove all traces of the attack, such as log files or Intrusion Detection System (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunneling protocols, and altering log files.

1.6 Difference between Hackers, Crackers and Phreakers

- Cybercrime is an activity performed by the criminals who employ their diverse technological skills and internet to achieve their nefarious ends. Recognizing a cybercrime depends upon the activity being committed.
- Some of the examples are, downloading a software or file from an unknown source which may slow down the performance of the computer, phishing attacks wherein the attacker repeatedly sends spam emails to the receiver and prompts the receiver to send confidential information, some criminals may also use a compromised computer using it as a victim to attack on other systems and using key loggers in the background for stealing passwords and other information without the users being informed.
- Resolving cyber crimes is the task of police, national cyber security departments and commercial cyber security firms. On a personal level one can prevent cyber crimes by installing proper antivirus software for scanning the system, removing dangerous files from the system, safe browsing and maintaining backup of our daily work.

1. **Hacker :**
   - A hacker is an individual who is having good understanding of computers, networking, programming and hardware but with no malicious intentions.
   - A malicious hacker on the other hand is an individual who breaks into a system or network illegally and tries to steal or damage the information.
   - A Hacker is a person who seeks knowledge by understanding how the systems operate, how is the system being designed and how to deal with different components present into the software.
   - Honest hackers with no such malicious intentions are referred to as "White Hats" whereas those with malicious intentions are referred to as "Black hats".
   - Recognizing about an malicious activity is important and some of the examples of such activity are, money which is being transferred from the senders account to the receivers account without the permission of the sender, providing confidential information to unknown websites or organizations, browsing the links which do not implement Secure Socket Layer (SSL).
   - Hacking can be prevented by using proper antivirus software which will scan our system or network for vulnerabilities or for any malicious software and remove it. A malicious hacker can also be termed as an intruder or an interceptor if the attacker is monitoring the information being exchanged or analyzing the traffic present on a network to know the IP address, the protocol being used by the network and payload contents of a packet.
   - Some organizations install an Intrusion Detection System (IDS), for example SNORT, on the server machine or on a network host which is present at the network segment to examine each and every packet being transmitted over the network and if a packet contains some malicious code or data then the IDS will generate an alert and will not forward the packet on the network.

2. Crackers :

- While hacking is the process of bypassing computer security in order to gain access into the system, cracking specifically refers to the same practice, but with criminal intents. Cracking relies more on persistent repetition of a handful of fairly known tricks in order to break into systems, rather than cleverly exploiting the system's weaknesses.
- Cracking can be recognized by, for example, software companies don't come to know that whether their software has been cracked, public Wi-Fi networks being cracked and examined by individuals to hamper their private information, somebody sending phishing emails to other people from your email address.

Difference between Hacker and Cracker :

Parameter	Hackers	Crackers
Meaning	They are constantly looking for the flaws in the computer and internet security and their sole aim is to rectify these flaws and improve the security of the content.	The purpose of a cracker is to break the security of computers and networks to damage the private data.
Known for	There is a common view that hackers build things.	The crackers are believed to break the things.
Skill Level	Hackers have an advanced knowledge of the computer related security.	Crackers are usually not as skillful as hackers. Very few of them are skilled enough to create their own software and tools.
Internet Security	Hackers potentially restore the security set ups across the corrupted networks and they help in catching the specific crackers.	Crackers always know that their activities are illegal and they are breaking the law so they tend to cover up their tracks.
Knowledge of computer programs	Hackers have an upper hand when it comes to programming languages such as C, C++, HTML, Java, etc.	Crackers on the other hand are incompetent when it comes to computer programs.
Purpose	A professional hacker breaks into the secure networks to look out for any discrepancies.	The crackers break into the secure networks for malicious purposes.

3. **Phreakers :**

- Phreakers are the people who break into the public and private telephone systems illegally. Phone phreaking occurs when our phone is exploited without our knowledge so that criminals can gain access to international calls or voicemails.
- Once phreakers gain access to a number of phone systems they then start gathering them together to create their own networks and use them all over the world. The typical phreak was or is usually equipped with a specially-made "box" designed to "fool" the network in some way. Different boxes are used for different phreak approaches.
- A "black box" allows us to make free calls from a home phone, a "red box" to make free calls on a pay phone, and the infamous "blue box" provides complete control over the telephone system. Each call is then routed via the phreaked phone lines which makes them hard to trace the result is a financial crippling bill which the customer has to pay.
- A customer can stop the phreaking attack by regularly analyzing the telephone bills and the call history to know that if there were any outgoing calls made which are unknown to the customer.

1.7 Rules of Ethical Hacking

The Ethical hackers have to follow some guideline or code of conduct that is given as follows :

Hacker Ethics

1. Early hackers developed a code of ethics, which has been adopted in large part by computer professionals today.
2. Code of ethics has evolved based on technological and societal changes.
3. Some hackers reject this code for a variety of reasons.

ACM Code of Ethics and Professional Conduct

1. Contribute to society and human well-being.
2. Avoid harm to others.
3. Be honest and trustworthy.
4. Be fair and take action not to discriminate.
5. Honour property rights including copyrights and patents.
6. Give proper credit for intellectual property.
7. Respect the privacy of others.
8. Honor confidentiality Know and respect existing laws pertaining to professional work.
9. Improve public understanding of computing and its consequences.
10. Access computing and communication resources only when authorized to do so.

11. All these rules highlight a need to obey the law, avoid harm, and respect others' privacy and property, but also to further knowledge and understanding.

Ten Commandments of Computer Ethics (CEI)

1. Do not use a computer to abuse and harm other people.
2. Do not interfere with other people's computer work.
3. Do not peep in around other people's computer files.
4. Do not use a computer for theft
5. Do not use a computer to convey false witness.
6. Do not use a duplicate copy of proprietary software for which you have not paid.
7. Do not use other people's computer resources without permission.
8. Do not appropriate other people's intellectual output.
9. Always think about the social importance of the program you are writing or the system you are designing.
10. Always use a computer in ways that assure consideration and respect for your companion humans.

1.8 Self Learning Topics : Exploring Various Online Hacking Tools for Reconnaissance and Scanning Phase

1.8.1 Tools used for Reconnaissance

When an IT security investigation is to be initiated, the primary phase is data reconnaissance and gathering information about the target. After acquiring the needed information, we will have all the information about the domain names, IP addresses, servers, protocols used and technology details used by the target. Some of the tools used by the Information Security (InfoSec) professionals are mentioned as follows :

1. **CheckUserNames** : When an attacker tries to gain access into a system, he needs to provide a username and a password for proper authentication as per the accounts which are created on that system (admin, student), some systems also allow a guest login but limits the privileges available to the user.

   CheckUserNames is a tool which helps the research professionals to find the username on different social networking sites such as linkedIn, Instagram, Facebook etc.

2. **HaveIbeenPwned** : During the registration phase on a third party website, we need to provide our confidential information for example email-id, phone number, alternate email-id, so that during password recovery or account recovery phase they will be sending messages or keys for verification purpose.

HavelbeenPwned is a tool developed by Troy Hunt, which helps us to examine that whether our email account has been compromised by sharing our personal information with other entities by the third party websites without the users permission. The tool can track the compromise from many sources like gmail account, hotmail account or yahoo account.

3. **BeenVerified** : BeenVerified is a tool which helps us to search for people on public internet records. This tool is very useful when an IT security investigation is to be conducted about an unknown target. When the results are available, the tool will create a result page with the list of all the names which match with the names provided, along with their geographic location, phone numbers, which can then be used to prepare reports. BeenVerified also includes information about the criminal records and government organizations. The background information used by BeenVerified is collected from multiple databases, cyber attacks on banks, career history, social media profiles and even online photos.

4. **Censys** : In order to identify a device uniquely on the internet, an address is assigned to the device by the router or the DHCP (Dynamic Host Configuration Protocol) server present on that network. This address is known as IP (Internet Protocol) address (logical address), along with IP address there is a Hardware address (MAC- Medium Access Control address) which is imprinted on the network interfacing card to indentify a device physically on a network. IP addresses help the routers to take the decision as to which line or link the packet needs to be forwarded so as to minimize the delay. Once the packet enters the network the host present on that network is identified and then the packet is forwarded to that host.

   Censys tool provides the latest information about the device connected to the internet, which can be servers or domain names. This tool helps us to find all the geographic and technical details about the 80 and 443 ports running on the servers, as well as HTTP/S body content and GET response of the target website, chrome TLS (Transport Layer Security), full SSL (Secure Sockets Layer) Certificate Chain information which works between the Transport Layer and the Presentation layer of the OSI model, and WHOIS information, which provides information about the IP addresses, registrar of the domain and the domain names used.

5. **BuiltWith** : When we want to gather information about a particular website, that is whether it an government or an enterprise website, different technologies used by the website for example CMS (Content Management Systems) like Wordpress, entity which is responsible for hosting of the website to make it accessible anytime, web server type used, full depth javascript and CSS libraries implemented and the SSL provider, BuiltWith has the functionality to provide all the details mentioned above.

6. **Google Dorks** : Google Dorks are simply ways to query Google against certain information that may be useful for our security investigation. Search engines are capable of indexing a lot of information about almost anything on the internet, including individual, companies and their data. Some popular operators used to perform Google Dorking :

   - **Filetype** : This dork can be used to find any kind of filetypes.

- **Ext :** Can help us to find files with specific extensions (eg. .txt, .log, etc).
- **Intext :** Can perform queries which can search for specific text inside any page.
- **Intitle :** It will search for any specific words inside the page title.
- **Inurl :** Will look out for mentioned words inside the URL of any website.

7. **Maltego :** Maltego is a tool developed by Paterva organization and is a part of the Kali Linux distribution. In order to use this tool, we need to create a free account on the website of Paterva, so that we can download the tool can understand the features. Maltego allows us to design tests for a specific target.

   One of the main feature which Maltego includes is the 'transforms'. The 'transforms' helps us to run different kind of test cases on a machine and to integrate data with external applications. Once we choose our transforms, Maltego will start running all the transforms on Maltego servers. When the result is available with the tool, it shows the specified targets, IPs, domains, AS numbers. An important reason for the wide use of this tool is that it provides the user to design its own test cases to be executed on a different machine and analyze the performance.

8. **Nmap :** Nmap stands for "Netowrk Mapper". Nmap is a security auditing tool which can be used to explore the information about the hosts present in a network or remote hosts. It is an open source utility. Some of the main features include :

   - **Host detection :** Nmap has the ability to identify hosts inside any network that have certain ports open, or that can send a response to ICMP(for example, PING uses ICMP Protocol to test the connectivity between two nodes on a same or different network) and TCP packets.
   - **IP and DNS information detection :** This includes device type, Mac addresses and even reverse DNS names.
   - **Port detection :** Nmap can detect any port open on the target network, and let us know the possible services currently running on it.
   - **OS detection :** Provides full OS version information and detection of the hardware specifications of any host connected.
   - **Version detection :** Nmap is also able to get application name and version number.

9. **Recon-ng :** Recon-ng is an already built in tool in the Kali Linux distribution which can be used to perform a quick inspection on remote targets. Recon-ng is a web reconnaissance framework written in Python and includes many modules, convenience functions, and an interactive menu based interface to help us perform different commands. This simple command-based interface allows you to run common operations like interacting with the database, run web requests, manage API keys or standardizing output content. Fetching information about the target becomes easy and it can be done after installation. Some modules of the recon-ng tool are passive as they never hit the target, while others can launch interesting stuff right against the remote host.

10. **theHarvester** : theHarvester is another important tool used to collect information about subdomain names, virtual hosts, open ports on the server which are ready to accept connection request from the client, email address of company or websites. This information is very useful when we are in the initial phase of a penetration test which is performed to analyze the local network, or third party authorized networks. This tool is also included in the Kali Linux distribution. The tool uses many resources to fetch data like PGP (Pretty Good Privacy) which is used for non repudiation of data and to encrypt the files stored on the mail server thereby preventing them from unauthorized access, from search engines like Bing, Google, Yahoo, and also from social networks like LinkedIn, Twitter and GooglePlus.

11. **Shodan** : Shodan is a tool developed by John Matherly to keep track of publicly accessible computers inside any network. Shodan is a network security monitor and a search engine which closely resembles Google, but instead of showing informative websites and images, it shows results that are related to the IT security researchers like SSH (Secure Shell), Telnet, FTP, SNMP, HTTP server banners and public information. Results will be shown ordered by country, operating system, network and ports. Shodan can not only be used to reach servers, routers and webcams but also to scan almost anything that is connected to the internet. It is often called as "search engine for hackers".

12. **OpenVAS** : OpenVAS stands for Open Vulnerability Assessment System, a security framework which includes particular services and tools for infosec professionals. OpenVAS is an open source vulnerability scanner and security manager which can be used to analyze the security of remote hosts. OpenVAS scanner is a highly efficient program that executes all the network related tests over the target machine, and, the other component is OpenVAS manager which basically provides vulnerability management solution that allows us to store the scanned data into an SQLite database, which can later on be used to search, filter and order the scanned results in an appropriate and suitable way.

13. **Fierce** : Fierce is an IP and DNS reconnaissance tool written in PERL for helping IT security professionals to find target IPs associated with domain names. Once we have defined our target network, Fierce will launch several scans against the selected domains and then it will try to find misconfigured or unauthorized networks and vulnerable points that can be exploited by the attacker which can later leak private and valuable data. The results will be made available on the screen, but it takes a little more time as compared to Nessus, Nikto and Unicornscan scanning tools.

14. **FOCA** : FOCA (Fingerprinting Organizations with Collected Archives) is a tool written by ElevenPaths which can be used to scan, analyze, extract and classify information from remote web servers and their hidden information. Foca has the ability to analyze and collect valuable data from MS Office suite, OpenOffice, PDF, as well as Adobe InDesign, SVG and GIF files. This security tool also works actively with Google, Bing search engines to collect additional data from the above mentioned files. Once the full file list is ready, it starts extracting information to identify valuable (important) data from the files.

1.8.2 Tools used for Scanning Network Vulnerabilities

A vulnerability scanner is a computer program designed to access computers, computer systems, networks or application for determining the weaknesses present on the system which can give the attacker an opportunity to gain unauthorized access thereby violating security policies and stealing confidential data. In order to prevent such activities from occurring, identification of vulnerabilities are important. Following are the tools which can be used to scan the network for analyzing the potential errors :

1. **Nessus** : Nessus is an open source vulnerability scanner developed by Tenable Network Security. Initially when the Nessus tool was deployed, it consisted of two main components, nessusd, which is the Nessus daemon, which performs the scanning, and the nessus client, which controls scans and presents the vulnerability results available to the user. Later versions of Nessus (4 and greater) employs a web server which provides the same functionality as the client.

   Apart from the functionality of testing network vulnerabilities, it can also be used to examine patch levels on computers running Windows Operating System by using Windows credentials and perform password auditing using dictionary and brute force methods. Nessus 3 and later versions can also audit systems to ensure that they have been configured as per the policy such as the NSA's guide used for hardening of Windows servers. This functionality utilizes Tenable's proprietary audit files or Security Content Automation Protocol (SCAP) content. Nessus provides the support for scanning following types of vulnerabilities :

   - Vulnerabilities that permit a remote attacker to control or access sensitive data stored on a system.
   - Misconfiguration (e.g. open mail relay).
   - Search for default passwords, common passwords, blank/absent passwords which are set up on some systems.
   - Denials of Service against the TCP/IP stack by using malformed packets.

2. **WebShag** : WebShag is a server auditing tool written in Python to scan HTTP and HTTPS (Secure Hyper Text Transfer Protocol) protocols. It is a part of Kali Linux which can be used for penetration testing. The features provided by WebShag include port scan, URL scanning, file fuzzing, and website crawling. In order to avoid the hurdles enforced by remote server security systems, it uses an intelligent IDS (Intrusion Detection System) evasion system by launching random requests per HTTP proxy server, so that we can keep auditing the server without being banned.

3. **Unicornscan** : Unicornscan is one of the top information gathering tools for security research. It has also a built-in correlation engine that aims to be efficient, flexible and scalable at the same time. Main features of the tool includes :

   - Full TCP/IP device/network scan.
   - Asynchronous stateless TCP scanning (including all TCP Flags variations).

- Asynchronous TCP banner detection.
- UDP Protocol scanning.
- A/P OS identification.
- Application and component detection.
- Support for SQL Relational Output.

4. **Nikto** : Nikto is an open source web server scanner which performs comprehensive test against web servers for multiple items such as potentially dangerous files/programs, checking outdated versions and version specific problems of the software and applications installed. Nikto also checks for server configuration items such as the presence of index files, HTTP server options, and will attempt to identify installed web servers and software.

   The tool will test a web server in the quickest time as possible. Not every security inspection check performed by the tool on the item present on the server may lead to a problem, but there are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know about existence of such types of items present on the server. These items are usually marked appropriate in the information printed. There are also some checks for unknown items which have been observed during scanning of the log files. Some of the features provided by the tool are listed are as follows :

   - SSL Support
   - Full HTTP proxy support.
   - Checks for outdated server components.
   - Save reports in plain text, XML, HTML, NBE or CSV.
   - Template engine to easily customize reports.
   - Scan multiple ports on a server, or multiple servers via input file.
   - Identifies installed software's via headers, favicons and files.
   - Mutation techniques to "fish" for content on web servers.
   - Reports "Unusual" contents seen
   - Save full request/response for positive tests.
   - Auto-pause at a specified time and replay saved positive requests.

Review Questions

Q. 1 What is cybercrime? Explain various types of cybercrime.

Q. 2 Explain classification of cybercriminals.

Q. 3 What is the role of computer in cybercrime?

Q. 4 Explain the prevention of cybercrime.

Q. 5 What is ethical hacking and what are the goals of ethical hacking?

Q. 6 Write the difference between hackers, crackers and phreakers.

Q. 7 Explain the rules of ethical hacking.

Q. 8 What are the various phases involved in ethical hacking?

Q. 9 Explain ethical hacking reconnaissance tools and scanning tools.

❑❑❑

Digital Forensics Fundamentals

Syllabus

Introduction to Digital Forensics, Need and Objectives of Digital Forensics, Types of Digital Forensics, Process of Digital Forensics, Benefits of Digital Forensics, Chain of Custody, Anti Forensics.

Digital Evidence and its Types, Rules of Digital Evidences.

Incident Response, Methodology of Incident Response, Roles of CSIRT in handling incident.

Self Learning Topics : Pre Incident preparation and Incident Response process.

Topics

2.1 Introduction to Digital Forensics

2.2 Types of Digital Forensics

2.3 Process of Digital Forensics

2.4 Benefits of Digital Forensics

2.5 Chain of Custody

2.6 Anti Forensics

2.7 Digital Evidence and its Types

2.8 Incident Response

2.9 Roles of CSIRT in Handling Incident

2.10 Self Learning Topics : Pre-Incident Preparation and Incident Response Process

2.1 Introduction to Digital Forensics

Digital forensic is collection, preservation, analysis and presentation of computer-related evidence. It determines the past actions that have taken place on a computer system using computer forensic techniques.

Digital/Computer forensics is the process of methodically examining computer media (Hard disks, diskettes, tapes, etc.) for evidence.

History of Digital Forensic

Digital Forensics was established as a distinct scientific domain during the 1800s and early 1900s. The contributions of this new area of science intensely changed the effectiveness of law enforcement. Some notable milestones of forensic science are given in Table 2.1.1.

Table 2.1.1 : History of Digital Forensics

Year	Development in Forensic Science
1787-1853	Mathieu Orfila considered the father of forensic toxicology, published the first scientific text on forensic toxicology in 1814.
1853-1914	Alphonse Bertillon developed a method for identification through body measurements and published a system on personal identification in 1879.
1822-1911	Francis Galton studied fingerprints as a means of identification and published the book Finger Prints in 1892.
1847-1915	Hans Gross established the principles for the application of science in investigations in several publications, the first one in 1893.
1858-1946	Alberts S. Osborn established scientific principles for document examination and published the book Questioned Documents in 1910.
1887-1954	Leone Lattes studied characteristics of blood types for identification and created a method for the analysis of blood groups in blood stains in 1915.
1877-1966	Edmond Locard recognized worldwide for promoting the scientific method in criminal investigation, established a police laboratory in Lyon in 1910.

2.1.1 Need and Objectives of Digital Forensics

Need of Digital Forensics

- A few criminals are becoming smarter; they use data-hiding techniques which include *encryption* and *steganography*. Here, the evidence of criminal activity is placed in such a way where traditional search methods cannot able to find it.
- Digital forensics is necessary to collect, analyze and present proofs to the criminal or civil courts. Network administrator and security staff administer and manage networks and information systems should have complete knowledge of computer forensics. The meaning of the word "forensics" is "to bring to the court". Forensics is the process which deals in finding evidence and recovering the data. The evidence includes many forms such as finger prints, DNA test or complete files on computer hard drives etc. The consistency and standardization of computer forensics across courts is not recognized strongly because it is new discipline.
- It is necessary for network administrator and security staff of networked organizations to practice digital forensics and should have knowledge of laws because rate of cyber crimes is increasing greatly. It is very interesting for mangers and personnel who want to know how computer forensics can become a strategic element of their organization security. Personnel, security staff and network administrator should know all the issues related to computer forensics.
- Computer experts use advanced tools and techniques to recover deleted, damaged or corrupt data and evidence against attacks and intrusions. These evidences are collected to follow cases in criminal and civil courts against those culprits who committed computer crimes.
- The survivability and integrity of network infrastructure of any organization depends on the application of digital forensics. In the current situations computer forensics should be taken as the basic element of computer and network security. It would be a great advantage to any company if you know all the technical and legal aspects of digital forensics. If your network is attacked and intruder is caught then good knowledge about computer forensics will help to provide evidence and put on trial the case in the court.
- There are many risks if you practice digital forensics badly. If you don't take it in account then vital evidence might be destroyed. New laws are being developed to protect customers' data; but if certain kind of data is not properly protected then many liabilities can be assigned to the organization. New rules can bring organizations in criminal or civil courts if the organizations fail to protect customer data.
- As organizations are increasing in number and the risk of hackers and contractors is also increase so they have developed their own security systems. Organizations have developed security devices for their network like Intrusions Detection Systems (IDS), proxies, firewalls which report on the security status of network of an organization.

- So technically the major goal of computer forensics is to recognize, gather, protect and examine data in such a way that protects the integrity of the collected evidence to use it efficiently and effectively in a case.
- Investigation of computer forensics has some typical aspects. In first area computer experts who investigate computers should know the type of evidence they are looking for to make their search effective. Computer crimes are wide in range such as child pornography, theft of personal data and destruction of data or computer. Second, computer experts or investigators should use suitable tools to recover the deleted, encrypted or damaged files and prevent further damage in the process of recovery.
- In digital forensics two kinds of data are collected. Persistent data is stored on local disk drives or on other media and is protected when the computer is powered off or turned off. Volatile data is stored in random access memory and is lost when the computer is turned off or loses power. Volatile data is located in caches, Random Access Memory (RAM) and registers. Computer expert or investigator should know trusted ways to capture volatile data. Security staff and network administrators should have knowledge about network and computer administration task effects on computer forensics process and the ability to recover data lost in a security incident.

Objectives of Digital Forensics

The following are the primary objectives of employing digital forensics :

- It aids in the recovery, analysis, and preservation of computer and associated materials in order for the investigating agency to submit them as evidence in a court of law.
- It aids in determining the reason for the crime and the identify of the primary perpetrator.
- Creating processes at a suspected crime scene to guarantee that the digital evidence gathered is not tainted.
- Data collection and duplication : Recovering lost files and partitions from digital media in order to extract and evaluate evidence.
- Allows you to rapidly discover evidence and evaluate the possible impact of harmful action on the victim.
- Creating a computer forensic report that provides a comprehensive report on the investigative process.
- Keeping the evidence safe by adhering to the chain of custody.

2.2 Types of Digital Forensics

There are many sub branches of digital forensics, they are as follows :

1. Network Forensics
2. Database Forensics

3. Mobile Forensics
4. Computer Forensics
5. Disk Forensics
6. Wireless Forensics
7. Email Forensics
8. Enterprise Forensic
9. Web Forensics
10. Cyber Forensics
11. Malware Forensics

1. Network Forensics

Network forensics is a sub-branch of digital forensics. Network forensics is related to monitoring, capture, storing and analysis of network activities to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.

2. Database Forensics

Database forensics is related to the study and investigation of databases and their relative metadata. The analysis of data and metadata contained in databases like Microsoft SQL, Oracle and others. This information is helpful in tracking financial crime activity in addition to establishing timelines of events.

3. Mobile Forensics

As mobile phones began to become ubiquitous in the near the beginning aught, this category emerged. Mobile forensics is used to recover data from the mobile devices. A mobile device is generally defined as one with a built-in communication system (GSM or SMS) and location information through GPS; however, mobile devices also include cameras and USB drives. It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS, MMS, Audio, videos, etc.

4. Computer Forensics

This computer forensics deals with computers, embedded systems and static memories like USB drives. Extensive range of information from logs to original files on drive can be investigated in computer forensics.

5. Disk Forensics

Disk forensics deals with the storage media like hard disk, pen drive etc. It extracts data from storage media by searching active, modified, or deleted files.

6. Wireless Forensics

Wireless forensics is a division of network forensics. Wireless forensics offers the tools required to collect and analyze the data from wireless network traffic.

7. Email Forensics

Email forensic deals with the crimes done through the email like fraud, abuse, defamation etc. In Email forensics recovery and the analysis of the emails is performed. It includes the deleted emails, contacts and calendar information.

8. Enterprise Forensic

Enterprise forensics helps to provide end-to-end post analysis data which gives support departments the ability to identify evidence that can be pursued or sent to legal authorities to manage.

9. Web Forensics

Web forensics deals with the investigation of the crime that has happened on the Internet. It analyzes the origins, contents, patterns and transmission paths of email and Web pages as well as browser history and Web server scripts and header messages. See computer forensics.

10. Cyber forensics

Cyber forensics is an electronic discovery technique used to collect and protect evidence from a particular computing device that determines and reveals technical criminal evidence. It deals with electronic data storage extraction for legal purposes. Cyber forensic deals with Cross-driven analysis that correlates data from many hard drives, live analysis in which it obtains data acquisitions before a PC is shut down, and recovery of deleted file.

11. Malware Forensics

Malware forensics deals with the identification of malicious code, to study their payload, viruses, worms and so on.

2.3 Process of Digital Forensics

For forensic investigation there are following four common steps :

1. Collection
2. Examination
3. Analysis
4. Reporting

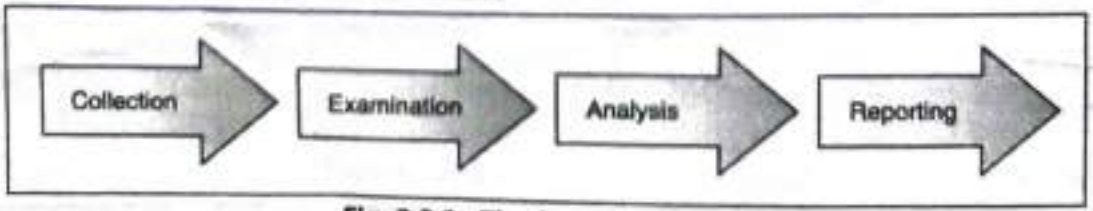


Fig. 2.3.1 : The forensic process

1. **Collection** : This is the first phase in forensic process. In this phase data is identified, labelled and recorded and gathering the data and physical evidence related to the incident being invested is done. Simultaneously integrity of the chain of custody is also preserved.
2. **Examination** : In this phase from the collected data identify and extract the pertinent information, using proper forensic tools and techniques and also maintain integrity of the evidence.
3. **Analysis** : In this phase results of the examination phase are analyzed. From the analysis useful answers to the questions are generated which are presented in the previous phases. Most probably the case gets solved in this phase.
4. **Reporting** : In the reporting phase the results of the analysis are done, which contains :
   - The information pertinent to the case.
   - Actions that have been accomplished actions left to be performed.
   - Moves left to be performed.
   - Advocated enhancements to processes and tools.

What things are we investigating?

- Investigating the identity theft.
- Investigating the fraud and embezzlement.
- Investigating the software piracy and hacking.
- Investigating the blackmail and extortion.
- Investigating the child pornography and exploitation.
- Investigating the prostitution, infidelity, domestic violence.
- Investigating the terrorism and national security.
- Investigating the theft of intellectual property and trade secrets.

What Evidence can we Recover at the Time of Investigation?

1. **Investigation of Computer Fraud**

   While investigating the computer fraud we recover following information :

   - Credit card data
   - Financial and asset records
   - E-mail, notes, and letters
   - Accounting software and files
   - Account data from online auctions.

2. Investigation of Child Exploitation

While investigating the Child exploitation we recover following information :

- Photos and digital camera software
- Internet activity logs
- Movie files
- User-created directory and file names to classify images.
- Chat logs
- Graphic editing and viewing software.

3. Investigations of Network Intrusion and Hacking

While investigating the network Intrusion and hacking we recover the following information :

- Names of the Network users.
- Internet Protocol (IP) addresses.
- Executable files which also includes viruses and spyware.
- Security logs and Configuration files.
- Text files and other documents containing sensitive information such as passwords.

4. Investigation of Identity Theft

Investigation of Identity Theft will recover the following information :

- Credit card numbers and the credit card readers, writers and scanners.
- Identification Templates such as driving license, birth certificates etc.
- Images of the electronic signatures.
- Information of online trading.

5. Investigation of Harassment and Stalking

While investigating the Harassment and Stalking we recover following information :

- Research of the victim's background
- Victim's location maps
- Photos of the victim
- Diaries of the victim
- Internet activity logs
- E-mails, notes, and letters.

6. **Investigation of Software Piracy**

While investigating the Software Piracy we recover following information :

- Serial numbers of the software.
- Utilities for the software cracking.
- Image files of software licenses.
- Binary files which are required for software installation.
- Chat logs and Internet activity logs.

2.4 Benefits of Digital Forensics

The key benefits of digital forensics :

1. To ensure the computer system's integrity.
2. Produce evidence in court that can lead to the perpetrator's punishment.
3. It assists businesses in capturing critical data if their computer systems or networks are compromised.
4. Tracks down cybercriminals from all over the world with ease.
5. Aids in the safeguarding of the organization's funds and time.
6. Allows you to extract, process, and interpret factual evidence in order to prove cybercrime in court.

2.5 Chain of Custody

- Chain of custody means documentation that identifies all changes in the control, handling, custody and ownership of a piece of evidence.
- The gathered evidences should stored in a tamper - proof manner means that evidence cannot be accessed by unauthorized person, it helps in maintain the chain of custody. For each obtained item a complete chain-of-custody record is kept.
- Chain of custody needs that you can trace the place of the evidence from the instant it was collected to the instant it was presented in a judicial court. Many police departments and federal law enforcement agencies have property departments that store evidence in a secure place to meet the chain of custody requirement.
- Whenever the Experts and law enforcement officers required reviewing the evidence then check-out the evidence, and then check-in the evidence every time it is returned to storage.
- Organization's best evidence should be stored in a safe room or storage so that is inaccessible to anyone other than the appointed evidence custodians. This storage area is also known as "evidence safe." Access to evidence safe is controlled by the evidence custodians.

Chain of Custody Process

The chain of custody should extend from the first step of data collection to examination, analysis, reporting, and the time of presentation to the courts in order to preserve digital evidence. This is critical in order to avoid any suggestion that the evidence has been tampered with in any way.

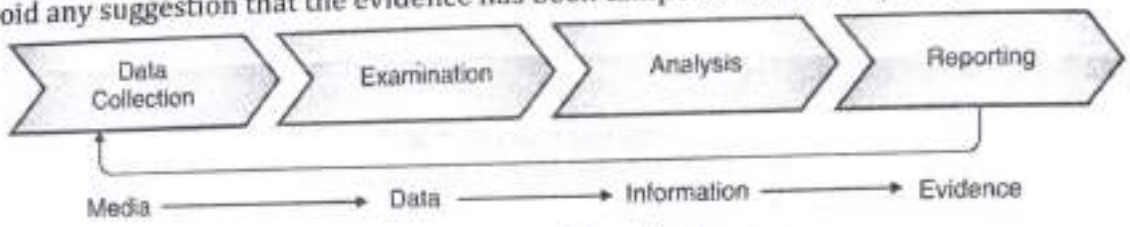


Fig. 2.5.1 : Chain of Custody Process

1. **Data collection** : It is the first step in the chain of custody process. It entails the identification, labelling, recording, and acquisition of data from all relevant sources while maintaining the data and evidence's integrity.
2. **Examination** : During this step, the chain of custody information is documented, as well as the forensic procedure that was followed. It's critical to take screenshots throughout the process to demonstrate the tasks that have been completed and the evidence that has been discovered.
3. **Analysis** : The result of the examination stage is the analysis stage. In the Analysis stage, legally justifiable methods and techniques are used to gather useful information in order to respond to the questions posed in the case.
4. **Reporting** : In the Examination and Analysis stage, this is the documentation phase. The following items are included in reporting :
   - A statement about the Chain of Custody.
   - The various tools that were used are explained.
   - A description of how various data sources were analysed.
   - Issues have been identified.
   - Vulnerabilities have been discovered.
   - Additional forensics measures that can be taken are suggested.

The procedure for establishing the Chain of Custody

A series of steps must be followed in order to ensure the chain of custody's authenticity. It's worth noting that the more information a forensic expert obtains about the evidence, the more reliable the chain of custody created becomes. According to the chain of custody for electronic devices, you should ensure that the following procedure is followed :

- Save the original files.
- Photograph the physical evidence.

- Taking screenshots of the digital evidence is a good idea.
- Date, time, and any other information about the evidence's receipt should be documented.
- Inject forensic computers with a bit-for-bit clone of digital evidence content.
- To authenticate the working clone, perform a hash test analysis.

2.6 Anti Forensics

- Digital forensics investigators are frustrated by anti-forensics techniques. They have the skills and tools to deceive digital forensics investigators. Furthermore, after a data breach or malware campaign, cybercriminals use anti-forensics tools to hide their tracks from computer forensics experts.
- Any strategy or software used to thwart a computer investigation is known as anti-forensics. Information can be hidden in a variety of ways. By altering data, some applications can deceive computers. Data can be circumvented by changing the header or metadata, or by changing the file extension from .jpg to .mp3 to fool people into thinking it's an audio file.
- Anti-forensic techniques are used by cybercriminals to falsify the cyber forensics evidence report, leading forensic investigators down the wrong path. As a result, retrieving any evidence from the crime scene becomes a difficult task for the forensic investigator. To identify these anti-forensic techniques, the forensics investigation process takes a long time.
- Anti-forensic methods are employed to :
  1. Cybercrime evidence should be removed.
  2. Reports from forensic analysts that have been compromised.
  3. Delete or change.
- It's difficult for forensic investigators to recover any solid evidence against the attacker or track down the attacker's digital footprints. As a result, they are unable to pinpoint the source of the attack in order to recover stolen data or contact the attacker group in order to negotiate the attacks' outcomes. A threat or malware detection tool or security analysis may miss several anti-forensic techniques.

2.6.1 Anti-Forensic Techniques

With the rise in ransomware attacks and other malware campaigns, it's clear that cybercriminals are becoming more sophisticated in their attack methods. Threat attackers use a variety of anti-forensics techniques, including :

1. **Encryption**

Encryption, the art of embedding confidential and sensitive information into ciphertext, is one of the most widely used anti-forensic techniques (garbled text). Unwanted eyes are prevented from seeing the hidden text, image, or code using modern encryption algorithms. To hide their malicious codes or campaigns, attackers use full-volume encryption and a key file.

A secret key is used to encrypt the data, which is then decrypted at the destination point, converting ciphertext to plain text. Without an authenticated secret key, forensic analysts are unable to decrypt malicious files. Many security screening techniques and tools fail to detect malicious files that are encrypted.

2. Program packers

Attackers use a variety of anti-forensics techniques to hide their data from detection and scanning methods. Program packers are just one of them. The packers compress/encrypt the data files and other executable file codes first, similar to cryptography. Initially, programme packers were used to reduce the size of files and programmes. However, hackers began to use packers to conceal an infected file or programme in order to evade detection by anti-malware tools or security analysis.

UPX, The Enigma Protector, MPRESS, and other packers have been used for malicious purposes.

3. Overwriting data

To avoid forensics investigations and reduce digital footprints, attackers overwrite programmes. Securely deleting data, also known as data cleaning or data erasure, is an old trick used by cybercriminals. Many tools exist today that can overwrite critical text, metadata, or entire media files on a storage system, obstructing forensic analysts' recovery efforts. The attacker's digital footprints of false and altered data are reduced using this technique of overwriting original data. Examples of data that have been overwritten are :

- All original data is overwritten.
- Individual files are overwritten
- Overwriting and working on previously deleted files until there is no more free space.

4. Onion routing

Onion routing is a technique for communicating anonymously over a network in which messages are layered encrypted. The name comes from the fact that the layered encryption looks like an onion. Hackers can use the Onion Router, or TOR, to access the internet anonymously, giving them a great way to access the dark web, hide their tracks, and launch cyberattacks. Hackers can use Onion Routing to hide their online activities, IP addresses, and network usage.

Data is routed through multiple network nodes using onion routing, each with layered encryption. When the last encryption layer is passed through, the data reaches its destination. To find the attacker, forensic investigators will successfully break through each layer from the destination to the exit node. Onion routing makes it more difficult for forensic investigators to track down the attacker and lengthens the time it takes to conduct a security analysis.

5. **Steganography**

Steganography is the process of concealing secret messages or information in a non-suspicious manner within an audio, image, video, or text file. To provide an extra layer of security, steganography techniques are frequently combined with encryption. The secret data is extracted using a steganography tool for decoding the hidden message by the authenticated person with access to the destination. To get around security and obfuscate their tracks, hackers have been using steganography to hide malicious codes and files within legitimate files. This anti-forensic technique enables attackers to carry out malicious activities while avoiding detection by threat detection tools and other security parameters. Hackers have been known to use invisible ink to hide secret malicious payloads or suspicious messages within images of celebrities, news articles, advertisements, and other media.

6. **Changing Timestamps**

By determining the location and time of the attack, forensic investigators can track down the perpetrator. As a result, attackers employ anti-forensic techniques such as changing timestamps to conceal or eliminate logs, as well as determining the attacker's location or the time of attack. Changing timestamps can cause entries to be deleted or entry logs to be overwritten, making it difficult for the investigator to determine the true information for evidence. Attackers can also change the timestamp of a file or programme to get around the investigation. To get around network security, they change the timestamp on the servers, launch an attack, and delete the evidence without it being logged into the server.

2.7 Digital Evidence and its Types

Evidence is any information of supporting value, that means which proves something or helps to prove something relevant to the case.

The types of evidences are :

1. Real evidence
2. Documentary evidence
3. Testimonial evidence
4. Demonstrative evidence

1. **Real evidence :** Real evidences are something that one can carry into courtroom and show it in front of the jury. Real evidences are the most powerful evidences. This evidence typically "speaks for itself."
2. **Documentary proof :** The evidence which is in the written form is nothing but the documentary evidence. For example server logs, email, database document etc. Documentary evidence might be faked via a professional pc user and therefore must be authenticated to be admissible in courtroom. Continually produce the original document, do not use the copy.

3. **Testimonial evidence :** Testimonial evidence is nothing but the statement of a witness, underneath oath, either in court or by deposition. This sort of evidence normally helps or validates the alternative types.
4. **Demonstrative evidence** : Demonstrative evidence recreates or explains different evidence. Demonstrative evidence does not "talk for itself" and is used to demonstrate and make clear previous points. This sort of evidence is maximum helpful in explaining technical topics to non-technical audiences.

2.7.1 Rules of Digital Evidences

There are 5 cardinal rules involved to facilitate a forensically sound investigation of the computer media. These rules enable the investigator to testify the evidences in the court in respect of their handling a particular piece of evidence.

The Rules of digital forensics are :

Rule 1 : Document everything

When the investigator carries out investigation then document each and everything that lying in front of investigator. This documentation of evidence helps to form the chain of evidence. It provides the following functions :

- Identify the evidence
- A legal authority copy should be obtained.
- Chain of custody as well as initial count of evidence to be examined.
- Information concerning the packaging and condition of the evidence upon receipt by the examiner.
- Lists the dates and times the evidence was handled.
- Documentation should be preserved according to the examiner's agency policy.

Rule 2 : Never trust the subject's operating system

Computer criminal can alter the routine operating system commands to carry out destructive commands. Using the subject's operating system could easily destroy data with just a few keystrokes. When the subject computer starts, booting to hard disks overwrites and changes evidentiary data. To make sure that data is not altered, we need to monitor the subject's computer during initial bootstrap to identify the correct key to use access the CMOs setup.

Rule 3 : Never Work on the original evidence

Never work on the original evidence as the digital evidence is very delicate in nature. To preserve the integrity of the digital evidence and any unknowing change, preserve the original evidence in its perfect condition. It is easy to work on the original evidence with less cost but if the evidence will lose its integrity, authenticity and will not be admissible in any court when it is used directly.

Rule 4 : Never Mishandle the Evidence

This rule states preserve that evidence. The evidence should not to be tampered with or contaminated. Secure collection of evidence is important to guarantee the evidential integrity and security of information. The best approach for this matter is to use disk imaging tool. Choosing and using the right imaging tool is very important in cyber forensics investigation.

Disk imaging tool make a bit stream duplicate or an image of the original disk. Imaging preserves the original evidence. Chain of custody is used to check who recovered the evidence and when, and who possessed it and when a chain-of-evidence form is generated and filled, which helps the examiner to document what has and has not been done with both the original evidence and the forensic copies of the evidence.

Rule 5 : The results should be repeatable and verifiable by a third party

This rule states that the analysis done on the evidence should be completely audited by the third party. To establish the integrity of information a cryptographic hash value, such as MD5 or SHA-1 are calculated so that it can be proven to the courts. Chain of custody forms are created if evidence are used in court or verified by any third party. The same process can be conducted and verified by any expert or person.

2.8 Incident Response

2.8.1 Computer Security Incident

Computer security Incident is any unlawful, unauthorized, or unsuitable activity that includes a computer system or a computer network. Such an activity can incorporate any of the following events :

1. Theft of the trade secrets.
2. Email spam or harassment.
3. Embezzlement.
4. Unauthorized or unlawful intrusions into computing systems.
5. Denial-of-service (DoS) attacks.
6. Extortion.
7. Any unlawful action when the evidence of such action may be stored on computer media.

   For example fraud, threats, and traditional crimes.
8. Possession or dissemination of child pornography.

2.8.2 Goals of Incident Response

The goals of the Incident response are as follows :

1. To prevent a disconnected, no cohesive response.

2. Confirms or dispels whether an incident happened.
3. Promotes gathering of accurate information.
4. Establishes controls for proper retrieval and handling of evidence.
5. Protects privacy rights established by law and policy.
6. Minimizes damage to business and network operations.
7. Allows for criminal or civil action against culprits.
8. Provides accurate reports and useful recommendations.
9. Provides quick detection and containment.
10. Minimizes exposure and compromise of proprietary data.
11. Protects your organization's reputation and assets.
12. Educates senior management.
13. Promotes quick detection and/or prevention of such incidents in the future.

2.8.3 Methodology of Incident Response

Computer security incidents are often complicated, multifaceted troubles like any complex engineering problem. Black box approach is used to solve the incident problem. In this approach divide the larger problem of incident resolution into components and test the inputs and outputs of each component. Fig. 2.8.1 illustrates our approach to incident response.

In our methodology, there are seven important components of incident response :

- **Pre-incident preparation :** In this phase actions are taken to prepare the organization and the CSIRT before an incident occur.
- **Detection of incidents :** In this phase potential computer security incident is identified.
- **Initial response :** In this phase an initial investigation is performed. The basic details surrounding the incident are recorded. The incident response team is assembled and individuals who need to know about the incident are notified.
- **Formulate response strategy :** In this phase best response is determined and the management approval is taken based on the results of all the known facts. What types of civil, criminal, administrative, or other actions are appropriate to take are determined, based on the conclusions got from the investigation.
- **Investigate the incident :** In this phase thorough collection of data. To determine what happened, when it happened, who did it, and how it can be prevented in the future is reviewed from the collected data.

- **Reporting** : In this phase information is accurately reported about the investigation in a manner useful to decision makers.
- **Resolution** : In this phase security measures are employed. For any problem procedural changes, record lessons learned, and develop long-term fixes are identified.

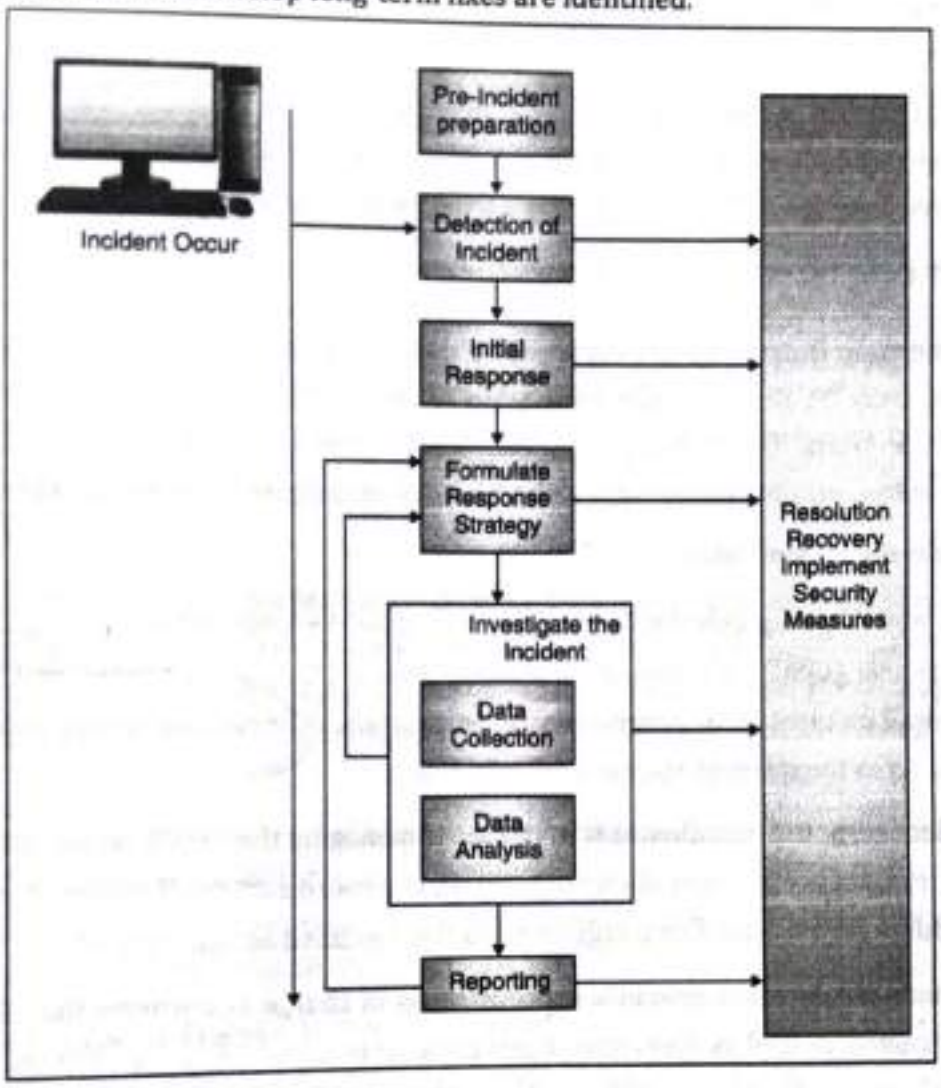


Fig. 2.8.1 : Incident Response Methodology

2.9 Roles of CSIRT in Handling Incident

- After the incident response charter has been finalised, the *Computer Security Incident Response Team* (*CSIRT*) will be staffed. Larger businesses with adequate resources may be able to assign employees to crisis response tasks on a full-time basis.
- However, more often than not, businesses will be forced to use employees that have other responsibilities in addition to incident response. Personnel in the internal CSIRT are classified into three groups :

1. Core team,

2. Technical support,
3. Organisational support.

- Each member of the CSIRT is responsible for a certain duty. It requires more than just assigning employees and developing a policy and procedure document to build this capacity within an organisation.
- An effective CSIRT, like any big project venture, needs a significant amount of effort. There are distinct duties and responsibilities for each of the CSIRT categories. This diverse group of individuals is intended to give direction and support during a wide range of situations, from minor to disastrous.

2.9.1 The CSIRT Core Team

The CSIRT core team is made up of people who either work full-time in incident response or take on incident response tasks on the side. The core team is frequently made up of people assigned to the information security team. Other companies can benefit from individuals with incident response experience. Some of the responsibilities that can be included in the core team are as follows :

1. The incident response coordinator

- The incident response coordinator is often the Chief Security Officer (CSO), Chief Information Security Officer (CISO), or Information Security Officer (ISO), as that individual is often in charge of the overall security of the organization's information. Other organisations may appoint a single person to act as the incident response coordinator.
- The incident response coordinator is in charge of managing the CSIRT before, during, and after an event. In terms of preparation, the incident response coordinator will ensure that any CSIRT plans or procedures are evaluated on a regular basis and modified as appropriate.
- Furthermore, the incident response coordinator is in charge of ensuring that the CSIRT team is properly trained, as well as overseeing testing and training for CSIRT employees.
- During an event, the incident response coordinator is in charge of ensuring effective incident response and remediation and guiding the team through the full incident response process. Coordination of the CSIRT with senior leadership is one of the most critical of these duties during an event. With the stakes of a data breach so high, top leadership, such as the CEO, will want to be kept up to date on crucial event information. It is the role of the incident response coordinator to keep senior leadership up to date on all incident-related actions.
- Finally, the incident response coordinator is responsible for ensuring that the event is correctly recorded and that reports of CSIRT activities are given to the relevant internal and external stakeholders at the conclusion of an incident. In addition, all CSIRT operations are thoroughly debriefed, and lessons gained are integrated into the CSIRT Plan.

2. **CSIRT Senior Analyst(s)**

- CSIRT Senior Analysts have significant training and expertise in incident response as well as related capabilities such as digital forensics or network data inspection. They frequently have several years of incident response expertise as a consultant or as part of an organisation CSIRT.
- During the incident response process's preparation phase, they are involved in ensuring that they have the appropriate skills and training to address their unique position in the CSIRT. They are also frequently instructed to help in the evaluation and revision of incident response plans. Finally, experienced analysts are frequently involved in the training of junior members of the team.
- Once an event has been detected, senior analysts will collaborate with other CSIRT members to gather and evaluate evidence, direct containment efforts, and aid other staff with clean-up. After an event, top analysts will ensure that both they and other staff properly document the occurrence. This will entail preparing reports for internal and external stakeholders. They will also ensure that any evidence is preserved or destroyed in accordance with the incident response strategy.

3. **CSIRT Analyst(s)**

- CSIRT Analysts are CSIRT professionals who have little exposure to or experience with incident response operations. They frequently have only one or two years of incident response experience. As a result, they can engage in a range of tasks, some of which are directed by senior analysts. Analysts' skills will be developed through training and exercises throughout the preparation period.
- They may also be involved in incident response plan evaluations and upgrades. They will be charged for acquiring evidence from possibly hacked hosts, network devices, or different log sources during an event. Analysts will also participate in evidence analysis and will support other team members with remedial efforts.

4. **Security operations centre analyst**

- Larger companies may have a 24/7 Security Operations Center (SOC) monitoring capacity in-house or hired. When it comes to incident identification and alerting, analysts assigned to the SOC are frequently the point person.
- As a consequence, having a SOC analyst on the team allows them to be taught on methodologies and respond to a possible security issue practically immediately.

5. **IT Security Engineer / Analyst(s)**

- Depending on the organization's size, there may be employees particularly assigned with the deployment, maintenance, and monitoring of security-related software such as anti-virus or hardware such as firewalls or SIEM systems. When an issue has been detected, having immediate access to these devices is important. Personnel assigned to these tasks will frequently have a direct part in the whole incident response process.

- The IT Security Engineer or Analyst will frequently be responsible for a substantial portion of the incident response process's preparation. They will be the key resource for ensuring that security apps and devices are correctly set to alert to potential issues and that the devices properly log information so that events may be reconstructed.
- They will be entrusted with monitoring security systems for additional signs of hostile conduct during an event. They will also help the other CSIRT members gather proof from the security equipment. Finally, following an event, these people will be charged with setting security devices to watch for suspicious behaviour in order to confirm that remediation operations have removed malicious activity from compromised systems.

2.9.2 Technical Support Personnel

Technical support employees are those inside the company that do not have CSIRT activities as part of their day-to-day operations but have knowledge or access to systems and procedures that may be impacted by an event. For example, the CSIRT may need to hire a server administrator to help the core team collect evidence from servers such as memory grabs or logs. Once accomplished, the server administrator's job is complete, and they may not be involved in the event again.

The following are some of the people that can help the CSIRT during an incident :

1. **Network Architect/Administrator :** Network infrastructure is frequently involved in incidents. This covers router, switch, and other network hardware and software assaults. The Network Architect or Administrator is critical for understanding typical and abnormal behaviour of these devices, as well as recognising anomalous network traffic. In events involving network infrastructure, these support staff can help acquire network evidence such as access logs or packet captures.
2. **Server Administrator :** Threat actors frequently target network systems that hold vital or sensitive data. Domain controllers, file servers, and database servers are common high-value targets. Log files from these systems can be obtained with the assistance of server administrators. If the server administrator(s) are also in charge of active directory structure management, they may be able to assist with detecting new user accounts or making modifications to existing user or administrator accounts.
3. **Application support :** Threat actors frequently attack web apps. Some security breaches are caused by coding flaws that enable for attacks such as SQL injection or security misconfigurations. As a result of having application support staff as part of the CSIRT, direct information about application assaults is possible. These experts are frequently able to spot code modifications or validate vulnerabilities found during an examination into a possible application attack.

4. **Desktop Support :** Desktop support workers are frequently involved in the maintenance of controls such as data loss prevention and anti-virus on desktop computers. In the case of an incident, they can aid in delivering log files and other evidence to the CSIRT. During the incident's remediation phase, they may also be in charge of cleaning up affected systems.
5. **Help desk :** When it comes to recognising an issue, help desk staff are the proverbial canary in the coal mine, depending on the company. When a user detects the first symptoms of a malware infection or other harmful behaviour, they are frequently the first people contacted. As a result, help desk staff should be included in CSIRT response training as well as their involvement in incident identification and escalation protocols. In the case of a large occurrence, they may also aid in locating other impacted personnel.

2.9.3 Organizational Support Personnel

Other organisational members that should be included in the CSIRT should be included outside of the technical area. Organizational people can help with a variety of non-technical concerns that are not handled by CSIRT core and technical support personnel. These include navigating the internal and external legal environments, aiding with customer contacts, and assisting CSIRT employees on-site.

Some of the organisational support individuals who should be included in a CSIRT Plan are as follows :

1. **Legal**
   - Data breaches and other occurrences raise a number of legal concerns. Many nations currently have breach notification regulations that compel businesses to notify customers if their information has been compromised. Other compliance mandates, such as HIPAA and the PCI DSS, require the impacted business to contact and alert various external organisations of a suspected breach.
   - Involving legal counsel early in the incident response process ensures that these notifications, as well as any other legal requirements, are addressed in a timely manner. If an inside source, such as an employee or contractor, is responsible for the breach, the harmed company may choose to seek restitution through legal action. Including legal assistance early in the process allows for a better-informed selection about the legal method to use.
2. **Human resources**
   - Employees or contractors are responsible for many incidents that occur in businesses. The CSIRT may be called in to examine acts ranging from fraud to large-scale data theft. If an employee or contractor is the subject of the inquiry, the human resources department can assist in verifying that the CSIRT's operations are in accordance with applicable labour laws and corporate regulations.
   - If an employee or contractor is to be terminated, the CSIRT can work with human resources to ensure that all necessary documentation on the event is completed, reducing the possibility of a wrongful termination claim.

3. **Marketing/communications**

- If an incident, such as a Denial-of-Service attack or data breach, may have a negative impact on external clients or customers, the marketing or communications department can assist in crafting the appropriate message to assuage fears and ensure that those external entities are receiving the best information possible.
- When looking back at previous data breaches, there was a reaction against those businesses that tried to keep the facts to themselves and did not notify customers. Having a good communications plan in place and putting it into action early can go a long way toward calming any possible consumer or client negative reactions.

4. **Facilities**

- The CSIRT may require access to places after hours or for an extended period of time. The facilities department can assist the CSIRT in acquiring the appropriate access as soon as possible.
- Additionally, facilities may have access to extra meeting places for the CSIRT to use in the case of a long-term crisis that necessitates dedicated workspace and infrastructure.

5. **Corporate security**

- The CSIRT may be called in to deal with an organization's theft of network resources or other technologies. Theft of laptops and digital material is quite prevalent.
- Surveillance footage from entrances and exits is frequently available to corporate security. They may also keep access badge and visitor records for the CSIRT to track employee and other personnel movement within the site. This allows for the reconstruction of events before a theft or other conditions that led up to the incident.

External resources

Many sectors have professional associations where practitioners may join together to discuss information, independent of their employment. At times, CSIRT staff may be entrusted with interacting with law enforcement and government authorities, particularly if they are targeted as part of a broader attack on a number of similar businesses. Relationships with other organisations and agencies can help the CSIRT share intelligence and resources in the case of an incident. Among these resources are the following :

1. **High Technology Crime Investigation Association (HTCIA)** : The HTCIA is a worldwide organisation of professionals and students dedicated to the investigation of high-tech crime. Resources range from digital forensics techniques to enterprise-level data that might assist CSIRT staff with new approaches and procedures.

2. **InfraGard** : The Federal Bureau of Investigation has established a private-public collaboration aimed at networking and information sharing for CSIRT and information security practitioners in the United States. This collaboration enables CSIRT members to share information about trends and discuss previous investigations.

3. **Law enforcement** : There has been an exponential increase in cyber-related criminal activities. As a result, several law enforcement agencies have strengthened their capabilities to investigate cybercrime. Leadership of the CSIRT should establish relationships with agencies that have cybercrime investigation skills. Law enforcement agencies can give insight into specific threats or crimes that are being perpetrated, as well as providing CSIRTs with any information that is of concern to them.

4. **Vendors** : In the case of an incident, external vendors can be used, and what they can give is frequently based on the specific line of business in which the company has engaged them. For example, an organization's IPS/IDS solution provider may be able to assist in the creation of bespoke alerting and blocking rules to aid in the identification and containment of malicious activity. Threat intelligence vendors can also give recommendations on harmful behaviour indications. Finally, some companies will need to employ vendors who specialise in a certain incident response expertise, such as reverse engineering malware, if such capabilities are outside an organization's competence.

2.10 Self Learning Topics : Pre-Incident Preparation and Incident Response Process

1. Pre-Incident Preparation

Preparation leads to successful incident response. Incident response is reactive in nature. In this phase there is need to prepare :

a. Organization

b. CSIRT

Preparing the Organization

Preparing the organization contains developing all of the company-wide strategies you want to employ to better pose your organization for incident response. This contains the following :

a. Applying host-based security measures.

b. Applying network-based security measures.

c. Training end users.

d. Hire an Intrusion Detection System (IDS).

e. Creating strong access control.

f. Performing timely vulnerability examination.

g. Ensuring backups are done on a regular basis.

Preparing the CSIRT

The organization will gather a team of specialists to handle any incidents that arise. Preparing the CSIRT consists of considering at least the following :

a. The hardware required to investigate computer security incidents.

b. The software required to investigate computer safety incidents.

c. The documentation like forms and reports required to investigate computer safety incidents.

d. The ideal guidelines and operating tactics to implement your response techniques.

e. The training required to perform the incident response to staff or employees.

2. **Detection of Incidents**

- The detection of incidents phase is one of the maximum critical elements of incident reaction. Detection of incident is a most decentralized phase. In this phase the incident response expertise have the least control. If any unauthorized or illegal thing happened involving organization computer network or data processing unit, the computer security incident are identified.
- At the initial stage the incident may be reported by an end user, detected by a system administrator, recognized by intrusion detection system or discovered by means of much other method. In most groups, end users may additionally document an incident through certainly one of three ways :
  a. Their immediately supervisor,
  b. The company help desk.
  c. An incident hotline controlled by the Information Security entity.
- Normally technical issues are reported to the help desk by the end users. Issues related to the employee are reported to the Human Resource department.
- Prepare an initial response checklist to record the pertinent facts. This checklist list includes :
  - Current time and date of the incident
  - Who reported the incident
  - Nature of the incident
  - When the incident happened
  - What Hardware/software involved
  - Points of contact for involved personnel.
- This information is used by CSIRT from the initial response checklist to begin the next phase of the response process which is the initial response.

3. **Initial Response**

- Initial response is the first step of investigation. In this investigation step gather enough information to determine the proper response. The initial response phase consist of gathering the CSIRT, gathering network-based and other data, determining what type of incident that has occurred, and assessing the impact of the incident.
- The initial response phase document steps that must be taken. The individuals who are involved with detecting an incident actually begin the initial response phase. Whoever will detect or notify the incident this is their duty to document the details surrounding the incident.
- At the early stage in the process the control of the response should be forwarded to the CSIRT to take benefit the team's expertise; the more steps in the initial response phase performed by the CSIRT, the better. Initially initial response does not poke the affected system.
- The data collected during this phase consist of reviewing network-based and other evidence. This phase does the following tasks :
  - Interviewing system administrators.
  - Interviewing business unit personnel.
  - Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has happened.
  - The network topology reviewing and access control lists to determine if any ways of attack can be ruled out.
- The team must have to verify :
  - Incident has actually occurred,
  - which systems are directly or indirectly affected,
  - Which users are involved,
  - The potential business impact.

4. **Formulate a Response Strategy**

The goal of the response strategy formulation is to determine appropriate response strategy, given the circumstances of the incident. The strategy must have to take into account the political, technical, legal, and business factors that surround the incident. The final result depends on the objectives of the group or individual with responsibility for selecting the strategy.

Considering the Totality of the Circumstances

Circumstances of the computer security incident affect the response strategies. Some factors need while deciding the resources required for investigating an incident.

So the strategy must have to take into account whether to make a forensic duplication of pertinent systems, whether to make a criminal referral, whether to accompany civil litigation, and added aspects of your response strategy :

- How critical are the affected systems?
- How sensitive is the compromised or stolen information?
- Who are the abeyant perpetrators?
- Is the incident known to the public?
- What is the level of unauthorized access achieved by the attacker?
- What is the obvious skill of the attacker?
- How many system and user downtime is required?
- What is the overall dollar loss?

Considering Appropriate Responses

The response strategy has consideration the organization's business objectives. The prepared business strategy should be approved by upper-level management the response strategy options should be quantified with advantages and disadvantages related to the following :

- Estimated dollar loss.
- Network downtime and its impact to operations.
- User downtime and its impact to operations.
- Whether or not your organization is legally compelled to take certain actions.
- Public announcement of the incident and its effect on the organization's reputation / business.
- Theft of intellectual property and its potential economic impact.

Taking Action

Organizations have to take action to discipline an employee. The organization also has to respond to a malicious act done by an outsider.

Legal Action

There are two legal choices, one is to file a civil complaint or another is to notify law enforcement. Law enforcement involvement will results in reducing the autonomy that the organization has in dealing with an incident and cautious deliberation ought to arise earlier than you have interaction the precise government. The following standards have to be considered while identifying whether or not to include law enforcement in the incident response :

- Does the damage/cost of the incident merit a criminal referral?
- Is it likely that civil or criminal action will accomplish the outcome desired by your organization?

- Has the reason of the incident been reasonably established?
- Does your organization have proper documentation and an organized report that will be conducive to an effective investigation?
- Can tangible investigative leads be given to law enforcement officials for them to act on?
- Does your organization know and have a working relationship with local or federal law enforcement officers?
- Is your organization wishing to risk public exposure?
- Does the previous performance of the individual merit any legal action?
- How will law enforcement involvement impact business operations?

Administrative Action to

The administrative of an organization can discipline or terminate employees instead of initiating civil or criminal actions. Following are some administrative actions to discipline internal employees :

- Letter of scolding
- Immediate dismissal
- Mandatory leave of absence for a specific length of time
- Reassignment of job duties
- Temporary reduction in pay to account for losses/damage
- Public/private apology for actions conducted
- Withdrawal of certain privileges, such as network or web access.

5. **Investigate the Incident**

The investigation phase involves determining who, what, when, where, how, and why surrounding an incident. One can also conduct the investigation by, reviewing host-based evidence, network-based evidence, and evidence gathered traditionally.

Incident Action

At the point when there is a DoS attack Contact upstream suppliers to endeavour to recognize the possible wellspring of the DoS attack. On the off chance that the source is distinguished, consider informing law requirement to penetrate the obscurity of the attacker and/or end the activity. Your organization might likewise look for the assistance of the source.

ISP by asking for a break of "Terms of Service" of the ISP by the attacker. Outside attacker identify an IP address as the conceivable source and consider utilizing law requirement to puncture the secrecy behind the IP address. Ownership of tyke erotic entertainment your organization might be required to inform law implementation. Contact legitimate direction and Human Resources promptly.

Computer security investigation can be divided into two phases :

a. Data collection
b. Forensic analysis

a. Data Collection

Data collection is the gathering of facts and clues that are considered during forensic analysis. The data you gather forms the basis of your conclusions. Information gathering includes a few extraordinary forensic challenges :

- You should gather electronic information in a forensically stable way.
- You are frequently gathering more information than you can read in your lifetime
- You should handle the information you gather in a way that ensures its integrity.

The data you get amid the information accumulation stage can be partitioned into three key ranges : host-based data, system based data and other.

Host-based Information

Host-based evidence contains logs, records, documents, and any other information that you get on a system and not gathered from network-based nodes. Host-based information might be a system backup. Host-based data collection is done in two ways : *live data collection* and *forensic duplication.*

In few cases, the evidence that is required to understand an incident is temporary or lost when the victim/relevant system is powered down. Such type of volatile data can give critical information when attempt to understand the nature of an incident. The first step of data collection is the collection of any volatile information from a host before this information is lost. This volatile data gives a "snapshot "of a system at the time you respond. The following volatile information is recorded :

- Date and time of the system
- The applications currently running on the system
- Network connections which are currently.
- Sockets which are currently open
- The applications listening on the open sockets
- The state of the network interface

Live response is performed to collect this information. A live response is can be performed when a computer system is still powered on and running. It means you can collect the information contained in these areas without impacting the data on the compromised device.

There are three types of live response :

- **Initial live response :** Initial live response collect only the volatile data from a target or victim system. An initial live response is usually done when you have wanted to conduct a forensic duplication of the media.
- **In-depth response :** In this response the CSIRT gather enough additional information from the target/victim system to decide a valid response strategy. Even the Non volatile information is collected like log files d to help understand the nature of the incident.
- **Full live response :** It is a full investigation on a live system. For forensic duplication all data for the investigation is collected from the live system which requires the system to be powered off.
- **Network-based Evidence :** Network-based evidence contains information gathered from the following sources :
  - Intrusion Detection System logs
  - Consensual tracking logs
  - Non consensual wiretaps
  - Pen-register/trap and traces
  - Router logs
  - Firewall logs
  - Authentication servers

An organization frequently performs network surveillance acquire evidence, and perceive co-conspirators involved in an incident. It may be possible host-based auditing get fail; network surveillance may fill in the gaps.

Network surveillance permits an organization to accomplish a number of tasks :

- Confirm or dispel suspicions surrounding an alleged computer security incident.
- Gather additional evidence and information.
- Verify the scope of a compromise.
- Identify any other parties involved.
- Form a timeline of events happening on the network.
- Ensure compliance with a desired activity.

Other Evidence

It is the other information obtained from the people. Other evidences follow the traditional investigative techniques to collect the evidence. Other evidence you get when you collect personnel files, interview employees, interview witnesses, interview character witnesses, and document the information gathered.

b. Forensic Analysis

Forensic analysis reviews all the collected data. Forensic analysis review includes log files review, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files. When you perform software analysis, review time/date stamps, perform keyword searches, and take any other necessary investigative steps. Forensic analysis also examines the information which has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to the investigation.

6. Reporting

The most difficult phase in incident response process is reporting. The big challenge in reporting is to create reports that precisely describe the details of an incident. This reports should be understandable to decision makers, that can bear the wall of legal scrutiny, and that are produced in a timely manner.

The guidelines for reporting are :

(i) Document immediately

Document all investigative steps and conclusions which are necessary to document as early as possible It results in time saving and ensure that can be communicated more clearly to others at any time.

(ii) Write concisely and clearly

Write down everything in such a way that it is easy to understand to everyone. Try to avoid the shorthand or shortcuts.

(iii) Use a standard format

Build up a format for your reports and stick to it. Make forms, outlines, and layouts that sort out the response process and cultivate the recording of all relevant information. This makes report writing versatile, spares time, and advances exactness.

(iv) Use editors

Recruit technical editors to read the forensic reports. This helps to develop reports that are conceivable to nontechnical personnel who affect your incident response procedure and resolution.

7. Resolution

The objective of the resolution stage is to execute host-based, network-based, and procedural countermeasures to keep an incident from creating additional harm and to give back your organization to a protected, solid operational status.

The accompanying steps are frequently taken to determine a computer security incident :

- Identify your organization's top needs.
- Determine the way of the incident in enough detail to understand how the security occurred and what host-based and network-based remedies are required to address it.
- Determine if there are basic or systemic reasons for the incident that need to be addressed.
- Restore any affected or compromised systems.
- Apply corrections required to address any host-based vulnerabilities.
- Apply network-based countermeasures, for example access control lists, firewalls, or IDS.
- Assign responsibility for correcting any systemic issues.
- Track progress on all corrections that are required.
- Validate that all remedial steps or countermeasures are viable.
- Update your security policy and methods as needed to improve your response process.

Review Questions

Q. 1 What is digital forensics? Why there is need of digital forensics?

Q. 2 What are the objectives of digital forensics?

Q. 3 Explain the different types of digital forensics.

Q. 4 Explain the process of digital forensics.

Q. 5 What are the benefits of digital forensics?

Q. 6 Explain chain of custody.

Q. 7 Explain anti forensics.

Q. 8 What is digital evidence and its types?

Q. 9 What are the rules of digital evidences?

Q. 10 Explain incident response.

Q. 11 Explain the methodology of incident response.

Q. 12 Explain the roles of CSIRT in handling incident.

Q. 13 What is mean by Evidence? What are the types of evidence? Explain the characteristics of the evidence.

Q. 14 Explain the Incidence Response methodology or explain the components of Initial Response or explain the steps of initial response.

□□□

Computer Forensics

Syllabus

Introduction to Computer Forensics, Evidence collection (Disk, Memory, Registry, Logs etc), Evidence Acquisition, Analysis and Examination (Window, Linux, Email, Web, Malware), Challenges in Computer Forensics, Tools used in Computer Forensics.

Self Learning Topics : Open source tool for Data collection & analysis in windows or Unix.

Topics

3.1 Introduction to Computer Forensics

3.2 Evidence collection (Disk, Memory, Registry, Logs etc.)

3.3 Evidence Acquisition

3.4 Analysis and Examination (Window, Linux, Email, Web, Malware)

3.5 Challenges in Computer Forensics

3.6 Tools used in Computer Forensics

3.7 Self Learning Topics : Open-Source Tool for Data Collection & Analysis in Windows or Unix

3.1 Introduction to Computer Forensics

Computer Forensic

- Computer forensics is a scientific method of gathering evidence from digital devices, computer networks, and components that can be presented in a court of law or legal body.
- It entails conducting a structured investigation while maintaining a documented chain of evidence in order to determine exactly what happened on a computer and who was to blame.

Why is Computer Forensics Important ?

1. A few criminals are becoming smarter. So data-hiding techniques which includes ***encryption*** and ***steganography***. The evidence of criminal activity is placed in such a way where traditional search methods cannot able to find it.
   - **Encryption :** Scrambling data, for example an e-mail message, so that it cannot be readable to the interceptor.
   - **Steganography :** It is nothing but hiding a message into a larger file, typically in a photographic image or sound file.
2. Computer forensics is not just about "detective work" searching for and trying to find out information. Computer forensics is also worried with :
   - Sensitive data handling responsibly and confidentially.
   - Taking precautions to not nullify findings by corrupting data.
   - Taking precautions to make certain the integrity of the information.
   - Staying within the regulation and guidelines of evidence.

3.1.1 Advantages of Computer Forensics

- Produce evidence in court that can lead to the perpetrator's punishment.
- It assists businesses in gathering critical information about their computer systems or networks that may have been compromised.
- Tracks down cyber criminals from all over the world with ease.
- Aids in the safeguarding of the organization's funds and time.
- Allows you to extract, process, and interpret factual evidence in order to prove cybercrime in court.

3.1.2 Disadvantages of Computer Forensics

- It must be proven that the digital evidence has not been tampered with before it can be used in court.
- The cost of producing and storing electronic records is high.

- Legal professionals must have a strong understanding of computers.
- Evidence that is both authentic and convincing is required.
- If the tool used for digital forensics does not meet specified standards, the evidence may be disapproved by justice in a court of law.
- Due to a lack of technical knowledge on the part of the investigating officer, the desired outcome may not be achieved.

3.2 Evidence Collection (Disk, Memory, Registry, Logs etc.)

3.2.1 Disk

- Now a day's hard disk is a permanent storage media in a computer. Today we get maximum size hard disk. Hard drive contains from one to a few platters like flat, round disks. The platters are stacked one on top of another on a shaft that goes through an opening in the centre of every platter, similar to LPs on an old-fashioned record player.
- There is a motor connected to the spindle that rotates the platters, which are made of some inflexible material and are covered with a magnetic substance.
- Electromagnetic heads compose data onto the disks in the type of magnetic motivations and read the recorded data from them.
- Data can be written on the both the sides of each platter. On the tracks the information is written. The tracks are divided into *sectors*. A particular bit of data resides in an exact sector of an exact track on an exact platter.

Restored Image

- A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium. The restoration process is more complicated than it sounds.
- For example, one method involves a blind sector-to-sector copy of the duplicate file to the destination hard drive. If the destination hard drive is the same as the original hard drive, everything will work fine. The information in the partition table will match the geometry of the hard drive.
- Partition tables will be accurate; if the table says that partition 2 starts on cylinder 20, head 3, and sector 0 that is where the data actually resides. But what if the destination hard drive is not the same as the original hard drive? If you restore the forensic duplicate of a 2.1GB drive to a 20GB drive, then the geometries do not match.
- In fact, all of the data from the original drive may occupy only three cylinders of the 20GB destination drive. The partition that started on cylinder 20, head 3, and sector 0 on the original drive may actually start on cylinder 2, head 9, and sector 0.

- The software would look in the wrong location and give inaccurate results. How does the restoration software compensate for this? As the forensic duplicate is restored to the destination hard drive, the partition tables (in the master boot record and partition boot sectors) are updated with the new values. Is the restored image an exact duplicate of the original? If the analyst generates hashes of the restored image, will they match the original? The answer is no in both cases. Is the data on the restored image still a true and accurate representation of the original? For the purposes of analysis, yes.
- The method of updating the partition tables on the destination hard drive is not reliable. When hard drives grew beyond 512MB, the PC-BIOS manufacturers were scrambling to update their software to recognize such huge drives. Hard drive manufacturers came up with a way around the problem.
- Instead of forcing everyone to buy new motherboards with updated BIOS code, they released software that emulated modern BIOS. This software would "push" all of the real data on the drive down one sector and store its program and information in sector 1. The real partition table would be at cylinder 0, head 0, and sector 2.
- When the software restored the forensic duplicate to a large destination drive, it would not update the correct table, leaving the restored image relatively useless. Most forensic processing software will detect this drive overlay software and create a valid restored image.
- The following tools are used to create a restored image from the qualified forensic duplicate :
  1. SafeBack,
  2. EnCase,
  3. dd
- Depending on your method of analysis, EnCase and dd images may not need to be restored. EnCase, the Forensic Toolkit, treats the images as virtual disks, eliminating the need for restoration.

Mirror Image

- A mirror image is created from hardware that does a bit-by-bit copy from one hard drive to another. Hardware solutions are very fast, pushing the theoretical maximum data rate of the IDE or SCSI interfaces.
- Investigators do not make a mirror image very often, because it introduces an extra step in the forensic process, requiring the examiner to create a working copy in a forensically sound manner.
- If your organization has the ability to keep the original drive, seized from the computer system being investigated, you can easily make working copies. If the original drive must be returned (or never taken offsite), the analyst will still be required to create a working copy of the mirror image for analysis.

- The small amount of time saved onsite is overshadowed by the overhead of making a second working copy. We will not cover the process of creating a mirror image of evidence here. Most hardware duplicators are relatively simple to set up and operate.
- Two such duplicators are Log cube's Forensic SF-5000 and Intelligent Computer Solutions' Image MASSter Solo-2 Professional Plus. You do need to ensure that the hardware duplicator actually creates a true mirror image.
- Many duplicating machines on the market are made for systems integration companies who use them for installing operating systems on large numbers of hard drives. When used in this capacity, the hardware device will typically alter items in the boot and partition blocks to ensure that the partitions fall on cylinder boundaries.
- This alters the resulting image, which means that you do not walk offsite with an exact duplicate of the original. As with any process, test it thoroughly before you need to rely on it.

Creating a Forensic Duplicate of Hard Drive

To create the forensic duplicate of hard drive the following tools are used.

1. dd and dcfldd
2. ODD (open data duplicator)

1. Creating forensic duplicate using dd and dcfldd

- The dd tool is the part of the GNU software suite, afterwards dd was improved by the programmers and re-released as dcfldd. The dd tool is very reliable to create the true forensic duplicate.
- The dd tool performs a complete bit-by-bit copy of the original. While using the dd tool simply transposing a single character may destroy evidence, so one must have to be familiar with the dd tool before using it as well as with the Unix environment address storage devices.
- The steps require for duplicating hard drive using dd are :
  1. Create a boot media
  2. Perform the duplication with dd. In some situations, the duplication is stored in the series of the files which are sized to fit on a specific media type or file system type, we call this as segmented image. So do the following things to perform the duplication.
     - Write the script to perform hard drive duplication.
     - Write down the source device name.
     - Write down the output file name and set the output file size.
     - Use the dd command.
- It is also possible to create the duplicate without splitting the output file in Linux. To create such type of duplicate, calculate MD5 sum of the entire drive in one pass over the source hard drive.

2. Creating forensic duplicate with Open Data Duplicator (ODD)

- The Open Data Duplicator (ODD) is an open-source tool which follows the client server model. This client server model allows the investigator to perform forensic duplications on a number of computer systems simultaneously over a local LAN.
- We can use the software on a single forensic system because both halves can be run on the same computer system. ODD can perform additional functions on the data as it is being processed. ODD includes modules (plug-ins) that will calculate checksums and hashes, perform string searches, and extract files based on the file headers.
- The ODD package is having three portions :
  - **Bootable CD-ROMs :** These are similar to the Trinux Linux distribution.
  - **Server-side application :** The server will perform most of the processing of the duplicate image, including the calculation of hashes, string searches, and the storage of the true forensic duplication.
  - **Client-side application :** This portion may be run locally if you are duplicating drives on a forensic workstation.
- When we perform the forensic duplication of hard drive using ODD. Firstly, it detects the location of the ODD server. Then the ODD server detects the device and files which we can use to direct ODD for the duplication of some portions. After detecting the device, the next step is processing.
- The process stores the forensic image and performs simple string searches and extracts certain types of files based on their file headers. We also manage some notes using the Notes plug in which give the information like the case number, the computer's date and time, the actual date and time, and the system description.
- Then we use the Carv plug-in to extract a certain number of bytes from the incoming data stream, based on file headers. For example, we have selected gif and jpg for extraction, once the duplication has completed, the carved files may be found in a directory on the ODD server.

3.2.2 Memory

- The data stored in temporary memory on a computer while it is running is known as volatile data. Volatile data is lost almost instantly when a computer is turned off. Data such as browsing history, chat messages, and clipboard contents are examples of volatile data stored in a computer's short-term memory storage. If your computer lost power while you were working on a document in Word or Pages that you had not yet saved to your hard drive or another non-volatile memory source, you would lose all of your work.
- A memory dump (also called a core dump or system dump) is a snapshot of computer memory data taken at a specific point in time. A memory dump can contain important forensic information about the state of the system prior to an incident like a crash or a security breach.

- Memory dumps contain RAM data that can be used to determine the cause of an incident as well as other important details.
- Memory forensics is an important aspect of computer security investigation because it allows investigators to spot unauthorised and unusual activity on a target computer or server. This is usually accomplished by running special software that creates a snapshot file, also known as a memory dump, of the current state of the system's memory. The investigator can then take this file offsite and search it.
- This is useful because of the way processes, files, and programmes run in memory, and once a snapshot has been taken, the investigator can determine many important facts, such as :
  - Processes that are currently running
  - Executable files that are currently running
  - Open ports, IP addresses, and other networking data
  - Users who have logged into the system and from where they are accessing the system,
  - Files that are open and who is accessing them.
- We can already see how useful this information can be to investigators looking for system anomalies, and by capturing the volatile information stored in the system's memory, they can create a permanent record of the system's previous state.
- Memory forensics is a current snapshot of a system that provides investigators with a near-real-time image of the system while it is in use. Data recovery and decryption are usually the focus of hard drive forensics, which is usually done using an image of the drive-in question.
- Memory forensics can be thought of as a real-time response to a current threat, whereas hard drive forensics is more of a post-mortem of what has already happened. Memory forensics is time-sensitive because the required information is stored in volatile system memory, which is flushed from system memory when the system is restarted or powered off.
- Hard drives, on the other hand, are a type of computer storage that is not volatile. Hard drives contain some volatile components, such as cache and buffer stores, which must be considered by the forensic investigator.

Acquisition methods

- Forensic investigators are highly skilled and can spot activity on a system that should not be there, allowing them to prove that it has been hacked. It enables them to detect rootkits and malware, as well as find unusual processes and reveal covert communication, all of which can provide insight into what is going on in a target system at the time.
- The following are some examples of memory forensics acquisition formats. There are numerous types of memory acquisition, but the following are five of the most common methods and formats in use today :

- **RAW format :** Extracted from a live environment
- **Crash Dump** : Data gathered by the operating system after a crash.
- **Hibernation File** : A saved snapshot of your operating system that your operating system can return to after hibernating
- **Page File** : A page file is a file that stores information that is similar to that which is stored in your system RAM.
- **VMWare Snapshot** : A VMWare Snapshot is a snapshot of a virtual machine that saves its state as it was at the time the snapshot was taken.

Tools for memory data collection

On the market, there are both free and commercial products, and many forensics investigators will have their own preferences. Some investigators may only be able to use commercial products, but many professionals will use a combination of free and paid tools to complete their work. Some examples are as follows :

- **Volatility Suite :** It is an open-source suite of programmes for analysing RAM that works on Windows, Linux, and Mac computers. It can easily analyse RAW, Crash, VMWare and VirtualBox dumps.
- **Rekall** : This is an end-to-end solution that includes both acquisition and analysis tools for incident responders and investigators. It's better to think of it as a forensic framework suite rather than a single application.
- **Helix ISO :** This is a bootable live CD and a standalone application that makes capturing a memory dump or memory image of a system very simple.

  Running this directly on a target system carries some risks, namely an acquisition footprint, so make sure it meets your requirements.
- **Belkasoft RAM Capturer** : It is a forensic tool that allows you to capture the volatile section of your system memory to a file. The functionality and wide range of tools available in this software package will allow first responders to get started on their investigations as soon as possible.
- **Process Hacker :** This is an open-source process monitoring application that can be run on the target machine while it is in use. It will give the investigator a better idea of what is currently affecting the system before the memory snapshot is taken, and it will go a long way toward identifying any malicious processes or processes that have been terminated within a certain time frame. The following are some examples of memory forensics acquisition formats.

3.2.3 Registry

- The Windows Registry consists of information, settings, options, and other values for programs and hardware installed on all versions of MS Windows operating systems. For instance, when a program is installed, a new subkey containing settings like a program's location, its version, and how to start the program, are all put into the Windows Registry.

- When windows were at the start launched, it relied closely on .ini files to store windows and windows programs configurations and settings. Despite the fact that .ini files are still routinely used, most windows programs rely on settings made to the windows Registry after being installed.
- At the point when Microsoft made Windows 95, it combined instatement (.ini) files into the Registry, a database that stores hardware and software configuration data, user preferences, network connections, (counting usernames and passwords), and setup data. The Registry has been updated is still utilized as a part of Windows Vista.
- Windows Registry is containing valuable evidence for the investigative purposes.

  One can views the Registry.
- By using the Regedit (Registry Editor) program for Windows 9x.
- By using Regedt32 for Windows 2000, XP, and Vista.

Advantages of windows registry are :

- In the registry editor the can use the Edit, Find menu commands to locate the entries which might have the trace evidence like information identifying the last person who logged on to the computer, which is usually stored in user account information.
- Windows 9x systems don't record a user's logon information reliably, but you can find related user information, such as network logon data, by searching for all occurrences of "username" or application licenses.
- You can also use the Registry to determine the most recently accessed files and peripheral devices. In addition, all installed programs store information in the Registry, such as Web sites accessed, recent files, and even chat rooms accessed.

As a computing investigator, you should explore the Registry of all Windows systems. On a live system, be careful not to alter any Registry setting to avoid corrupting the system and possibly making it unbootable.

Windows Registry Organization

Before focusing on the registry first of all we will understand some Windows registry terminologies.

Table 3.2.1

Terminology	Description
Registry	A collection of files containing system and user information.
Registry Editor	A Windows utility for viewing and modifying data in the Registry. There are two Registry Editors : Regedit and Regedt32.
HKEY	Windows splits the Registry into categories with the prefix HKEY_Windows 9x systems have six HKEY categories and Windows 2000 and later have Five. Windows programmers refer to the "H" as the handle for the key.

Terminology	Description
Key	Each HKEY contains folders referred to as keys. Keys can contain other key folders or values.
Subkey	A key displayed under another key is a subkey, similar to a subfolder in Windows Explorer.
Branch	A key and its contents, including subkeys, make up a branch in the Registry.
Value	A name and value in a key; it's similar to a file and its data content.
Default value	All keys have a default value that may or may not contain data.
Hives	Hives are specific branches in HKEY_USER and HKEY_LOCAL_MACHINE. Hive branches in HKEY_LOCAL_MACHINE\Software are SAM, Security, Components, and System. For HKEY_USER, each user account has its own hive link to Ntuser.dat.

- It is important to understand that where data files that the Registry reads are located. The Table 3.2.2 shows the windows version and the files used :

Table 3.2.2

Sr. No.	Version	Files
1	Windows 9x/Me	2
2	Windows NT, 2000, XP, and Vista	6

- When the number of records the Registry utilizes relies on upon the Windows version. In Windows 9x/Me, it utilizes just two files; in Windows NT, 2000, XP, and Vista, it utilizes six files. While looking at Registry information from a suspect drive, you have to know where these records are found with the goal that you can extract them and investigate their content. You can discover these documents with tools, for example, Access Data Registry Viewer.
- Table 3.2.3 shows how Registry data files are organized and explains these files' purposes in different versions of Windows.

Table 3.2.3

Windows 9x/Me	
Filename and location	**Purpose of file**
Windows\System.dat	User-protected storage area; consist of installed program settings, usernames and passwords associated with installed programs and system settings.
Windows\User.dat Windows\profile\User Account	Consist of the Most Recently Used (MRU) files list and desktop configuration settings; every user account created on the system has its own user data file.

Table 3.2.4

Windows NT, 2000, XP, and Vista	
Filename and location	**Purpose of file**
Documents and Settings\user-account\Ntuser.dat (in Vista, Users\UserAccount\Ntuser.dat)	User-protected storage area; contains the MRU files list and desktop configuration settings.
Winnt\system32\config\Default	Consist of the computer's system settings.
Winnt\system32\config\SAM	Consist of user account management and security settings.
Winnt\system32\config\Security	Consist of the computer's security settings.
Winnt\system32\config\Software	Consist of installed programs settings and associated usernames and passwords.
Winnt\system32\config\System	Consist of additional computer system setting.

Viewing Windows registry

To view and make changes to the Windows Registry, type regedit or regedt32 at command line you will get the Windows Registry Editor (shown in the Fig. 3.2.1). This Editor allows you to view all keys and values that are in the Registry as well as change Windows, program, or driver values you feel are necessary.

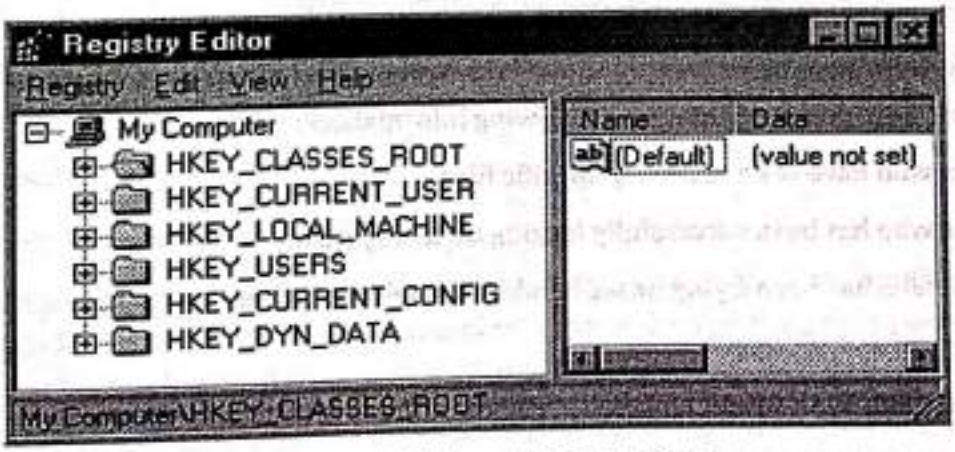


Fig. 3.2.1 : Windows Registry Editor

When we open the Windows Registry Editor first time, it displays root keys that contain all Registry values. The description of the root keys is given in the Table 3.2.5.

Table 3.2.5

Root Key	Description
HKEY_CLASSES_ROOT (HKCR)	It describes file type, file extension, and Object Linking and Embedding (OLE) information.
HKEY_CURRENT_USER (HKCU)	This key contains the information of currently logged users into Windows and their settings.
HKEY_LOCAL_MACHINE (HKLM)	This key Contains computer-specific information about the hardware installed, software settings, and other information. This information is used for all users who log on to this computer and is one of the more commonly accessed areas in the Registry.
HKEY_USERS (HKU)	This key contains information about all the users who log on to the computer, including both generic and user-specific information.
HKEY_CURRENT_CONFIG (HKCC)	This key contains the details about the current configuration of hardware attached to the Computer.
HKEY_DYN_DATA (HKDD)	This key is only used in Windows 95, 98, and NT this key contained the dynamic status information and Plug-and-Play information. This information may change as devices are added to or removed from the computer. The information for each device includes the related hardware key and the device's current status, including problems.

3.2.4 Logs

- In windows system maintain three log files : the System log, Application log, and Security log. By reviewing these logs, you may obtain the following information :
  1. Determine who have been accessing specific files.
  2. Determine who has been successfully logging on to a system.
  3. Determine who has been trying unsuccessfully to log on to a system.
  4. Track usage of specific applications.
  5. Track alterations to the audit policy.
  6. Track changes to user permissions.
- **System log** contains the recorded System processes and device driver activities. System events audited by Windows contain device drivers that fail to start properly; hardware failures; duplicate IP addresses; and the starting, pausing, and stopping of services.

- **Application log** include activities related to user programs and commercial off-the-shelf applications Application events that are audited by Windows include any errors or information that an application wants to report. The Application log can include the number of failed logons, amount of disk usage, and other important metrics.
- System log include system auditing and the security processes used by Windows. Security events that are audited by Windows include changes in user privileges, changes in the audit policy, file and directory access, printer activity, and system logons and logoffs.
- Any user can view the Application and System logs, but only administrators can read the Security log. The Security log is usually the most useful log during incident response. An investigator must be comfortable with viewing and filtering the output to these logs to recognize the evidence that they contain.
- Additionally, many third-party applications and Windows system utilities create log files specific to their corresponding applications.

Logs on a Live System

Windows provides a utility called Event Viewer to access the audit logs on a local host.

Event Log Dumps

Obtain the event logs from the victim system and also perform an offline review across a TCP/IP network during the initial response to an incident. Use PsLogList or dumpel.exe/elogdmp.exe to dump the logs. After dumping the log use the file-transfer tool (netcat or cryptcat) to send them across the network.

Investigation of Logs Offline

It is necessary to obtain copies of the secevent.evt, appevent.evt, and sysevent.evt files from the forensic duplicate. It helps to view the event logs from an offline system. Once you recover all the three .evt files then you can view the log files on your forensic workstation.

Event Log Drawbacks

The drawback of event logs is as follows :

1. Windows system's default security event log settings is log nothing at all. So the Windows systems do not log successful logons, shutdowns, files accesses, and many other important events. Because of this default setting, it has become a challenge for investigation.
2. Windows logging event Viewer permits you to view only a single record at a time which is time-consuming and difficult.
3. The event logs only record the source NetBIOS name, rather than the IP address of the remote system. This helps in making identification of remote connections to Windows systems impossible using only event logs.

4. In Windows default setting each log files maximum size is 512 KB and a time length of seven days. After reaching the limit of fixed size, the log file is closed, and is cleared before you are able to begin logging to that log file again.
5. The disadvantage of reviewing system logs offline is that the logs populate the description field by utilizing values from various Dynamically Linked Library (DLL) files. This should not affect offline review of the Security log. The messages are standard, but the Application log may contain entries that do not have the proper description text messages that correspond to the event ID an application generated.

IIS Logs

- It is necessary to review the log files for each IIS service, especially the web server. These logs are ordinarily located in Log Files directory, in the corresponding subdirectories of each service.
- For IIS, the default log file name is based on the current date, in the format ex*yymmdd*.log. A new log file is generated each day. You can activate and configure IIS logging through the Web Site Properties settings of the IIS Manager.
- The default log file stores the time, client IP address, method, URI stem, and HTTP status (a numerical status code). IIS logging is enabled by default, so these log files probably will be present.
- Most of the log fields are self-explanatory, but the HTTP Status field requires some explanation. In general, any code in the 200 to 299 range indicates success. The common 200 code indicates that the client request was fulfilled. Codes in the 300 to 399 range indicate actions that need to be taken by the client to fulfil a request. This usually means an automatic redirection, such as when a web site's content moves to another location.
- Codes in the 400 to 499 and 500 to 599 ranges indicate client and server errors, respectively. Among the two most common 400 series codes are the 404 code, indicating that the requested resource is not found on the server, and the 403 code, indicating that retrieving the requested resource is forbidden.

3.3 Evidence Acquisition

- Once exhibits have been seized an accurate sector level duplicate (or "forensic duplicate") of the media is created, usually via a write blocking device, a process referred to as Imaging or Acquisition. Obtaining Volatile Data Prior to Forensic Duplication.
- Data which is in a state of change is called volatile data. The data in the computer system will get lost as the power loss. Volatile data is present in the active physical memory. We will find the volatile data in physical memory, registers, virtual memory in the file system, and in the peripheral device memory.
- To ensure all relevant data are collected, you should prepare an order of volatility while gathering evidence, the Order of Volatility (OoV) should be from the most volatile to the least.
- When you acquire volatile data, you'll want to respond to the target device at the console, in preference to getting access to it over the network. This eliminates the possibility of the attacker monitoring your response and ensures that you are running trusted commands.

- If you are certain that you may be doing a forensic duplication of the target device, you have to focus on obtaining the volatile system data before powering down the system. The risky information consists of presently open sockets, strolling approaches, the contents of system RAM, and the location of unlinked documents.
- The unlinked files are documents marked for deletion while processes that get entry to it to terminate. The documents marked for deletion will "disappear" while the system is powered down. Therefore, the preliminary reactions have to get better, each type of unstable proof inclusive of the documents marked for deletion! This could save you some grief because getting a deleted report in maximum flavours of UNIX isn't as simple as running a report undeletion device or tool.

Collecting the Data

1. Date and time of the system.
2. Currently logged on the user's list.
3. Entire file systems time and date stamp.
4. Currently running processes list.
5. Currently, open sockets list.
6. The applications listening on open sockets.
7. A list of the systems that have current or had recent connections to the system.

The following steps are taken to collect the live data :

1. Execute a trusted shell.
2. Record the system time and date.
3. Determine who is logged on to the system.
4. Record modification, creation, and access times of all files.
5. Determine open ports.
6. List applications associated with open ports.
7. Determine the running processes.
8. List current and recent connections.
9. Record the system time.
10. Record the steps taken.
11. Record cryptographic checksums.

Remember that the steps we outline are just a game plan. You need to modify the order and the tools used based on the whole of the circumstances. You may choose to include tools we do not mention, as well as carry out your steps in a different manner :

1. Executing a Trusted Shell

- When you are responding to a targeted system on which UNIX operating system is running, you will come across one of two scenarios :
  1. The system runs in console mode.
  2. The system runs X Windows, a GUI like to the Windows desktop.
- Exit the X windows prior to you begin your response; it helps to avoid common X Windows-based vulnerabilities that permit the attacker to log keystrokes. If you are responding to a Linux system, you possibly able to switch to another virtual console by pressing ALT-F2.
- To avoid generating traffic Log on locally at the victim console with root-level privileges. Now mount the trusted toolkit and respond with trusted tools. The following is the command syntax to mount a floppy drive when responding to a Linux system :

```
mount /dev/fd0 /mnt/floppy
```

- This command mounts your trusted toolkit on the mount point /mnt/floppy. To access the trusted file change the directory to /mnt/floppy.
- The first step in all response is to be certain you are executing a trusted command shell.
- The Unix shells can be trojaned by attackers to log all the commands executed or to perform immoral and evil operations invisible to the investigator.
- Therefore, you will want to execute your own trusted shell. Once you have executed your trusted shell, set your PATH environment variable equal to dot (.).
- This will decrease the chances of someone accidentally executing untrusted commands that are in the target system's PATH.

2. Recording the System Time and Date

- The local date and time settings are important for later correlation of time/date stamps, and they also show when you were on the system.
- To capture this information, use the date command :

```
[root@conan /root]# date
Tue Dec 17 16:12:43 UTC 2003
```

3. Determining Who Is Logged on to the System

- The (what) command determines who is logged on. It displays the logged on user IDs, and from which system they have logged on.
- It also shows what they are currently executing on the system with the date and system time.

4. Recording File Modification, Access, and Inode Change Times

- You may need to retrieve all of the time/date stamps at the file device. As with home windows structures, Unix structures have 3 time/date stamps to collect for every file and listing : get right of entry to time (atime), amendment or modification time (mtime), and the inode alternate time (ctime). An inode is a data structure in Unix which is used to represent file system objects.

- You can use a depended on ls command with the proper command-line arguments to obtain those times for every file. The subsequent strains show the way to obtain the time/date stamps and show the output on a trusted floppy disk :

```
ls -alRu / > /floppy/atime
ls -alRc / > /floppy/ctime
ls -alR / > /floppy/mtime
```

5. Determining which Ports are Open

- The netstat command is used to determine the open ports. By using *netstat – a* command is used to view all open ports.
- The *-n* option tells netstat to not resolve hostnames, which reduces the impact on the system and speeds the execution of the command.

6. Listing Applications Associated with Open Ports

With the netstat command *–p* option is used which maps the name of the application and its Process ID (PID) to the open ports.

7. Determining the Running Processes

- Taking a snapshot of all the running processes during the initial response is critical. This can be done by using the standard ps (process status) command.
- The output varies a bit among the different UNIX flavors.
  1. Use ps -eaf on Solaris systems,
  2. Use ps -aux on FreeBSD and Linux systems.

8. Listing Current and Recent Connections

- The netstat command provides information about another aspect of live response: current and recent connections.
- The command usage is identical for determining which ports are open.

9. Recording System Time

- Use the date command again (repeat step 2) to record the current system time. The reason for another timestamp is so that you will know the exact time window during which you manipulated the system.
- Thus, any changes that take place outside this time window are not due to your investigation.

10. Recording the Steps Taken

- Finally, record all of the commands you have issued to the system. There are several possibilities here: use script, history, or even vi if you performed your live response from the editor.

- Since you issued all commands from a trusted shell, using the history command will record all of the commands you have executed. However, a better choice is the script command, which will record your keystrokes and the output. If you choose to use the script command, you'll need to run this command before you perform the live response.

11. Recording Cryptographic Checksums

- Finally, record the cryptographic checksums of all recorded data.
- Simply run the md5sum program against all files in the data directory, as shown here :

```
[root@conan /root]# md5sum * > md5sums.txt
```

12. Scripting the Initial Response

- Write a simple shell script to automate the live data collection.
- Steps of a UNIX system are same as windows system. Place your script in the same directory as the response toolkit and it calls the local tools.

3.4 Analysis and Examination (Window, Linux, Email, Web, Malware)

3.4.1 Investigating Live Systems Windows

- This section will explore the various ways to investigate windows systems. This is assumed that you have done the initial response and confirmed for further investigation is required; you have consulted with legal counsel and done the forensic duplication of the evidence drive.
- It is very important to know that where the evidence resides on windows system, so generally evidence can be found in the following areas :
  1. Volatile data present in kernel structures
  2. Slack space
  3. Free or unallocated space
  4. The logical file system
  5. The event logs
  6. The Registry, which contains an enormous log file
  7. Application logs not managed by the Windows Event Log Service
  8. The swap files
  9. Random Access Memory
  10. Special application-level files, for example Internet Explorer's Internet history files (index.dat), Netscape's fat.db, the history.hst file, and the browser cache.

11. Temporary files created by many applications
12. The Recycle Bin
13. The printer spools
14. Sent or received email, like the .pst files for Outlook mail.

Steps for Conducting a Windows Investigation

- The steps for conducting the windows investigation are as follows :
  1. Review all relevant/ pertinent logs.
  2. Perform keyword searches.
  3. Review relevant files.
  4. Identify unauthorized user accounts or groups.
  5. Identify rogue processes and services.
  6. Look for unusual or hidden files/directories.
  7. Check for unauthorized access points.
  8. Examine jobs run by the Scheduler service.
  9. Analyze trust relationships.
  10. Review security identifiers.
- These steps are not ordered chronologically or in order of importance. You may need to perform each of these steps or just a few of them. Your approach depends on your response plan and the circumstances of the incident.

1. Reviewing All Pertinent Logs

- In windows system maintain three log files : the System log, Application log, and Security log. By reviewing these logs, you may obtain the following information :
  1. Determine who have been accessing specific files.
  2. Determine who has been successfully logging on to a system.
  3. Determine who has been trying unsuccessfully to log on to a system.
  4. Track usage of specific applications.
  5. Track alterations to the audit policy.
  6. Track changes to user permissions.
- **System log** contains the recorded System processes and device driver activities. System events audited by Windows contain device drivers that fail to start properly; hardware failures; duplicate IP addresses; and the starting, pausing, and stopping of services.

- **Application log** include activities related to user programs and commercial off-the-shelf applications Application events that are audited by Windows include any errors or information that an application wants to report. The Application log can include the number of failed logons, amount of disk usage, and other important metrics.
- System log include system auditing and the security processes used by Windows. Security events that are audited by Windows include changes in user privileges, changes in the audit policy, file and directory access, printer activity, and system logons and logoffs.
- Any user can view the Application and System logs, but only administrators can read the Security log. The Security log is usually the most useful log during incident response. An investigator must be comfortable with viewing and filtering the output to these logs to recognize the evidence that they contain.
- Additionally, many third-party applications and Windows system utilities create log files specific to their corresponding applications.

Logs on a Live System

Windows provides a utility called Event Viewer to access the audit logs on a local host.

Event Log Dumps

Obtain the event logs from the victim system and also perform an offline review across a TCP/IP network during the initial response to an incident. Use PsLogList or dumpel.exe/elogdmp.exe to dump the logs. After dumping the log use the file-transfer tool (netcat or cryptcat) to send them across the network.

Investigation of Logs Offline

It is necessary to obtain copies of the secevent.evt, appevent.evt, and sysevent.evt files from the forensic duplicate. It helps to view the event logs from an offline system. Once you recover all the three .evt files then you can view the log files on your forensic workstation.

Event Log Drawbacks

The drawback of event logs is as follows :

1. Windows system's default security event log settings is log nothing at all. So the Windows systems do not log successful logons, shutdowns, files accesses, and many other important events. Because of this default setting, it has become a challenge for investigation.
2. Windows logging event Viewer permits you to view only a single record at a time which is time-consuming and difficult.
3. The event logs only record the source NetBIOS name, rather than the IP address of the remote system. This helps in making identification of remote connections to Windows systems impossible using only event logs.

4. In Windows default setting each log files maximum size is 512 KB and a time length of seven days. After reaching the limit of fixed size, the log file is closed, and is cleared before you are able to begin logging to that log file again.
5. The disadvantage of reviewing system logs offline is that the logs populate the description field by utilizing values from various Dynamically Linked Library (DLL) files. This should not affect offline review of the Security log. The messages are standard, but the Application log may contain entries that do not have the proper description text messages that correspond to the event ID an application generated.

IIS Logs

- It is necessary to review the log files for each IIS service, especially the web server. These logs are ordinarily located in Log Files directory, in the corresponding subdirectories of each service.
- For IIS, the default log filename is based on the current date, in the format ex*yymmdd*.log. A new log file is generated each day. You can activate and configure IIS logging through the Web Site Properties settings of the IIS Manager.
- The default log file stores the time, client IP address, method, URI stem, and HTTP status (a numerical status code). IIS logging is enabled by default, so these log files probably will be present.
- Most of the log fields are self-explanatory, but the HTTP Status field requires some explanation. In general, any code in the 200 to 299 range indicates success. The common 200 code indicates that the client request was fulfilled. Codes in the 300 to 399 range indicate actions that need to be taken by the client to fulfil a request. This usually means an automatic redirection, such as when a web site's content moves to another location.
- Codes in the 400 to 499 and 500 to 599 ranges indicate client and server errors, respectively. Among the two most common 400 series codes are the 404 code, indicating that the requested resource is not found on the server, and the 403 code, indicating that retrieving the requested resource is forbidden.

2. Performing Keyword Searches

- Performing the string searches of the subject's hard drive is necessary while doing the investigation. It may be possible that many keywords are dangerous or risky involving user IDs, passwords, code words, known filenames, and subject-specific words (for example, *Seeta, Mohan*). To examine the contents of an entire drive string searches can be performed on the logical file structure or at the physical level.
- Most disk-search tools or forensic software do raw reads from the hard drive and conducts a physical-level string search of the drive. Such tools requires the booting of the target system from a controlled boot floppy or other media and run the tool, because you cannot physically read a drive that is running a Windows operating system.

- Frequently used disk-search utilities include :
  1. The *dtSearch* tool is offered by dtSearch Corp. It performs the search from a physical level.
  2. EnCase perform a string-search that can be run against the evidence image file. This makes keyword searching is an art.

3. Reviewing Relevant Files

- Windows systems write input and output to most files at a time that almost all actions taken on the system leave some trace of their occurrence. Windows has temporary files, cache files, and a registry which keeps track of recently used files, a Recycle Bin that keeps the deleted files, and countless other locations where runtime data is stored. It is important to recognize files by their extensions and true file headers.
- We at least must have to know what .doc, .tmp, .log, .txt, .wpd, .gif, .exe, and .jpg files are. EnCase cannot view all the files, so you need a comprehensive file viewer, such as Quickview Plus. Quickview and similar file viewers ignore the file extensions, thus the name of a file does not "trick" the application.
- **Incident Time and Time/Date Stamps :** Timeframe is used to find which files might be relevant to the current incident. Then inspect closely those files created, modified or accessed during this timeframe. The files "touched" during the relevant timeframe provide the information required to determine which files were stolen, executed, removed, or uploaded to a system. You will need :
  1. To scour network-based logs.
  2. Use oral testimony.
  3. "Action days" days when relevant activities took place.
- To recognize interval when an incident must have happened. After getting the timeframe review the time/date stamps encapsulated within those timeframes. The files that were changed, created, or changed during the time that the doubtful event took place can be considered pertinent files. To get a directory listing which includes file access, modification, and creation times the dir command is used. NTI'S file listing tool *FileList* can checksum all the files on the system. It lists all the directories and files, along with their last access time, modified time, and creation time.
- **Proprietary Email Files :** To determine the suspicious Email send by attacker review the send and receive time/date stamp. The most common email clients Outlook, Netscape Messenger and AOL each have its own proprietary format. When reviewing the email sent or received by a suspect, you must use the appropriate client software to view the suspect's email.
- **Deleted Files and Data :** There are various occasions when incident response needs the recovery of lost files which is that might have been deleted by malicious users to cause harm or simply erased by those who are willing to cover up their misdeeds. There are four ways to recover deleted data :

1. Use the undelete tools.
2. Restoring files located in the Recycle Bin.
3. Recovering temporary files.
4. Use the low-level tools to repair the file system.

(i) Undelete Tools

One tool that performs undeletion on the NTFS file system is File Scavenger. File Scavenger can undelete files as long as the space they occupy on the hard drive has not been used by more recent I/O storage. File Scavenger may work even after the disk has been reformatted. Realize that some utilities can be set to prevent the deletion of files.

(ii) The Recycle Bin

- The Recycle Bin is a feature that prevents accidental deletion of files. Think of it as a file limbo, where files will reside until the user decides to empty the Recycle Bin. The Recycle Bin captures only files deleted from Windows Explorer and other Recycle Bin aware applications (such as Microsoft Office applications).
- The Recycle Bin process creates a directory that is different for every user. The directory is created the first time a user deletes a file. To restore files from the Recycle Bin, you must first find the hidden Recycle Bin directories. You can find the contents of the Recycle Bin by going to the root directory of a partition (drive letter) and then changing directories into the hidden RECYCLER directory.

(iii) Temporary Files

- Numerous applications, for example, web programs, email customers, and different sorts of end-client programs make temporary files to work appropriately. Impermanent record won't get erased after the application close or ended.
- For instance, in the event that you have as of late gotten email messages with extensive connections, it is conceivable that almost all the attached files are put away as impermanent documents.
- A survey of all records with a temporary filename extension might uncover year-old documents that were deleted, old PowerPoint presentations, and documents that were gotten as attachments.

(iv) Backup File Recovery

- Likely the most awkward yet most reliable approach to recover lost information is to locate the most current backup of the system and after that endeavor to find the significant records. The confirmation that is lost from the system you are investigating can regularly be found on one of the backup tapes.

- Windows system transfer with intense backup devices. For instance, Windows NT'S NTBACKUP.EXE is a GUI tool that makes a log document recording the date of the backup, what number of documents were moved down, what number of documents were skipped amid the re backup process, what number of mistakes were recorded, and to what extent the backup took to wrap up.
- To figure out if a backup was as of late made of the restored picture, hunt down BACKUP.LOG, or just *.log, and figure out if it was made by NTBACKUP. Likewise, never falter to get some information about the presence of any system backups.

The Windows Registry

- The Windows Registry is a gathering of data files that stores very important configuration data for the system. The operating system uses the Registry to accumulate data about the hardware, software and components of a system.
- The registry has lot of data which is useful to investigators. The Registry can reveal the software installed in the past, the security configuration of the machine, DLL Trojans and start-up programs, and the Most Recently Used (MRU) files for many different applications.

The Swap File

- The swap file is a hidden system document that is utilized for virtual memory. At the point when the system turns out to be excessively occupied for the measure of memory in a system, the swap file is utilized to work temporarily as RAM. The operating system will swap out the lesser-utilized segments of RAM to free space for more dynamic applications.
- The swap file is usually about double the measure of RAM on a system. The bits of memory swapped to the hard drive's swap file are called pages. The swap file might contain pieces of content from document, passwords, and different goodies of data that a client as of late saw or wrote on his system. The key is that the client may not understand that the information arrives.

Broken Links

- Another vital step is to check for broken connections on the system. Checking connections can likewise offer you some assistance with determining what software had been on a system. Connections are utilized to relate a desktop alternate route or a Start menu item with an application or a record.
- Actually, removing applications or documents does not remove the connections that were made for them. Clients might delete documents however forget to delete the desktop symbol on the system. The NTRK tool's chklnks.exe is fabulous for uncovering files that were once introduced however mysteriously gone.

Web Browser Files

- Employees need access to the Internet at work, however numerous organizations don't need their employees spending the larger part of their work hours shopping, surfing, exchanging stocks, talking, or downloading obscenity on organization systems. These exercises require the utilization of web programs.

- Web programs, for example, Netscape and Internet Explorer keep up log records. Both programs record browser history and track sites that were as of late gone to. They additionally keep up a cache that contains a specific measure of the genuine documents and site pages as of late saw. To view the activities Netscape uses fat.db file which maintains history. Internet explores index.dat file holds viewer history and in dialup networking reviews the dialup setting.

4. Identifying Unauthorized User Accounts or Groups

The wrong doers can create fake accounts on the system or get the hold on unauthorized privileges to access the data. To find out such user accounts and groups there are following ways :

- Look in the User Manager for unauthorized client accounts.
- Use *usrstat* from the NTRK to view all domain accounts on a domain controller, searching for suspicious entries.
- Examine the Security log utilizing Event Viewer, filtering for event ID 624 (expansion of another record), 626 (client account empowered), 636 (changing a record bunch), and 642 (client account changed).
- Check the system root directory for the profiles of the user. On the off chance that the client account exists, however there is no comparing user account registry, that client account has not been utilized to log into the system yet. If that directory does exist, but the user account is no more listed in the User Manager or Registry, that user ID did exist at one time but no more exists.
- Review the SIDs in the Registry, When a user account is deleted, the relating Profile directory entry is not deleted, and the corresponding SID will stay in the Registry, This permits you to follow which user IDs have been deleted over the course of a system's life.

5. Identifying Rogue Processes

Rogue processes listen for network connection for clear text client IDs and secret key. Finding these processes are easy when they are executing.

A few tools get data about running processes :

- **PsList** lists the name of the running process.
- ListDLLs gives the full command-line arguments for every running process.
- Fport shows which processes are listening on which ports.

Important question is how can you find rogue processes that are on a cold system? The easiest solution is to run the most up-to-date virus scanner on the whole logical volume of evidence. An excellent tool that identifies Trojans, backdoors, keystroke loggers, and other "malware" is Pest Patrol.

6. Looking for Unusual or Hidden Files

- When the attacker got the access to the system, he/she need to hide the file for later use. The attacker can also make the few files invisible by taking the advantage of NTFS file stream.legitimate files.

- NTFS is developed on various levelled document system, it has a feature of putting away different instances of record under one passage. These different information streams might be utilized to shroud information, since Windows Explorer does not indicate the presence of the additional streams.
- Other regularly utilized techniques to stow away documents inside of the logical record system incorporate changing the document augmentation or imaginatively naming the records to match those of critical system records. Neither of these techniques ought to divert from an accomplished analyst, however they can trick some mainstream mechanized measurable tools.

7. Checking for Unauthorized Access Points

- Any service that permits some level of remote access could give a section point to undesirable intruders. Notwithstanding implicit and third-party applications, Trojans might give such services. These services incorporate the accompanying :
  - SQL/Oracle
  - Windows 2000 Telnet Server
  - Terminal server
  - Remote-access services (PPP and PPTP)
  - Third-party telnet daemons on Windows NT
  - Third-party FTP daemons
  - Web servers (such as Apache and IIS)
  - Virtual network computing (TCP port 5800) and PC Anywhere (TCP port 5631)
  - X Servers
- At the point when reacting to victim systems, you should recognize the access point focuses to the system to decide how access was obtained.
- Tools used to recognize access points are :
  1. netstat
  2. Fport
- They utilize API calls to peruse the contents of kernel and client space TCP and UDP connection cables. In the event that you expect to catch this data, you should permit the restored picture or image to boot. In the event that you performed this step amid the live system audit, before the system was closed down for imaging, think about the after effects of the two operations. Errors might be indicative of an unauthorized daemon.

Remote Control and Remote Access Services

- Dial-in utilities are the common remote-access points into a Windows system. The examples of dial-in utilities are Window's native Remote Access Service (RAS), PC Anywhere, and similar utilities that allow dial-in or network-based command-level access.

- Windows systems remote access is divided into two classes :
  1. Those that permit remote control
  2. Those that permit remote access.
- The distinction between these two classes is the amount of network traffic and performance speeds. The remote client can take the control over system by utilizing these utilities. To identify remote-control software on the system, use netstat, Fport and PsList to locate the open ports. You can likewise examine the file system to figure out if the remote-control software has been introduced. Remote-control applications permit just a solitary remote client to control the system at once. Consequently, assailants like to connect with a service that permits remote access, instead of remote control.

Administrative Shares

- It is possible to share any file or folder that is accessible over a network through Windows networking. If any user has decided not to share a folder, it means it is not creating an access point for attackers. Windows systems have *administrative shares*, which are automatically offered to remote users after each boot process.
- These administrative shares are hidden shares, they all have the $ character appended to their names. Windows RAS enables multiple remote users connect simultaneously to the system through a modem connection. RAS is a favourite access point for the ex-employee who wants to maintain access to his previous employer's network. RAS is the only remote-command-level access that comes standard with Windows NT Server systems. The tool *rasusers* list all the user accounts that have the privilege to log in to the RAS server.

Patch Levels

- Service packs are collections of patches, new applications, improvements, and settings that are designed to improve the original release. Windows system is frequently having security problems with service *packs*.
- Service packs repair different vulnerabilities and security holes. Service packs correct a number of issues all at once. Service packs are supported by Microsoft and are fully tested. *Hot fixes* are issued as quick fixes, and they are quite frequently released within days of a publicly addressed problem.
- Hot fixes are released by Microsoft but not supported by Microsoft. If you are aware about the patch level present on a system then you can eliminate any chances of certain attacks being effective on that system. You can reconstruct events and create sound hypotheses to describe an incident by doing the process of elimination.

8. Examining Jobs Run by the Scheduler Service

A typical ploy by attackers is to have a scheduled event start backdoor programs for them, change the audit policy, or perhaps even something more alarming for example a scheduled wiping of files. The *at* and *soon* utilities are used to schedule the malicious jobs. The *at* command, with no command-line arguments shows any jobs that have been scheduled.

Analyzing Trust Relationships

- Trust relationships among domains can positively expand the extent of a compromise ought to a compromise ID and secret word be stolen by an assailant. Shockingly, deciding trust inside of a Windows domain is not as basic as it is in the UNIX environment. Windows NT bolsters nontransitive, or one-way, trust. This implies access and services are given in one direction only.
- In the event that your NT PDC trusts another domain, it doesn't have to trust your PDC. Thusly, clients on the trusted area can utilize services on your space, yet not the other way around. Windows 2000 can give a two-way, or transitive, trust relationship.
- Areas situated inside of an Active Directory woods require two-route trusts to convey legitimately. For instance, in Windows 2000 Active Directory Services, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C.

9. Reviewing Security Identifiers (SIDs)

- Security Identifiers are utilized to recognize a client or a group. Every system and client has their own particular identifier which builds up the actions of a particular client ID, you might need to compare SIDs found on the victim machine with those at the central authentication authority.
- The computer identifier and the client identifier are combined to make the SID. In this way, SIDs can extraordinarily distinguish client accounts. SIDs doesn't have any significant access to share security. Access to shares is refined to usernames and passwords. Be that as it may, SIDs does have any significant access when remote access to a space is given.
- A SID with the server's unique sequence of numbers is set in the Registry of the workstation after the first fruitful logon to that server. In this way, SIDs can be the advanced fingerprints that demonstrate that a remote system was utilized to log on to a machine and get to a space.

3.4.2 Investigating Live Linux System

The Unix operating system is flexible, powerful, and extremely functional. The Unix operating system functionality makes it so useful as well as makes it a challenge to protect and investigate. You will use the data you collected during the initial response for the investigative step.

Steps in a Linux Investigation

The following actions must have to take to identify the relevant evidence :

1. Review all relevant/pertinent logs.
2. Perform keyword searches.
3. Review relevant files.
4. Identify unauthorized user accounts or groups.

5. Identify rogue processes.
6. Check for unauthorized access points.
7. Analyze trust relationships.
8. Check for kernel module rootkits.

1. **Reviewing Pertinent Logs**

LINUX operating systems have different log files like System activities log such as logons, startups, and shutdowns logged and events associated log with Linux network services. Some log files are located in common directory and some on alternate directory or some logs are place in nonintitutive locations. Logs file on the system are not in question but relative logs on network server security device like firewall and IDS are important to review.

Network Logging

- In Linux operating system most useful logging capability is the syslog (system log) file. This file captures events from programs and subsystems within Linux. The activities of syslog are controlled through the syslog configuration file.
- A syslog daemon, syslogd, runs on the system to log messages. Syslog also offers the ability to log messages remotely, across a network. The logging capability provided by syslog is extremely powerful and flexible. The syslog configuration file controls which types of messages are sent to which logs. Each line in the configuration file contains three fields :
  - **The facility field** denotes the subsystem that produced the log file.

    For example, send mail logs with the mail facility.
  - **The priority field** indicates the severity of the log.
  - **The action field** specifies how the log will be recorded.

Remote Syslog Server Logs

- The log documents produced locally by the syslog daemon are text files that are normally world-decipherable yet writable just by root. This implies any attacker who has picked up director - level access can without much of a stretch, alter the syslog log records removing selected entries, modifying selected entries, or adding misleading entries.
- These adjustments are about difficult to identify. In the event that you think that an attacker has picked up root-level access on the system where the logs are put away, don't believe the logs. The best way to tell for certain if an attacker changed the log records is to perform repetitive logging to a safe, remote syslog server if we maintain the remote syslog server, the entire host should log to the same syslog server. In the event that the attacker deleted/erase the log document then a flawless duplicate ought to exist on the remote syslog server.

- Attacker can add spurious entries to the remote syslog server; however the attacker couldn't alter or remove entries without first compromising the remote server. Thus, the remote syslog server ought to be a solidified (secure) host with insignificant access ideally, just reassure or secure shell (ssh), which likewise exploits system logging. The server's records and passwords ought to be remarkable, to avoid access taking into account the trade off of passwords from different systems.

TCP Wrapper Logging

TCP Wrappers is a host-based access control for TCP and UDP services. Any connection attempts to "wrapped" services are logged via syslog. Notice that the log entry provides a lot of valuable information: the time and date of the attempted logon, the hostname, the service, the account, and the IP address of the system that attempted to log on.

Other Network Logs

Other network logs are primarily service-specific, such as the log files for web servers. This log entry provides the following information :

1. The time and date that the transfer occurred
2. The number of seconds that the transfer took
3. The remote host
4. The number of bytes transferred
5. The name of the transferred file
6. The type of file transfer
7. A special action flag
8. The direction of transfer
9. The access mode
10. The username
11. The service name
12. The authentication method
13. The user ID
14. The status of the transfer.

Host Logging

Linux provides a variety of log files that track host operations. Some of the more useful logs record *su* command execution, logged-on users, logon attempts, and *cron* job (scheduled program) execution.

su Command Logs

The *su* command allows a user to switch to another user ID during a session. Attackers sometimes use this command to attempt to gain root access to a system. Linux records every attempt to execute the *su* command on the system. The log shows the time and date of the *su* attempt, whether the attempt was successful, the terminal device from which the user attempted to execute *su*, and the user ID before and after the *su* attempt.

Logged-on User Logs

The *utmpor, wtmp file* is used to store information about users currently logged on to the system. The log file is named differently and stores slightly different information. The basic information stored is the name of the user, the terminal used to log on, and the time of the logon. The file is stored in a binary data.

Logon Attempt Logs

In most of the Linux systems Logon attempts such as failed and successful are recorded by default.

Cron Logs

Linux has a feature called cron. It t allows users to schedule programs for future execution. It is frequently used for attacks. All executed cron jobs are logged in default logging directory called cron.

User Activity Logging

Linux logs also record other types of user activities. The commands executed by users are recorded by Process accounting logs and shell history files.

Process Accounting Logs

In the process accounting every command run by every user is logged. This type of logging is not enabled by default. To use this feature in Linux you need to have acct or *pacct* log file on your system otherwise you will not be able to use this feature. If any one of the file is exists then you can use the *lastcomm* or *acctcom* command to review the contents of the file. The attacker would need to delete the log file to remove this evidence.

Shell Histories

Linux systems use shell command. These shells provide the capability to log all commands, along with their command-line options. Typically, the history file is stored as a hidden file in the user's home directory.

2. Performing Keyword Searches

Keyword searches are a critical part of incident response investigation, ranging from email harassment to remote network compromise cases. Keywords can be a wide range of ASCII strings, including an attacker's backdoor password and username.

- **String Searches with grep :** grep command is powerful and a primary tool for string searches. To perform a string search within a file, use the grep command. Early Investigators used grep to search the entire disk for evidence of sniffers. Virtually every sniffer had the same strings associated with captured traffic.

- **File Searches with find :** *Find* command is used for searching any filename that matches a regular expression. Find command can search a file system for files that match a wide variety of characteristics, including modification or access time, owner of file, string inside a file, string in the name of the file, and so on. You can also use find in combination with other commands, such as strings or grep, using the powerful exec feature.

3. Reviewing Relevant Files

There are methods to recognize the relevant files to any given incident. These methods include recognizing relevant files by their time/date stamps and by the information got during the initial response to Linux. Configuration and system files commonly are also searched which are abused by attackers.

Incident Time and Time/Date Stamps

- To search for files and directories that were accessed, modified, or created around the time of a suspected incident, you must first know the time of the suspected incident. The timeframe may be very specific, such as when a network IDS discovered and logged the attack as it happened.
- On the other hand, the timeframe may be general, such as in the case where a system administrator connected the system to the Internet two weeks ago and evidence of compromise was found today.
- If you have a good record from an outside source of when the attack occurred, the first step is to make sure that the system time on the IDS matches that of the victim system. Linux file system saves three different timestamps for each file or directory :
  1. The atime, or access time, is the last time that a file or directory was accessed.
  2. The mtime, or modification time, records the last time a file was modified.
  3. The ctime, is similar to the mtime, but it records the last time the inode value was changed. This value can change with events such as changing permissions or ownership.

Special Files

Linux operating system contains some special files such as SUID and SGID files, unusual and hidden files and directories, configuration files, and the temporary directory.

SUID and SGID Files

- Linux contains features known as set userid (SUID) and set groupid (SGID), which are designed to allow programs to operate with higher privileges than those of the user running the program. For example, if user Bob executes a program, that program runs with the privileges of user Bob.
- However, if the program is SUID and Bob executes it, the program runs with the privileges of whichever user owns the executable, usually the root. SGID works the same way, except that the program runs with the privileges of the associated group.
- SUID and SGID root programs are the source of most privilege-escalation attacks on Linux systems, and they are also a favourite backdoor for attackers.

Unusual and Hidden Files and Directories

- Any file or directory in Linux system that begins with a dot (.) is hidden from casual view.
- When you will run the *ls* command it will not appear listing unless the -a option is used. Attackers frequently name files and directories with seemingly innocent names.

Configuration Files

- Configuration files are the main location of evidence during many incidents. Attackers may modify or delete configuration files to allow particular computers to connect to the victim system at will. The inetd. conf configuration file controls many of the Linux system's network services, for example telnet, FTP, and TFTP are started via this file. An attacker may add some extra entries to this file so that the victim system listens on many ports. You find the backdoor here in the inetd.conf file.
- **StartupFiles :** The Linux operating system has several locations that are used to start services and applications. For example, inetd.conf files. Other examples include cron, rcstartup files, and user startup files. Attackers can easily add an entry to any of the startup scripts to start Trojan programs upon bootup. Check each of the startup scripts for spurious entries, and verify that the programs being run from the rc directory are legitimate and not modified by an attacker. Startup files are also stored in each user's home directory. Attackers can embed Trojan commands within these files. Examine all configuration files of this type for spurious entries.
- **Temporary (Tmp) Directory :** Temporary directory is the only world-writable file system on a Linux system. Not only attacker but also many publicly available exploits use this directory to attack and to store temporary files during privilege-escalation attacks, and sometimes they leave trace evidence. Check the temporary directory carefully in the event of an incident to determine if hidden directories or suspicious files exist there.

4. Identifying Unauthorized User Accounts or Groups

It is very important to recognize the unauthorized user account and groups because attackers will frequently modify account and group information on victim systems. This modification can come in the form of additional accounts or increase in privilege of current accounts. So the audit of user and group accounts on suspected victim systems is necessary.

User Account Investigation

- The text file is used to store the user information. This file is also known as password file. This password file contains the entries of every user on a Linux system. The user entry has seven fields such as username, password, user ID, groupID, GECOS field, home directory, and default login shell.
- To assure that user account are not manipulated examine any accounts that should be disabled or unavailable for remote logon, for example daemon, sync, or shutdown. Try to make careful note of each user ID and groupID.

- A user ID of 0 or 1 on a user account is suspicious, it represent root-level and bin-level access, respectively. If a normally privileged user account now has a higher privilege level, it is likely a backdoor for an attacker to gain privileged access.

Group Account Investigation

- Group accounts have the group ID for the groups. The group account document records the groups alongside the clients that are connected with that group. Note that a section in the group record does not have to exist for a group to exist. Group membership depends on the group ID in the password file.
- As you review group accounts on the system, search for any clients who are in exceptionally privileged groups. For instance, a client account that is in the bin group is a reason for further investigation, since this access gives the client account access to delicate system files and is by and large not allowed.

5. Identifying Rogue Processes

Rogue processes identification is easy while examining a live system. It is necessary to record all listening ports and running processes during the initial investigation. Examine carefully the running processes to verify their validity. Review all binaries related with listening services and running processes to assure that they have not been modified.

6. Checking for Unauthorized Access Points

- Linux system offers an array of network services, for example telnet, rlogin, NFS etc. Any one of the networked services on Linux systems can potentially allow some degree of remote access to unwanted intruders, as can a phone line connected to a modem.
- The common access points that intruders can take advantage of include X Servers, FTP, telnet, TFTP, DNS, sendmail, finger, SNMP, IMAP, POP, HTTP, and HTTPS. Unfortunately, this is just a partial list. When you conduct your investigation of the Linux system, you will need to examine all network services as potential access points. Network services could be vulnerable, allowing intruder's access to your system, or network services could already be trojaned by a successful intruder.

7. Analyzing Trust Relationships

- Trust relationships within Linux systems were once a primary mechanism of attack. Trust can be established between Linux systems with a variety of services, the most popular of which include rlogin, rsh, the Network Information Service (NIS and NIS+), NFS, and ssh. Trust relationships can be convenient time-savers for system administrators and users.
- If machine A trusts machine B, then the user on machine B can access machine A with no additional credentials.
- Trust relationships are usually configured through files such as /etc/hosts.equiv or any rhosts file in a user's home directory. Trust relationships can be established with ssh through shared keys and through NFS shares.

- Furthermore, firewalls and host-based access controls such as TCP Wrappers are often configured to let certain source IP addresses communicate with protected hosts, another form of trust. Investigate all possible trust relationships to determine if they played a part in the incident.
- Another type of trust is created through network topology. If attacker compromises one host in the network, it means he can compromise the full network.

8. Detecting Trojan Loadable Kernel Modules

- Loadable Kernel Modules (LKMs) are found on the different sorts of Linux, BSD, and Solaris. LKMs are dynamically loaded by a user with root-level access. LKMs are run at the kernel level instead of at a normal user-process level.
- A few intrusion-based LKMs have been developed, and once a malicious user acquires privileged access to system, they can install one. *Adore, Knark,* and *itf* are the examples of some common malicious LKMs. These LKMs give a few abilities to attackers, for example, giving remote root access to and hiding files, processes, and services.

LKMs on Live Systems

- Detecting Trojan LKMs on a live system can be complicated because these tools actually intercept system calls (such as ps or directory listing) to provide false information. They are specifically designed to prevent detection with traditional response methods.
- However, in many cases, you can find them by combining externally executed commands with local commands to detect anomalies or discrepancies.
- An example would be an external port scan compared to a port scan performed directly on the local suspect system.

LKM Elements

In some cases, the intruder uploads and compiles the source, and successfully installs the LKM; however, she forgets to delete the actual LKM source files! When this happens, you may not only discover the presence of the LKM, you may also find additional configuration information.

LKM Detection Utilities

Developers have created several utilities specifically designed to detect malicious LKMs. Two such utilities are chkrootkit and KSTAT. The *chkrootkit* utility detects several rootkits, worms, and LKMs and The KSAT utility provides several functions useful for detection of Trojan LKMs.

3.4.3 Email Analysis

- Email is used to communicate with the two parties. Where file transfer taken place between the two servers on a particular port number. A client-side application is required to compose an e-mail.

- The examples of client-side application are yahoo mail, Web Client, MS Outlook, hotmail. It requires a Sender's identity, stores it as a file and then delivered to a destination user address through one or more number of servers.
- The Email communication makes the things simple, powerful and efficient. Email writing and communication have been under the focus of malicious intruders over the last few decades. Emails can be forged easily.
- Email abuse is also increasing day by day. Email crimes like spam, threatening mails, narcotic trafficking etc are also increased.

Email Clients and Servers

- Email client message is made up of two parts that are header and the body. The header contains the information about the email origin, like the address from where it comes, how it reached to the destination and who send it. The body contains the message and attachment if any.
- Many organizations have their own mail server. Some Users dials for the internet service provider. When this user sends the mail that mail first go to the ISP server then ISP send that mail to receiver's mail server.
- The message stays on the receiver server till the recipient retrieve it. An email server is a computer which runs on Linux, Windows or any other operating system. The server contains the software to manage the transmission and holds the messages.
- When we investigate the email crime, the internal corporate emails are easy to trace. They use Universal Naming Conventions (UNC) coupled with central authentication and controls. So it makes easy to find the sender and receiver of email.
- The email client performs task like listing all the messages in mailbox by displaying message header as well as the time and date of the messages. It also tells the senders and the size of the message. The client can view, compose or delete the message.
- The email server is having the list of all the accounts. It has text file for each account. When a person clicks the send button to send the mail. It passes the mail to the mail server with sender and receiver name and message. The server formats this information and appends it to the bottom of the recipients' text file. To interact with the server the following email protocols are required.
    - **Post Office Protocol (POP)** : It stores only incoming messages. Investigation is done at the workstation.
    - **Internet Message Access Protocol (IMAP)** : This protocol stores all the messages. Copies of incoming and the outgoing messages are stored on the server or workstation or both.
    - **Microsoft's Mail API (MAPI)** : This protocol also work same as IMAP.
    - **HTTP** : This protocol is used for web based send and receives.
    - **Simple mail transfer protocol (SMTP)** : It is responsible for sending and receiving the email. It uses TCP port 25. It is easy to spoof SMTP and send the fake mail.

E-mail Analysis/ investigation

Email crime investigation or analysis contains the following steps :

1. Examine the email message	2. Copy the email message
3. Print the email message	4. View the mail headers
5. Examine the email headers	6. Examine attachment if it is there in email
7. Trace the Email.	

1. Examine the email

When it is come into the light that email crime has happened then it is necessary to collect the evidence which is required to prove the crime in the court of law. Evidence may be gathers from the victim's computer. Evidence is the mail which the victim received.

- First take the image of machines hard drive.
- Obtain the victims machine password to open the encrypted file.
- Take the printed copy of the crime mail (including header).
- Examine the IP address of the sender's server.

2. Copy the email message into the USB key.

3. Take the printout of the email message by using the print option available in the mail program.

4. View the mail header

- To check the mail header
- Open your mail.
- Right click on your mail.
- After right click menus will display. Click on view full header.
- The file header will get opened.

5. Examine the email header

The email header contains the message header and the subject body. The email header contains the information of the email origin. You can see in the given message that the IP address of the sender's machine is sent i.e. X-originating- IP : [200.85.213.54]. It also gives the return path, and the receiver mail id.

- **From** Suvarna Pansambal Tue Feb 2 12:16:14 2016
- **X-Apparently-To :** suvarnashirke@yahoo.com; Tue, 02 Feb 2016 12:16:15 +0000
- **Return-Path :**<suvarna.atharv@gmail.com>
- **Received-SPF :** pass (domain of gmail.com designates 209.85.213.54 as permitted sender)
- X-Originating-IP : [209.85.213.54]
- **Authentication-Results :** mta1073.mail.gq1.yahoo.com from=gmail.com ; domain keys=neutral (no sig); from=gmail.com; dkim=pass (ok)
- **Received** : from 127.0.0.1 (EHLO mail-vk0-f54.google.com) (209.85.213.54) by mta1073.mail.gq1.yahoo.com with SMTPS; Tue, 02 Feb 2016 12:16:15 + 0000
- **Received** : by mail-vk0-f54.google.com with **SMTP id** n1so95500114vkb.3 for <suvarnashirke@yahoo.com>; Tue, 02 Feb 2016 04:16:14 -0800 (PST)
- **DKIM-Signature :** v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20120113;

  h=mime-version:date:message-id:subject:from:to:content-type;

  bh=7AWYrxUKcsQ8uhNfa2cJrervIPR8oNJDId+M28otZas=;
  b=TFIL3/WMYu9aLdGKBoSoYoWqerdG+Wjmmckw/kKA7tNfNncm1xvyqlRpOYMIO05LIq
- **X-Google-DKIM-Signature :** v=1; a=rsa-sha256; c=relaxed/relaxed;

  d=1e100.net; s=20130820;

  h=x-gm-message-state:mime-version:date:message-id:subject:from:to:content-type;

  bh=7AWYrxUKcsQ8uhNfa2cJrervIPR8oNJDId+M28otZas=;-Gm-Message-State:
  AG10YOT91xCYmn4COfUybd9MEb6HEtEU+MiOY99sDZQ6PbFlgE09G/boN2F9xMBQSk6aAFVx74W0+hL
  Mbo5SJg==
- **MIME-Version :** 1.0
- **X-Received :** by 10.31.16.197 with SMTP id 66mr16543831vkq.41.1454415374794; Tue, 02 Feb 2016 04:16:14 -0800 (PST)
- **Received** : by 10.31.151.147 with HTTP; Tue, 2 Feb 2016 04:16:14 -0800 (PST) Date : Tue, 2 Feb 2016 17:46:14 +0530
- **Message-ID:** <CAL1VNuOeJv075FDfSN=ENDdg_KhGNmQGizVsi9y9eA8OcX401w@mail.gmail.com>
- **Subject :** Threat mail
- **From :** Suvarna Pansambal suvarna.atharv@gmail.com
- **To :** suvarnashirke suvarnashirke@yahoo.com
- **Content-Type :** multipart/alternative; boundary=001a11436378c545c7052ac877ff
- Content-Length : 542

Fig. 3.4.1 : Email Message header

6. **Examine the attachments**

   If the mail contains any attachment then copy that attachment and also take the print of the attachment.

7. **Trace the Email**

   - The IP address of the origination computer machine tells the owner of the email address which has been used in the possible crime that is being investigated. It may be possible that this information may be fake. So it's important to validate the evidence which you uncover. There are many sites which tell the owner associated with the domain name.

     For example: suvarna@yahoo.com, everything after the @ sign is the domain name.

   - The examples of the site which tells the owner of the mail associated with the sites are :

     1. **www.arin.net**

        The ARIN (American Registry for Internet Numbers) is used to find the domain name from the IP addresses. It also gives the contact personal listed against the domain name.

     2. **www.freeality.com**

        This website provides many different searching options like names, phone number and mail address. These websites permit the users to reverse email searches. This may help to reveal the subject's original identity.

e-mail Headers and Spoofing

We have studied the E-mail headers in the previous section. Email spoofing is the forgery of an email header. The message which you receive is actually originated from someone else than the actual user.

Email Spoof with PHP function mail ()

The mail () function allows you to send mail.

- Bool mail (string $to, string $subject, string $message [, string $additional_headers [, string $additional parameters]])
- **Example :** www.rootspot.com/jose/mai

Email Spoof with telnet

- Open command prompt and type telnet 25.
- mail from : your email id @ blah.com
- rcpt to : recipient email id @ blah.com

Email Recovery Tools

The list of the email recovery tools is as follows :

- FINAL e-mail
- Email Examiner
- Network E-mail Examiner
- R-mail

3.4.4 Analysis of Web

- Nowadays there are many web browsers available in the market like Internet Explorer, Google Chrome and Mozilla etc.
- These all-web browsers are slightly different in web services. To display the same website faster on future occasions, web browsers maintain the Downloaded web site data, so that it remains available on the computer even if the user closes the browser or shuts down the machine. This is a useful feature.
- The downloaded web files are known as caches, cached history or temporary files. Based on the operating system and browser applications they are in different locations.

Internet Explorer

The most famous web browser is Internet Explorer (IE) as it is a component of the Windows operating system. IE is very and is frequently used as a default web browser. In windows 10 IE is replaced with Microsoft EDGE (ME). IE and ME both work in In Private mode, without storing information about web resources visited by the user.

Google Chrome

- Google Chrome is browser by provided by Google. It has incorporation with Google services. It allows the Synchronization of user passwords between devices. One can use the extensions and plug-in. Google Chrome performs fast operations and collects user data but it Consumes large amounts of memory.
- The important feature of Google chrome is that it works in Incognito mode, which prevents the browser from permanently storing any history information, cookies, site data or form inputs.
- There are many web browsers created by the third-party developers based on Chrome Engine, like Chromodo, Amigo, Sputnik, Uran, Epic Browser, SafeZone, Comodo Dragon, Flock, Rockmelt, Sleipnir SRWare Iron, Titan Browser, Torch Browser, 360 Extreme Explorer, Avast Chromium, CoolNovo, Cốc Cốc, Vivaldi, Yandex. Browser, Opera, Orbitum, Breach, Nihrome, Perk, QIP Surf, Baidu Spark, etc. All of these borrowers' function like Google Chrome and create webbrowser artifacts like Google Chrome and also support most of Google Chrome's extensions and plugins.

Opera

The Opera web browser is also a famous web browser. It was the first web browser to introduce features that other web browsers adopted, like; pop-up blocking, Speed Dial, private browsing and tabbed browsing re-opening recently closed pages. Opera have a free Virtual Private Network (VPN) service, which permits users to surf the web incognito.

Firefox

Firefox is also one of the popular web browsers. It is more secure as compare to other browsers. It has advanced Incognito mode, disabling tracking of user's locations and advertisements. Firefox has its own extensions.

Difficulties of web browsers forensic analysis

There are following difficulties faced by the forensic examiner while analysing the web browsers :

- Many web browsers are available with lots of data. Different data.
- To protect the data Encryption is used.
- If the user is using the Incognito mode (private mode) then computer do not contain the browser artifacts.

Web browser forensic artifacts

Each web browser has its own artifacts in operating system. The artefacts are depending on the version of the web browser. Usually, one can get the following artefacts :

- History
- Cache
- Cookies
- Typed URLs
- Sessions
- Most visited sites
- Screenshots
- Financial info
- Form values (Searches, Autofill)
- Downloaded files (Downloads)
- Favorites.

3.4.4(A) Cookie Storage and Analysis

- Cookies are the text files. These files are used to feedback from the user to the server. When performing some actions with a web resource like viewing web links, downloading files, etc, these actions are registered in a cookie that is secretly sent by the server to the user's computer. By using this web resource, the server can find out what actions the user has taken on previous visits to this web resource.
- The cookies are stored in cookies folder, but the location of the cookies folder is based on the web browser and the operating system. The Table 3.4.1 illustrate the location of the cookies based on the browser and operating system.

Table 3.4.1

Browser	Operating System	location
Internet Explorer	Windows 98	\Windows\Cookies\
	Windows 2000, Windows XP	\Documents and Settings\Administrator\Cookies
	Windows 7	\Users\%userprofile%\AppData\Roaming\Microsoft\Windows\Cookies
	Windows 7	\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies
Firefox, Windows		\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite
Google Chrome, Windows		\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies.db

3.4.4(B) Analyzing Cache and Temporary Internet Files

Cache Files

- The cache folder contains the browser history and it automatically creates the profile folder at start. This folder is the storage place for the browsing history.

- The Table 3.4.2 shows the cache locations of the different browsers :

Table 3.4.2

Firefox	Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries
Google Chrome, Windows	\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cache\ \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\GPUCache\ \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Media Cache\
Opera	\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\ShaderCache\GPUCache\data_3
Safari, MacOS	\Users\%userprofile%\Library\Caches\com.apple.Safari\Cache.db

Windows Temporary Internet Files

- Temporary Internet Files (C:\Windows\Temporary Internet Files) are immediate downloads from the Internet, more often than not containing realistic pictures in Windows bitmap (bmp), jpeg, gif, or .art format. There will likewise be html and htm files for website home page components, and so forth. Approaching Yahoo and Hotmail messages may likewise exist as files in the Temporary Internet Files folder.
- Downloaded movies, mpegs, avi files, and Adobe PDF files will be found in Temporary Internet Files.

Temporary files

- Windows Temp files (C:\Windows\Temp) are temporary files made by Windows as different programs are running and diverse processes are occurring. They are regularly exact copy of files put away somewhere else on the PC. At different occasions they are exact duplicates of files which are waiting to be handled by the PC.
- For instance, a print work heading off to a laser printer will make a temporary document called an EMF (enhanced windows metafiles). EMF's (smaller than normal photos of the original) can frequently be found in the Temp index a very long time after laser printer was utilized.
- Numerous different sorts of files can be found in the Temp registry too (e.g., programmed report recuperation files).

How is the data stored?

- Internet Explorer and Windows Explorer store most of the data in index.dat files.INDEX.DAT files are used by Internet Explorer to store information about visited pages, cookies and the time they are used.
- To this end, Internet Explorer indexes files that are located in folders that are browser caches and maps these files to the network resource from which these files were downloaded. In addition, INDEX.DAT files contain such information as the decryption of HTTP-header packets, in which the file was transferred, the date of creation and last access to the file, the number of calls to it, and much more.
- The Table 3.4.3 are the locations for index.dat file.

Table 3.4.3

1	\Documents and Settings\%userprofile%\Local Settings\Temporary Internet Files\Content.IE5\index.dat
2	\Users\%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
3	\Documents and Settings\%userprofile%\Cookies\
4	\Documents and Settings\%userprofile%\Local Settings\History\History.IE
5	\Documents and Settings\%userprofile%\Local Settings\ History\History.IE\MSHist[timestamps]

3.4.5 Analysis of Malware

- Malware are the malicious programs which infect the system by executable code. Ransomware aims to compromise the system's Security, Integrity, and Availability (CIA). It runs without permission in an internal system. When it is on victim mode, it completely controls the system. Malware is classified into the following categories :
  1. **Viruses :** Viruses are pieces of executable code. It is extremely detrimental to the system. This type of programme destroys confidential information and modifies data.
  2. **Worm :** A worm is a self-replicating malware computer programme that accesses computer and network resources without the permission of an authenticated user. It consumes network bandwidth in the network. On the target computer, there is a security flaw.
- Malware analysis aims to gain a better understanding of how a particular piece of malware works so that defences can be built to protect an organization's hardware. Techniques for malware analysis and detection are listed as follows :

1. Signature based
2. Behavioural based
3. Anomaly based

1. Signature based Signature-based

- Signature based Signature-based technology is based on a binary pattern. The malware's hash value is determined and stored in the antivirus product's database. When a new programme is run over a network channel, the system compares it to the malware hash value stored in the antivirus database to determine whether it is malware or not.
- It's difficult to determine the new malware version because it only saves the old malware hash value. It is impossible to make a false positive comparison in this situation. Use the generic signature to avoid this issue. All new malware signatures are stored in the generic product database, which can be used to identify all malware families.

2. Behavioural based

- On a virtual sandbox environment, behavioural-based work is performed. In this environment, the sandbox downloads its own malware and discards it without causing any harm to the system or data. Because false positives are common, this technique is rarely used in the network channel.
- When an antivirus protector detects malware, the attacker changes the signature because malware attackers check the antivirus vendor signature and change the malware hash value and signature based on their behaviour. Malware uses two methods in this technique: first, it passes through a host-based antivirus, and second, it passes through an antivirus gateway.

3. Anomaly based

- Detecting user behaviour based on anomalies. If a user's behaviour changes in the network, it compares the signature to the previous signature stored in the antivirus database. In two phases, an anomaly-based detection approach is used.
- The first phase is the training phase, which identifies the system's behaviour in the absence of an attacker using machine learning techniques. The second phase compares previous user behaviour to current user behaviour. If there are any changes in current user behaviour, it determines whether or not it is malware.

Forensic Investigation Malware Analysis

- The details of the relationship between malware analysis and forensic investigation are presented in this section.
- In order to analyse malware in forensics, the right tool and technique must be used to overcome shortfalls in the organisation and network channels. In the investigation, the following tools are used :

1. **Grep** : Grep is a text-searching command-line tool for UNIX systems.
2. **AVG Antivirus** : AVG Antivirus is an antivirus programme that detects and removes malware.
3. **Whois** : This tool is used to query the RIPE database for registration information for IP addresses and domain names.
4. **IDA Pro** is a commercial disassembly and debugging programme.
5. **hexedit** : This programme is used to view and edit the raw data of a hex file.
6. **VMWare** is a virtualization software that can be used to create a virtual machine that can be used as a sandbox for malware analysis.
7. **FileAlyzer** : A tool for analysing files created by safer networking.
8. **Helix** : This is a live Linux distribution with forensics-oriented tools and features.
9. **Sysinternals** : This is a collection of tools for managing, troubleshooting, and diagnosing Windows systems and software. The investigation will be possible thanks to the next generation of automated forensic analysis tools, which present data in new ways and interact with the guide.

3.5 Challenges in Computer Forensics

When it comes to practical implementation, computer forensics investigation methods face some significant challenges. According to Fahdi, Clark, and Furnell, digital forensic challenges can be divided into three categories :

1. Technical challenges
2. Legal challenges
3. Resource Challenges

3.5.1 Technical Challenges

Crimes and criminals evolve in tandem with technological advancements. In digital forensics, this process is known as Anti-forensics technique, and it is considered a major challenge in the world of digital forensics. Digital forensic experts use forensic tools to collect shreds of evidence against criminals, and criminals use such tools to hide, alter, or remove the traces of their crime. The following are the different types of anti-forensics techniques :

1. Encryption

It is legitimately used to protect information's privacy by keeping it hidden from unauthorised users/persons. Unfortunately, criminals can use it to conceal their crimes.

2. Data hiding in storage space

Using system commands and programmes, criminals usually hide chunks of data inside the storage medium in an invisible form.

3. Covert Channel

A covert channel is a communication protocol that enables an attacker to get around intrusion detection systems and hide data on the network. It was used by the attacker to conceal his connection to the compromised system.

4. Steganography

"Steganography is an encryption technique that can be used in conjunction with cryptography to provide an extra layer of security for data protection." Janssen (2014, Janssen, Janssen, Janssen, Janssen, Janssen, Jan Steganography is a technique for concealing information within a file carrier without altering its appearance. This steganography is used by attackers to hide their hidden data (payloads) within the compromised system. When investigating computer crimes, the investigator must first locate the hidden data in order to reveal it for future use.

Other Technical challenges are Operating in the cloud, Time to archive data, Skill gap.

3.5.2 Legal Challenges

- The presentation of digital evidence is more difficult than its collection because there are many instances where the legal framework acquires a soft approach and does not recognize every aspect of cyber forensics, as in *Jagdeo Singh V. The State and Ors*, case Hon'ble High Court of Delhi held that *"while dealing with the admissibility of an intercepted telephone call in a CD and CDR which was without a certificate under Sec. 65B of the Indian Evidence Act, 1872 the court observed that the secondary electronic evidence without certificate u/s. 65B of Indian Evidence Act, 1872 is not admissible and cannot be looked into by the court for any purpose whatsoever."*
- This occurs in the majority of cases because the cyber police lack the necessary qualifications and ability to identify and prove a possible source of evidence. Furthermore, electronic evidence is frequently challenged in court due to its inconsistency. The acquisition of electronic evidence is dismissed in and of itself in the absence of proper guidelines and a proper explanation of the collection.
- The following are also few legal challenges :

1. Absence of guidelines and standards

There are no clear guidelines for collecting and acquiring digital evidence in India. Investigative agencies and forensic laboratories are developing their own set of guidelines. As a result, the value of digital evidence has been diminished.

2. Limitation of the Indian Evidence Act, 1872

The Indian Evidence Act of 1872 has a limited approach; it is unable to evolve with the times and address the fact that electronic evidence is more vulnerable to tampering, alteration, transposition, and other forms of fraud. The Act is silent on how e-evidence is collected; instead, it focuses on how electronic evidence is presented in court with a certificate in accordance with Section 65B, subsection 4. This means that whatever procedure is used, it must be documented with a certificate.

3.5.3 Resource Challenges

Because digital evidence is more sensitive than physical evidence, it can easily vanish as the rate of crime rises. As a result, the burden of analysing such vast amounts of data falls on a digital forensic expert. Forensic experts use various tools to check the authenticity of data in order to make the investigation process faster and more useful, but dealing with these tools is a challenge in and of itself.

The following are examples of resource challenges :

1. Change in technology

Reading digital evidence has become more difficult due to rapid changes in technology such as operating systems, application software, and hardware. Newer versions of software are not supported by older versions, and software developers have not provided any backward compatibles, which has legal implications.

2. Volume and replication

Electronic documents' confidentiality, availability, and integrity are all easily manipulated. Wide-area networks and the internet combine to form a large network that allows data to flow across physical boundaries. The ease with which people can communicate and the availability of electronic documents has increased the volume of data, making it more difficult to identify original and relevant data.

3.6 Tools used in Computer Forensics

Hardware tools

In Digital Forensics hardware devices like cables, adapters, cloning devices, cell phone acquisition devices, portable storage devices, write blockers, and other devices are used. Digital forensics relies significantly on a variety of gear, including PCs, servers, write blocks, cell phone kits, cables, and so on.

Computers

- Computers serve as the foundation of every digital forensics' lab. As a result, as an examiner, you will require the greatest computer workstation that you can buy. Digital forensic examinations need a significant amount of computational power. These jobs may strain even the most robust systems and smash those that fall short.

- A decent test machine should include numerous, multicore CPUs, as much RAM as possible, and huge, fast hard drives. Manufacturers of forensic software give extensive lists of minimum and recommended hardware requirements. You do it at your own risk if you deviate from the minimums.
- To have a better understanding, consider the minimal and recommended system requirements for AccessData's Forensic Tool Kit (as of press time) (FTK).
- The FTK from AccessData is made up of four separate components and/or applications. They are as follows :
  1. Oracle Database
  2. FTK Client User Interface (UI)
  3. Client-side Processing Engine
  4. Distributed Processing Engine.
- The minimum and recommended specs will vary depending on the component, but suffice it to say that there is no such thing as too much RAM or computational power. Access Data recommends the requirements listed in Table 3.6.1 for a computer running the Oracle database, the FTK user interface, and the principal processing engine.

Table 3.6.1 : Access requirement

	Minimum	Recommended
Processor	intel® i7 or AMD equivalent	intel® i9 Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
RAM	12GB (DDR3) 8 GB (DDR2)	12 GB (DDR3) 8 GB (DDR2)
Operating system	Vista, 2008, Windows 7 (64 bit)	Vista, 2008, Windows 7 (64 bit)

- Some components may be installed on separate machines. The minimum and recommended requirements will change depending on which configuration is used.
- Examiners frequently sift through massive amounts of data. As such, digital forensics labs need to have the capacity to store voluminous amounts of data.
- In browsing the PCs for sale on bestbuy.com, the majority of them have between 500 GB and 699 GB of hard drive space. Multiterabyte drives are also available. With numbers like these and caseloads ever increasing, it's easy to see that storage is a major concern.

Cell Phones and GPS units

- Digital forensics is no longer a "PC-centric" pursuit. Cell phones and GPS units, for example, are flooding into labs around the country. These gadgets need hardware that differs from that found in laptops and desktop computers. Over three thousand phones are supported by Cellebrite's FED (Cellebrite Mobile Synchronization LTD).
- Cellebrite's rival, Paraben Corporation, claims to support over 4,000 phones, PDAs, and GPS units (Paraben Corporation). When it comes to cell phones, having the right cable is important.
- Mobile devices, unlike PCs, lack significant uniformity in terms of connections and cords. To deal with the enormous diversity of handsets that walk through the doors, labs must have a wide range of cords. Fortunately, many of the necessary wires are provided by the makers of mobile phone forensic devices.

Cloning Devices

- A number of firms manufacture hardware cloning devices. A forensic clone, as you may recall, is a "bit stream" duplicate of a specific piece of media, such as a hard disc.
- These tools can significantly speed up the process by copying several discs at the same time. They can also offer write protection, hash authentication, disc wiping, an audit trail, and other features.

Crime Scene Kit

- The hardware and software we described earlier aren't the only things you'll need. Outside of the lab, crime scene kits are quite valuable. These kits come pre-stocked with everything an examiner would need in the field to capture digital evidence.
- Pens, digital cameras, forensically clean storage media, evidence bags, evidence tape, report forms, permanent markers, and other common things are included in kits.

Software tools

- Today's market offers a diverse range of digital forensic software packages. Some are general-purpose instruments that may be used for a number of purposes. Others are more concentrated, fulfilling a specific function. These programmes often concentrate on a single form of evidence, such as e-mail or the Internet.
- When picking software, a decision must be made between using open-source tools and purchasing a commercially developed product. Both have pros and downsides. Some of the variables that may be utilised to make this selection are cost, functionality, capacities, and support.
- The computer forensic tools perform the tasks : collection, preservation, analysis and presentation of computer-related evidence. The following are some forensic tools : (https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/).

1. **SANS SIFT**
   - The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu based Live CD which includes all the tools you need to conduct an in-depth forensic or incident response investigation.
   - It supports analysis of Expert Witness Format (E01), Advanced Forensic Format (AFF), and RAW (dd) evidence formats. SIFT includes tools such as log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.
2. **CrowdStrike CrowdResponse**
   - CrowdResponse is a lightweight console application that can be used as part of an incident response scenario to gather contextual information such as a process list, scheduled tasks, or Shim Cache.
   - Using embedded YARA signatures you can also scan your host for malware and report if there are any indicators of compromise.
3. **Volatility**
   - Volatility is a memory forensics framework for incident response and malware analysis that allows you to extract digital artefacts from volatile memory (RAM) dumps.
   - Using Volatility you can extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs, and more.
4. **The Sleuth Kit (+Autopsy)**
   - The Sleuth Kit is an open source digital forensics toolkit that can be used to perform in-depth analysis of various file systems. Autopsy is essentially a GUI that sits on top of The Sleuth Kit.
   - It comes with features like Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching out of the box, with the ability to add other modules for extended functionality.
5. **FTK Imager**
   - FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images or memory dumps.
   - Using FTK Imager you can also create SHA1 or MD5 hashes of files, export files and folders from forensic images to disk, review and recover files that were deleted from the Recycle Bin (providing that their data blocks haven't been overwritten), and mount a forensic image to view its contents in report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.

6. **ExifTool**
   - ExifTool is a command-line application used to read, write or edit file metadata information. It is fast, powerful and supports a large range of file formats (although image file types are its speciality).
   - ExifTool can be used for analysing the static properties of suspicious files in a host-based forensic investigation, for example.

7. **Free Hex Editor Neo**
   - Free Hex Editor Neo is a basic hex editor that was designed to handle very large files.
   - While a lot of the additional features are found in the commercial versions of Hex Editor Neo, I find this tool useful for loading large files (e.g. database files or forensic images) and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.

8. **Bulk Extractor**
   - bulk_extractor is a computer forensics tool that scans a disk image, file, or directory of files and extracts information such as credit card numbers, domains, e-mail addresses, URLs, and ZIP files.
   - The extracted information is output to a series of text files (which can be reviewed manually or analysed using other forensics tools or scripts).

9. **DEFT**
   - DEFT is another Linux Live CD which bundles some of the most popular free and open-source computer forensic tools available.
   - It aims to help with Incident Response, Cyber Intelligence and Computer Forensics scenarios. Amongst others, it contains tools for Mobile Forensics, Network Forensics, Data Recovery, and Hashing.

10. **Xplico**
    - Xplico is an open-source Network Forensic Analysis Tool (NFAT) that aims to extract applications data from internet traffic (e.g., Xplico can extract an e-mail message from POP, IMAP or SMTP traffic).
    - Features include support for a multitude of protocols (e.g., HTTP, SIP, IMAP, TCP, UDP), TCP reassembly, and the ability to output data to a MySQL or SQLite database, amongst others.

11. **LastActivityView**
    - LastActivityView allows you to view what actions were taken by a user and what events occurred on the machine.

- Any activities such as running an executable file, opening a file/folder from Explorer, an application or system crash or a user performing a software installation will be logged. The information can be exported to a CSV / XML / HTML file.
- This tool is useful when you need to prove that a user (or account) performed an action he or she said they did not.

12. DSi USB Write Blocker

- DSi USB Write Blocker is a software based write blocker that prevents write access to USB devices.
- This is important in an investigation to prevent modifying the metadata or timestamps and invalidating the evidence.

13. FireEye RedLine

- RedLine offers the ability to perform memory and file analysis of a specific host.
- It collects information about running processes and drivers from memory, and gathers file system metadata, registry data, event logs, network information, services, tasks, and Internet history to help build an overall threat assessment profile.

14. PlainSight

PlainSight is a Live CD based on Knoppix (a Linux distribution) that allows you to perform digital forensic tasks such as viewing internet histories, data carving, USB device usage information gathering, examining physical memory dumps, extracting password hashes, and more.

15. HxD

- HxD is one of my personal favourites. It is a user-friendly hex editor that allows you to perform low-level editing and modifying of a raw disk or main memory (RAM). HxD was designed with easy-of-use and performance in mind and can handle large files without issue.
- Features include searching and replacing, exporting, checksums/digests, an in-built file shredder, concatenation or splitting of files, generation of statistics and more.

16. HELIX3 Free

- HELIX3 is a Live CD based on Linux that was built to be used in Incident Response, Computer Forensics and E-Discovery scenarios.
- It is packed with a bunch of open-source tools ranging from hex editors to data carving software to password cracking utilities, and more.

17. Paladin Forensic Suite

- Paladin Forensic Suite is a Live CD based on Ubuntu that is packed with wealth of open-source forensic tools.
- The 80 + tools found on this Live CD are organized into over 25 categories including Imaging Tools, Malware Analysis, Social Media Analysis, Hashing Tools, etc.

18. USB Historian

- USB Historian parses USB information, primarily from the Windows registry, to give you a list of all USB drives that were plugged into the machine. It displays information such as the name of the USB drive, the serial number, when it was mounted and by which user account.
- This information can be very useful when you're dealing with an investigation whereby you need to understand if data was stolen, moved or accessed.

3.7 Self Learning Topics : Open-Source Tool for Data Collection & Analysis in Windows or Unix

1. FTK Imager

FTK Imager is a data preview and imaging tool that lets you look at files and folders on local hard drives, network drives, CDs/DVDs, and forensic images and memory dumps. You can also use FTK Imager to generate SHA1 or MD5 hashes of files, export files and folders from forensic images to disc, review and recover files deleted from the Recycle Bin (assuming their data blocks haven't been overwritten), and mount a forensic image to view its contents in Windows Explorer.

2. SANS SIFT

The SANS Investigative Forensic Toolkit (SIFT) is a Live CD based on Ubuntu that contains all of the tools you'll need to conduct a comprehensive forensic or incident response investigation. Expert Witness Format (E01), Advanced Forensic Format (AFF), and RAW (dd) evidence formats are all supported. SIFT includes tools like log2timeline, which creates a timeline from system logs, Scalpel, which carves data files, Rifiuti, which examines the recycle bin, and many others.

3. CrowdStrike CrowdResponse

CrowdResponse is a lightweight console application that can be used to gather contextual information such as a process list, scheduled tasks, or Shim Cache as part of an incident response scenario. You can also scan your host for malware and report any indicators of compromise using embedded YARA signatures.

4. Volatility

Volatility is a memory forensics framework that allows you to extract digital artefacts from volatile memory (RAM) dumps for incident response and malware analysis. You can get information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs, and more with Volatility.

5. The Sleuth Kit (+Autopsy)

The Sleuth Kit is an open-source digital forensics toolkit that can be used to examine various file systems in detail. Autopsy is a graphical user interface that sits on top of The Sleuth Kit. Timeline Analysis, Hash Filtering, File System Analysis, and Keyword Searching are all included out of the box, with the option to add more modules for more functionality.

6. Linux 'dd'

The majority of today's Linux distributions include **dd** by default (e.g. Ubuntu, Fedora). This tool can be used for forensically wiping a drive (zeroing out a drive) and creating a raw image of a drive, among other things.

7. CAINE

CAINE (Computer Aided INvestigative Environment) is a Linux Live CD with a plethora of digital forensic tools. A user-friendly interface, semi-automated report creation, and tools for Mobile Forensics, Network Forensics, Data Recovery, and more are among the features.

8. ExifTool

ExifTool is a command-line tool for reading, writing, and editing file metadata. It's quick, powerful, and can handle a wide range of file types (although image file types are its speciality). In a host-based forensic investigation, ExifTool can be used to examine the static properties of suspicious files.

9. Free Hex Editor Neo

Free Hex Editor Neo is a simple hex editor that was created to work with large files. While Hex Editor Neo's commercial versions have many more features, I find it useful for loading large files (such as database files or forensic images) and performing tasks like manual data carving, low-level file editing, information gathering, and searching for hidden data.

Review Questions

Q. 1 What is computer forensics? What are the advantages and disadvantages of computer forensics?

Q. 2 Explain mirror image.

Q. 3 Explain the memory evidence collection.

Q. 4 Write short note on registry.

Q. 5 Write short note on logs.

Q. 6 Explain the process of evidence acquisition.

Q. 7 Explain analysis and examination of window.

Q. 8 Write short note on Linux.

Q. 9 Write short note on email analysis.

Q. 10 Write short note on web analysis.

Q. 11 Write short note on malware analysis.

Q. 12 Explain challenges in computer forensics.

Q. 13 Explain tools used in computer forensics.

Q. 14 How to create a forensic duplicate of hard drive?

Q. 15 Write down the steps for investigating live Windows system.

Q. 16 Write a short note on email forensics?

Q. 17 Write a short note on email forensics?

Q. 18 Explain the steps involved in email analysis/investigation?

❑❑❑

Network Forensics

Syllabus

Introduction, Evidence Collection and Acquisition (Wired and Wireless), Analysis of network evidences (IDS, Router), Challenges in network forensics, Tools used in network forensics.

Self Learning Topics : IDS types and role of IDS in attack prevention.

Topics

4.1 Network Forensics Introduction

4.2 Evidence Collection and Acquisition (Wired and Wireless)

4.3 Analysis of Network Evidences (IDS, Router)

4.4 Challenges in Network Forensics

4.5 Tools used in Network Forensics

4.6 Self-Learning Topics : IDS Types and Role of IDS in Attack Prevention

4.1 Network Forensics Introduction

- **Network forensics** is the process of collecting and analyzing raw network data and tracking network traffic systematically to find out how an attack was carried out or how an event occurred on a network.
- Network attacks are increasing day by day. Few of the attacks are unintentional which happens because of lack of knowledge. Attacks can be done without gaining entry to the network or system, for example DoS attacks.
- The DoS attacks overload network resources to make the network unavailable to genuine users, but the attacker never gains access to any computer on the network. It's imperative, then, to be exact when we mention particular computer crimes.
- DoS attackers ought not to be referred to as intruders when no interruption happens. In like manner, not all intruders can precisely be named attackers inspite of the fact that the individuals who get access and then destroy information or plant viruses are legitimately called by both names.
- Network forensic helps you to find out that the attacks on the network are done intentionally or unintentionally.
- When the intruders attack the network they leave a trace behind. So, it is necessary to find out the variation in network traffic to track the intrusions. It is important to know the typical pattern of your network, for example, the peak hours of using internet in the city are between 6 a.m. and 6 p.m.
- If anything wrong or suspicious occur during night then the network administrator would find out it as an unusual activity and do the investigation
- The network forensics examiners have to set standard procedures to acquire data after an attack or intrusion incident.
- Normally, the network administrators desire to find compromised machines, get them offline, and restore them as fast as possible to reduce downtime.
- It is necessary to take time to follow the standard procedure to make sure that all the compromised systems are tracked and find out attack methods in an attempt to prevent them from happening again.

Securing a network

- Network forensics is used to find out the security breach due to attacks, Viruses and other incidents. Hardening contains a series of tasks, like applying the latest patches, using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the deepest part of the network. It make sure that if the attacker goes deeper than the access become more difficult and the more safeguard are in place.
- The National Security Agency (NSA) developed a similar approach, called the Defense in Depth (DiD) strategy.

- DiD has the following three modes of protection :
  1. People
  2. Technology
  3. Operations
- If any of the mode out of 3 fails the other mode is used to prevent the attack. Posting people as a mode of protection implies organizations must hire very much qualified individuals and treat them well so they have no motivation to look for revenge.
- Train the employees adequately in security procedures and the organizations security policy. This mode includes Physical as well as personnel security measures.
- The technology mode consists of, selection strong network architecture and using tested tools, for example, firewalls and Intrusion Detection Systems (IDSs).
- Regular penetration testing combined with risk assessment will help you to enhance network security, too. Having set up that permit speedy and exhaustive examination when a security break happens is likewise part of the technology mode of protection.
- At last, the operations mode tends to everyday activities. Updating antivirus software, security patches, and OSs falls into this class, as does evaluation and monitoring methods and disaster recovery plans.

4.2 Evidence Collection and Acquisition (Wired and Wireless)

- Network forensics includes wireless forensics as a sub-discipline. Wireless forensics' main goal is to provide the methodology and tools needed to collect and analyse (wireless) network traffic so that it can be used as legal evidence in court. The evidence gathered can be simple data or voice conversations, thanks to the widespread use of Voice-over-IP (VoIP) technologies, especially over wireless.
- Wireless data collection is accomplished by gathering and analyzing data from wireless networks and devices, such as cell phones. This includes voice communications in addition to normal traffic data. The location of a phone can also be determined. Wireless traffic analysis methods are similar to wired network traffic analysis methods, but different security issues must be considered.
- Consider that network of your organization is hacked and an insider from your organization is sending the business secrets to a friend at a competitor corporation.
- What would it be advisable for you to do? The most important network-based incident response activity is to deploy computer systems that capture or collect network communications. When we investigate any crime or abuse it is necessary to capture network communications. In this segment we are going to concentrate how to catch network activity the terrible and bare metal way.
- For this we utilize programming like tcpdump and WinDump. We are likewise going to concentrate how to gather a strong, secure, network-monitoring system and conduct full-content observing of network movement.

4.2.1 What is Network based Evidence?

- Network based evidence means the result of full-content network monitoring or the interception of electronic communication. Gathering network-based evidence contains setting up a computer system to perform network monitoring, deploying the network monitor, and evaluating the effectiveness of the network monitor. If we see carefully, we came to know that catching the traffic is only a part of the work but extracting meaningful results is the other challenge.
- When you gather the raw data which forms your network-based evidences then next step is to analyse the raw data. This network analysis-based evidences includes reconstructing the network activity, performing low-level protocol analysis, and interpreting the network activity.

4.2.2 What are the Goals of Network Monitoring?

Network monitoring is not done to prevent attacks, but it permits the investigator to do number of tasks. The goals of network monitoring are :

- Confirm or dismiss suspicions surrounding and an alleged computer security incident.
- Gather additional evidence and information.
- Verify the scope of a compromise.
- Identify other parties involved.
- Determine a timeline of events occurring on the network.
- Ensure compliance with a desired activity.

4.2.3 Types of Network Monitoring

Network monitoring can consist of several different types of data collection :

1. Event monitoring
2. Trap-and-trace monitoring
3. Full-content monitoring

1. Event Monitoring

Events are the alerts which tell that something has occurred on your network. Event monitoring is based on rules or thresholds employed on the network-monitoring platform. The network Intrusion Detection System generates the traditional events, but events can also be created by network health monitoring software like MRTG (Multi Router Traffic Graphed) or NTOP. The Snort tool is used to capture the event.

2. Trap-and-Trace Monitoring

Non-content monitoring records the session or exchange data summarizing the network movement. Law authorization refers to such non-content monitoring as a pen register or a trap-and-trace. It in general includes the protocol, IP addresses, and ports used by a network communication. While monitoring additional data is also considered, for example flag, counts of bytes of information sent by each side, and counts of packets sent by each side. The tcptrace tool is used to summarize the session.

3. Full-Content Monitoring

Full-content monitoring yields data that contain the raw packets collected from the wire. It offers the highest reliability, because it represents the actual communication passed between computers on a network. Full-content data contains packet headers and payloads. The tcpdump tool is used to capture the packets.

4.2.4 Setting up a Network Monitoring System

- As we know that software based network diagnosis tools IDS sensors, and packet capture utilities all have their specialized purposes. Network diagnostic and troubleshooting hardware can capture data consistently and usually are the most efficient at capturing data at the full rate of the monitored network segment.
- Drawbacks of network diagnostic and troubleshooting tools are :
  1. They lacked in remote management capabilities and proper storage space.
  2. They usually cost a lot of money.
- Intrusion-detection solutions have overcome the problems of remote management and storage and they can be easily deployed. Some platforms cannot reliably perform both intrusion detection and network surveillance duties simultaneously. Still many organizations are using IDS sensors as network-monitoring devices. If you once instruct an IDS sensor to begin full-content capture, its effectiveness as a sensor will diminish.
- Steps required for creating a successful network surveillance system are :
  1. Decide your objectives for performing the network observation.
  2. Ensure that you have the correct lawful standing to perform the monitoring activity.
  3. Acquire and implement the best possible hardware and software.
  4. Ensure the security of the stage, both electronically and physically.
  5. Ensure the proper position of the monitor on the network.
  6. Evaluate your network monitor.

- In the event that a blunder will happen in any of steps then it could deliver untrustworthy and ineffectual observation capacities inside of your organization.

1. Deciding Your Goals

- It is imperative to know why we are doing network reconnaissance. In this way, as a matter of first importance decide the objectives of your network monitoring, on the grounds that they will influence the hardware, software, and filters you use to gather proof or evidence.
- Choose what you intend to accomplish, for example,
  - Watch traffic to and from a particular host.
  - Monitor a particular individual's activities.
  - Verify interruption endeavors.
  - Look for particular attack marks.
  - Focus on the utilization of a particular protocol.

2. Choosing Appropriate Hardware

- Big organizations can buy the commercial system or they may build their own network monitor. Important thing is this system must have horse power to perform the monitoring functions.
- The small organizations will rely on home-grown solutions. How much data your system can collect, it depends on the three parameters : CPU type, RAM amount and hard drive.

(i) CPU and RAM

- Now a day's system will choose the Pentium machines with minimum 300MHZ and maximum whatever is available.
- The minimum requirement of RAM is 256 MB but if you are using fast Ethernet then it should be 512 MB or more is recommended. So if your RAM is more, then the network monitor will perform better.

(ii) Hard Drive

- The size of hard disk space your system require is depend upon the particularity of your filters and the amount of network traffic travel across the monitored segment.
- Now a day's hard disks are getting cheaper, so we will easily get the 80GB on out laptop and 1TB on drive on a tower. So we should have a big hard disk to overcome the dispersed storage by continually transferring your capture files to external media.

3. Choosing Appropriate Software

- Choosing software is the most difficult challenge in assembling network monitoring. Different monitoring tools are required to meet the different needs, and the tools are very expensive.

- Some free tools are also available to capture the network traffic, and they also perform well but the commercial tools outperform over free tools in analyzing and interpreting the network traffic. So we should know what we will get from the network surveillance software before acquiring it. Examples of the commercial sniffer software packages are Sniffer Network Analyzer for Ethernet, Explorer and LAN analyzer.
- The factors which will affect the software selection are :
  - What type of host operating system will you use?
  - Do you want to implement a "silent" network sniffer?
  - Do you need portability of the capture files?
  - How much data traverses the network?
  - Do you want to permit remote access to your monitor or access your monitor only at the console?
  - What are the technical skills of those responsible for the monitor?
- It is also important to choose the proper operating system. So let's have a look on operating system issues, remote access, silent sniffers, and data file formats.

(i) Operating System

- Some operating system performs well in network sniffing. As we know more the CPU and I/O time that is available to the network monitoring application the better the system will operate under the heavy network workload.
- While building the monitoring platform, make it a point that you have eliminate all the applications and processes which are not important to the operating system , sniffer and administrative functions. For example, remove unnecessary graphical user environments.
- The Unix platforms perform well as compare to other operating system, for example the FreeBSD operating system has provided the most efficient capturing environment, because the developers have streamlined the movement of network frames from the kernel memory space to user memory space.

(ii) Remote Access

- Use the network connection or modem for the remote access to the monitor. One way is install a second network adapter, connect it to a separate network or virtual LAN (VLAN), and then installs remote command-level software such as OpenSSH. You should limit the incoming IP addresses to those sites that are under your control. Another way is to access the system via a modem line for "out-of-band" communications, or communications that cannot be intercepted easily by an attacker.

- If for remote access modem is used then ensure that the remote access is secure and at least it requires user ID and password for authentication. Configure the remote access via modem line so that it accepts only calls that come from specific phone numbers.

(iii) Silent Sniffers

- Many times it happens that they forgot to delete the evidences that they are not aware of. You can prevent intruders from discovering your monitoring system by implementing a foolproof silent sniffer. A *silent sniffer* is a system that will not respond to any packets it receives, for example directed IP datagram, broadcast, or multicast. Most commercial sniffer applications configure the network adapters by keeping listening interface into *stealth mode*.
- Configure your interface to speak only TCP/IP to achieve the maximum stealth. Protocols like NetBIOS create a lot of traffic that may compromise the location of your monitor. Unix systems are generally configured out of the box to communicate with TCP/IP only. On Windows systems, check that you unbind all protocols (NetBIOS and IPX) except for TCP/IP. Disable system from responding to ARP packets, or your monitor may be detected by the attacker. The Unix system uses *ifconfig* command-line options to turn off ARP on your listening interface. If the monitoring software wants an IP address on the listening interface, assign the system a null IP address (0.0.0.0).
- Another approach to implement a silent monitor is to use a one-way Ethernet cable. The one-way connection protects the machine from any interactive attacks. Before deploying your monitor, run a port scanner (Nmap), as well as a sniffer detection tool (L0pht's AntiSniff).

(iv) Data File Formats

- It is important while choosing a tool for full-content monitoring. Practically, consider how the information captured on your system is stored. Many commercial applications have proprietary file formats that make case preparation difficult when other commercial or law enforcement entities get involved.
- Selecting software that creates files in an open standard format will save you from many headaches. Examples of sniffer that use their own proprietary format for the binary capture files they create are :
  - Lawrence Livermore National Labs libpcap-based sniffers (tcpdump, Ethereal, and Snort).
  - Sun Solaris Snoop
  - IBM AIX's iptrace
  - HP-UX's nettl (Network Tracing and Logging Tool)
  - Network Associates' Sniffer Pro
  - AG Group's Etherpeek
  - Novell's LANalyzer

4. **Deploying the Network Monitor**

- Placement of network monitor is important part in setting up a surveillance system. The challenges for the investigators are the newer devices, for example, network switches, VLANs, and multiple data-rate networks.
- The objective of network surveillance is to capture all activity relating to a specific target system. Switches will divide a network by detecting the presence of workstations based on their MAC addresses. Once the switch builds a port to a MAC address relationship table, it will release packets from a port only if the receiving system is present. For example, a network monitor on switch port 4 will never see packets destined for a system on switch port 2.
- There is a feature called *switched port analysis*, or *SPAN* in modern switches, it allows one port of the switch to transmit all frames, regardless of whether the switch has detected the presence of the destination address on that port. Keep the surveillance system in a physically secure location. When you're deploying a system to perform network surveillance keep the system in a locked room where only a select number of trusted employees can gain access.

5. **Evaluating Your Network Monitor**

When we do the network monitoring we have to check frequently that the disk is not filling rapidly. We have to also make sure that the packet capturing program is executing properly. Additionally we have to check that what type of load the network monitoring is carrying.

4.2.5 Performing a Trap-and-Trace

1. To capture the noncontent information from a network we use pen register or trap-and-trace.
2. Using trap-and-trace means monitoring the IP headers and the TCP headers, without monitoring any content within the packets themselves. In this way we can determine the source of the network based attack. It is also helpful to detect the network traffic.
3. It also can be used to detect network traffic anomalies, like backdoor programs that allow covert file transfers that subvert detection by normal IDS.
4. Trap-and-trace monitors are extremely helpful in Denial of Service attack, where they may provide the only evidence other than oral testimony.
5. If your network has an IDS, router, or web server that mysteriously crashes on a routine basis, a trap-and-trace of all network traffic to and from the victim system not only helps pinpoint the source of the problem, but will probably offer good clues about the proper technical fix.
6. It may also be used as evidence that the attack occurred. You can perform a trap-and-trace by using free, standard tools such as tcpdump and win Dump (for windows).
7. The attack occurred can be considered as evidence. You can perform a trap-and-trace by using free, standard tools such as tcpdump and win Dump (for windows).

The tcpdump and WinDump capture files have the same binary format, so you can capture traffic using tcpdump and view it using WinDump.

1. Initiate a Trap-and-Trace with tcpdump at command line or perform a Trap-and-Trace with WinDump for windows operating system.
2. Create a Trap-and-Trace Output File. It is a permanent output file can data can be view live on console. If we do not have the output file then the information is lost the minute you terminate your tcpdump or WinDump process. Unix cat command is used to view the capture file.

4.2.6 Using TCPDUMP for Full Content Monitoring

- We conduct the full-content monitoring for computer security incident response. For instance, if an employee of organization suspected of transferring business secrets to a conspiring party, do you just want the transaction information or would you also prefer to intercept the content of the data transmitted?
- When an attacker breaks the security of one of your servers, do you also want to intercept the full amount of data he sends and receives from the victim system? When you are done with your monitor system set up, then you are ready to begin full-content monitoring. Tcpdump tool is used for full content monitoring.

1. Filtering Full-Content Data

While monitoring the system we collect the much traffic, and it is needed to filter the full data content. As we know tcpdump relies on building Berkeley Packet Filters. So there are various options offered by the tcpdump tools to draw the attention towards specific packets.

2. Maintaining Your Full-Content Data Files

- The important aspect of collecting full-content data is file naming and ensuring the file integrity. It is important to give a filename to a capture file with some unique element to identify the origin and the purpose. So we include the timestamp, hostname and interface in capture filename. Where the timestamp is written as date (day, month, year) and time (hour, minutes, seconds) format.
- After giving the unique naming convention, perform MD5 or SHA hashing of full-content data files for ensuring the integrity of the evidence.

4.2.7 Collecting Network-based Log Files

- When you collect the evidences make sure that you are overlooking the potential sources of evidence when you respond to an incident. It happens that the most network traffic leaves an audit trail somewhere along the path it travelled.

- Some examples are given as follows :
  - Firewalls, routers, servers, IDS sensors, and other network devices may keep up logs that record network-based events.
  - DHCP (Dynamic Host Configuration Protocol) servers log network access when a PC requests an IP lease.
  - Modern firewalls permit administrator a broad measure of granularity when making review logs.
  - IDS sensors may grab a part of an attack because of a signature recognition or peculiarity detection filter.
  - Host-based sensors may detect the change of a system library or the addition of a file in a sensitive location.
  - System log files three time zones away on the primary domain; controller may show a failed authentication during a logon attempt.
- When all the existing segments of the network-based evidence are combined then they reconstruct a particular network event like file transfer, a buffer overflow attack and a stolen user account and password being used on your network.
- All the investigative clues have some unique challenges for the investigator. That challenges are :
  1. The network-based logs are stored in many formats.
  2. This logs may originate from several different operating systems.
  3. This logs may require special software to access and read.
  4. These logs are geographically dispersed, and sometimes use an inaccurate current time.
- The main challenge for investigators is in locating all these logs and correlating them. This is very time-consuming and also resource-demanding to obtain geographically dispersed logs from many different systems, maintain a chain of custody for each of them, and reconstruct a network-based event.
- Many times, the proper combination of all these logs still paints an ugly, incomplete picture.

4.3 Analysis of Network Evidences (IDS, Router)

- The process of monitoring and analysing network events for signs of possible incidents, violations, or imminent threats to your security policies is known as intrusion detection. The process of performing intrusion detection and then stopping the detected incidents is known as intrusion prevention. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are security systems that become part of your network to detect and prevent potential incidents.
- Routers/IDS role is also important in the incident. Routers lacks in data storage. Routers are the springboards for the attackers at the time of network penetration. Routers store the information like routing table, password and network block information. This information is used by attacker to attack the network as well as by investigators.

4.3.1 Obtaining Volatile Data Prior to Powering Down

- Every time firstly always obtain the volatile in the response process. Memory contains some information and it may be possible that information in the memory is important for the investigation, so that information should be saved before powering down the router. As we know that routers have less data storage capacity so the information in the memory is very important.
- Non-Volatile Random-Access Memory (NVRAM) stores the router configuration. When we reboot or power down the router there are chances of losing the system state information in memory like current routing tables, listening services and current passwords.
- The steps discussed in this section are typically important for routers that have been steps in router investigation :

1. **Establishing a Router Connection** is necessary before doing anything. Accessing router from the console port is the best way. Whenever router connection is established at that time make sure to log the entire session.
2. **Record System Time,** which helps in cross referencing the data.
3. **Determining who is logged on** which helps in finding who is logged on the router.
4. **Determine the routers uptime,** which is nothing but the time that the system has been online since the last reboot can also be important.
5. **Determine the listening sockets,** where we come to know that which ports are listening on the router. Use an external port scanner to determine which services are running on the router. We can also examine the configuration file which covers all aspects of the router's configuration.
6. **Save the Router Configuration,** Router configuration information is stored in single file in NVRAM. When the router boots it uses this stored configuration. It is possible to change the configuration of the router without modifying the configuration file stored in NVRAM. You should save the configuration that is in RAM as well as the configuration in NVRAM.
7. **Review the routing table,** the routing table contains the blueprint of how the router forwards packets. If an attacker does the changes to the routing table then the attacker also change the packets sending location. Manipulating the routing table is a primary reason for compromising a router. Static routes, which are within the configuration file, are also visible to attacker, so the attacker can change the routes.
8. **Check interface configurations,** the information of every routers interface which is available in configuration file should be checked.
9. **View the ARP (Address Resolution Protocol) Cache,** The ARP maps IP addresses and Media Access Control (MAC) addresses. Many times it happens that attacker spoof IP and MAC addresses to evade security controls, such as Access Control Lists (ACLs), firewall rules, or switch port assignments. So, the ARP cache can be useful when investigating attacks of these types. The ARP cache is easy to destroy and easy to save.

4.3.2 Finding the Proof

As at first, we have collected and saved the evidences, now the next step depends on the type of incident suspected, based on your initial investigation done. So, it is necessary to check the responses for the different incident types which involved the routers including how to identify collaborating evidence. The types of incidents that involve routers are as follows :

1. Direct compromise
2. Routing table manipulation
3. Theft of information
4. Denial of service

4.3.2(A) Direct Compromise

Handling Direct-Compromise Incidents

- When an attacker gets the privileged access or interactive access to the router it is called the direct compromise of the router. Direct compromise gives the attacker control of the router as well as access to the data stored on the router. Administrative access to the router is getting by many ways including telnet, console, SSH, web, Simple Mail Transfer Protocol (SNMP), modem and TFTP access.
- If a person has an interactive access to the router, he/she may use the router to identify and compromise other hosts via available router clients for example ping and telnet. This is mainly dangerous because the router is often allowed access to internal networks, even though a firewall may block all other access to internal networks.

Investigating a Direct-Compromise Incident

Till now we have collected the information like configuration file and the list of the listening ports. Now the investigation is off to a strong start.

1. Listening Services
   - The listening services on the router give the potential attack points from the system. The list of interfaces ought to let you know whether the router has modem access.
   - An audit of the physical security of the router will decide the relative availability of the console port. In all probability, just a few ways of attack are possible, and this simple exercise has limited down the scope.
2. Passwords
   - Many ways of attack to the router require a password. Routers can have different passwords for different services, for example telnet, SNMP, and enable access. Attacker can manage to get or learn the password to the router through different ways.

- One way is using the brute force password guessing. But if the password is big and complicated then it is extremely difficult to guess, then brute force password guessing probably was not the means of compromise.
- In the configuration file the passwords are stored in the form of cleartext or encrypted using the Viennese cipher (XOR) or MD5 algorithm. Another way for attackers to learn the password is via network sniffing. Any protocol that passes cleartext data and authentication information for example SNMP, telnet, HTTP, and TFTP is vulnerable to network sniffing.
- A quick review of the passwords in use will provide the investigator with some clues about the compromise.

3. Other Compromise Possibilities

- A person with console access to the router can gain administrative access to the box through a reboot and appropriate procedures. The system uptime information gained during the investigative steps will provide the last time the router was rebooted. Instead, if a modem is connected to the router, it's possible that the last legitimate user did not log off properly, allowing an attacker to get access to the router without a password.
- Another method of compromise, TFTP, deserves a bit of explanation. Routers use TFTP to store and reload configuration files over a network. TFTP is a UDP protocol, inherently insecure. It requires no authentication, and all data passes as cleartext. Router configuration files often use the naming convention of *<hostname>*- confg or *<hostname>*.cfg. To take advantage of these factors, an attacker only needs to scan a network for a router and a TFTP server.

The attacker learns the hostname of the router via Domain Name System (DNS) resolution and requests the configuration file from the TFTP server. At this point, the attacker can use the password information in the configuration file to access the router or modify the configuration file, and then upload to the TFTP server and wait for a network reload.

Recovering from Direct-Compromise Incidents

To do the recovery from a direct-compromise incident, all recovery steps should be taken while the router is offline. The following are the recovery steps :

- Remove all unnecessary services.
- Allow remote access only through encrypted protocols.
- Allow no SNMP access or read-only access.
- Do not use the SNMP password as the password for any other access.
- Change all passwords.
- Implement ACLs so that only connections from trusted hosts are allowed to the router.
- Upgrade the software with the latest updates.

4.3.2(B) Handling Routing Table Manipulation Incidents

Routers can use different types of protocols to update their routing tables. The examples of protocol are RIP, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), and so on. These protocols communicate information about the best path between networks to neighbour routers, and they have varying degrees of security.

1. **Investigating Routing Table Manipulation Incidents**

   The knowledge of the network is necessary to understand if there are any inconsistencies. If any of the routes do not pass the common sense test, or if packets appear to be routed through distant networks, then careful investigation is required. If unfamiliar static routes appear in the routing table, then the router may have suffered direct compromise.

2. **Recovering from Routing Table Manipulation Incidents**

   When the routing table attack is performed, then doing recovery from routing table attacks is simple. Remove unwanted static routes and reboot the router. It is little bit difficult to prevent the attack from occurring in future. ACLs are the solution to limit router updates to known-good source addresses. However, because some routing protocols are UDP, these addresses can be spoofed. Anti-spoofing ACLs can further limit exposure, but these lists are not foolproof. The routing protocol chosen should allow for authentication, and the authentication should be enabled.

4.3.2(C) Handling Theft of Information Incidents

- The information that an attacker can steal from the router is password, routing and topology information.
- The recovery from this data theft is to change passwords, avoid password reuse, and limit the ability of attackers to obtain sensitive information. A general problem that we see is the SNMP service enabled with the default community string (password) of public. With this service enabled, an attacker can gain a great deal of sensitive network information. Internet attackers can also learn the hosts and IP ranges on internal networks.

4.3.2(D) Handling Denial-of-Service (DoS) Attacks

DoS attacks are very often directed at routers. In DoS attack the attacker force a router to stop forwarding packets, then all hosts behind the router are effectively disabled. DoS attacks are divided into several basic categories :

- **Destruction** : Attacks that destroy the ability of the router to function, for example deleting the configuration information or unplugging the power.

- **Bandwidth consumption :** Attacks that attempt to beat the bandwidth capacity of the router's network.
- **Resource consumption :** Attacks that degrade the ability of the router to function, for example by opening many connections to the router simultaneously.

Investigating DoS Attacks

It is very easy to determine the type of Dos attack.

1. If the router does not work at all it might be a destruction attack. Check the observable problems first: power, cables, and configuration.
2. If the router is periodically rebooting or its performance regularly degraded then probably it is a point-to-point attack directed at the router. Regularly degraded performance may be either a resource or bandwidth- consumption attack. In either case, a network sniffer will reveal details. Look for packets destined directly to the router, as well as a flood of packets that are not part of established connections. Packets directed to the router will usually affect the router only if a port is listening on the router. A router is rebooting and not functioning well then there is a denial of service.
3. A flood of packets concentrating to the router can also cause degradation. If the router has open ports, then an excess of SYN or similar packets may badly impact the performance of the router. On the other hand, regardless of the fact that the router has no open ports, a flood of traffic might affect the router or use the bandwidth such that network performance is significantly degraded. A DDoS attack is an example of a bandwidth attack. In spite of the fact that this type of attack is not necessarily directed at a router, the router can be used to moderate the effects of the attack.

Recovering from DoS Attacks

The following steps are taken for recovery in DoS attack.

- Remove the listening services.
- Always upgrade software to the latest version.
- Restrict access to listening services using ACLs.
- Limit the malicious traffic by implementing ACLs.

4.3.3 Using Routers as Response Tools

During the incident response there are many uses of routers, particularly during recovery. A couple of the more useful router features are ACLs and logging capabilities. Moreover, there are particular actions that can be taken on routers to relieve the effects of DoS attacks.

1. Understanding Access Control Lists (ACLs)

ACLs are the process which control traffic passing through the router. Packets can be controlled based on a alluring array of attributes, including the following :

a. Source or destination IP address

b. Protocol

c. TCP or UDP source or destination port

d. Type of ICMP message

e. TCP flag

f. Time of day

To implement the security policies, Normally, ACLs are used. A well-configured router can give many of the capabilities of business firewalls, and routers are regularly used to supplement firewalls. The first thing we have to do is configure an ACL and then go for prevention of IP address spoofing.

Preventing IP Address Spoofing

If an attacker can impersonate as a trusted network address, a victim system will allow the attacker's packets to reach their goal. Routers play a vital role in preventing these attacks. Every interface on a router should disallow packets that logically could not be coming from that network interface.

2. Monitoring with Routers

Throughout the incidents frequently monitoring the network traffic is very helpful. For network monitoring routers are used. Other monitoring software cannot keep up with the bandwidth passing through the router. Logging is configured through ACLs, and logging can be configured for permitted traffic, rejected traffic, or all traffic.

3. Responding to DDoS Attacks

- DDoS attack uses the systems around the Internet to concurrently send large amounts of traffic to victim sites. Successive attacks have expanded on the theme, with traffic-amplification techniques that are capable of degrading service at even the largest of sites. The effects of these attacks can never be totally avoided.
- If adequate traffic hits a victim site at the same time, the victim site will not be able to respond to all requests. However, there are some specific actions that can be taken to ease the effects of these attacks and reduce their ability to deny service. The ICMP, UDP and TCP protocols are the part of DDoS attack, so DDoS attacks are also known as multiprotocol attacks.

- The attacks where ICMP and UDP packets are involved can be eased quickly by blocking ICMP and UDP packets. ACL is introduced because many networks do not need these protocols to be allowed in from the Internet.
- ACLs deny all ICMP traffic and all UDP except for DNS traffic to a particular DNS server(s). TCP attacks are harder to alleviate. TCP traffic is important, unless you don't get email, have a website, or utilize Internet associations in whatever other way. There are two types of TCP based DoS attacks : *connection-oriented* or *connectionless.*

(i) Responding to Connection-Oriented TCP Attacks

- In the Connection-oriented attacks, it completes the three-way TCP handshake to establish a connection. As this attack completes the three way handshake, the source address of the attack is virtually certain. Connection-oriented attacks are also known as *process table* or *resource allocation attacks.*
- It must originate from the genuine determined source address, so filtering the offending addresses is conceivable through an ACL. The unfortunate part is that the filtering is reactive it means you can only filter the source address after identifying the offender via log files or network monitoring.

(ii) Responding to Connectionless TCP Attacks

- The Connectionless TCP attacks first initiate TCP connections. It sends the SYN packets and it never completes the handshake. As in this attack sequence number plays no role so the source-address spoofing is unimportant. These attacks are difficult for the responder to filter because packets may contain different source addresses which are not the actual source of the packet.
- These attacks are not damaging as compared to connection-oriented attacks. Increase the TCP rate filtering to reduce the effect of connectionless attack. The basic idea of rate filtering is based on the characteristics of normal traffic versus the traffic experienced during SYN floods.
- Normal connections require the SYN packet to be sent only when the connection is first being established. Rate limiting the number of SYN packets into the network will throttle the amount of new incoming connections during normal operation. The importance of rate limiting comes during a SYN flood attack, when the router chokes the fake SYN packets being thrown at the router.
- For example, if the router passes SYN packets no more than 40 percent of the time, then at least 60 percent of the traffic will always be established connections. This solution should not affect overall bandwidth to the network; it impacts only the number of connections to the network.

4.4 Challenges in Network Forensics

The challenges of network forensics are depicted in the Fig. 4.4.1.

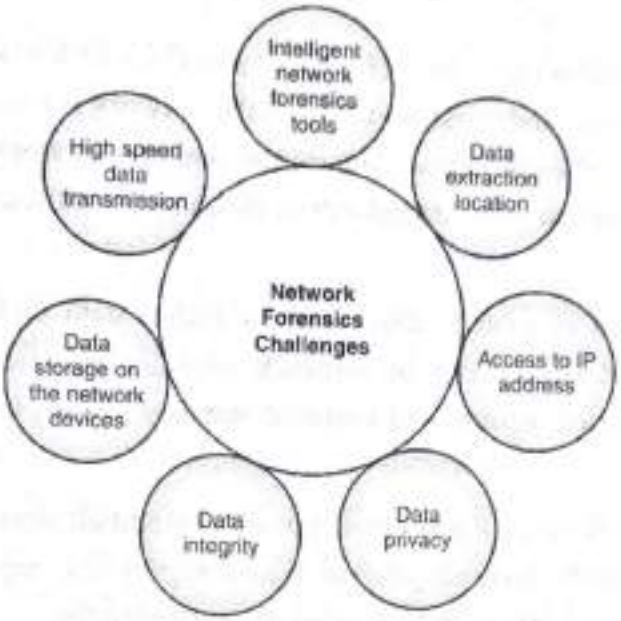


Fig. 4.4.1 : Challenges of network forensics

1. High Speed Data Transmission

- The high data rate of network traffic makes capturing and preserving all network packets difficult for network forensics. In a matter of seconds, millions of packets are sent across the network, which is made up of thousands of interconnected network devices. By analysing network data flow, such network devices serve as evidence for network forensics to investigate susceptibilities.
- In a high-speed data network, network susceptibilities necessitate the recording of all packets without losing any of them, which is a difficult and time-consuming task. Most businesses connect multiple distributive infrastructures with high-speed networks to expand and improve their network structure.
- As a result, security devices do not always capture all network traffic, resulting in incomplete logs for network data flows. These missing logs make reconstructing a suspicious attack more difficult, and thus identifying the intruder's source becomes more difficult. To solve the network forensics problem associated with high-speed packet transmission, a new solution is needed that can capture, preserve, index, and analyse such packets in real time.

2. Data Storage on the Network Devices

- The network transmits a massive amount of data, which is captured and analysed for investigation. However, such data makes retrieving evidence from the network more difficult for network forensics.

- For example, the captured data must be stored on devices with a large storage capacity, whereas the network interconnectivity devices' storage capacity is limited.

3. **Data Integrity**

- Data integrity is critical in the network forensics process, which must be addressed. The ability to keep accurate, complete, and consistent data in the network is known as data integrity. Network forensics must ensure the integrity of data captured on the network, which is a difficult and time-consuming task. The scope, size, and velocity of data make it difficult for investigators to maintain data integrity.
- Furthermore, the lack of trust in data integrity makes data and data systems unpredictable, adding to the complexities faced by network investigators. Hardware and software errors, malicious attacks, system failure, and frequent mobility of data in the network all compromise data integrity.
- If the integrity of the data is not preserved when it is modified intentionally or deliberately, it has a negative impact on the forensic process. Data integrity encompasses security, dependability, and consistency, all of which are critical network characteristics.
- Furthermore, data integrity enables network forensics investigators to present the case in court in order to prosecute the intruder as a criminal. End-to-end mode, which includes both software and hardware, must be used in a seamless manner to ensure data integrity.

4. **Data Privacy**

- In the network forensics investigation process, data privacy is a critical consideration. To address the aforementioned issue of user privacy, a forensic attribution solution is proposed. To enforce forensic attribution in the network, a forensic investigator can view the data of interest by verifying the packet signature.
- However, accessing data on an organization's network may be in violation of its privacy policies. As a result, organisations are wary of allowing network forensics investigators to access sensitive data. This is due to the fact that a single trace file accessed in the network for a malicious incident may contain other important records of multiple users or an organisation, such as financial and employee records.
- As a result, businesses prefer not to allow any third-party investigators to use their network data for any investigation. Furthermore, collecting network data raises a number of legal issues, including user data privacy and confidentiality, which could cause the network forensics process to be further, delayed.
- An investigator's trace file may contain a user's password, email content, bank account information, and other personal information. When data is transmitted across multiple networks via multiple ISPs installed centrally, network forensics becomes more sophisticated.

5. Access to IP Addresses

- In network forensics, gaining access to an intruder's source IP address is a crucial step. The origin of the attack is indicated by the source IP address, which aids in identifying the intruder and stopping the attacks. Intruders use a variety of techniques to conceal their original source IP address from various network security devices.
- For example, spoofing an IP address can result in the creation of a forged source IP address with the intent of concealing the sender or impersonating someone else. It's most commonly used in DDoS attacks to flood a network system with a massive amount of traffic from a variety of suspect systems. The use of a spoofed IP address makes forensics investigations more difficult, especially in large distributed networks environment where determining the original source IP address is difficult.
- In order to prevent network forensics investigators from properly addressing them, some intruders generate multiple source IP addresses. The fake IP addresses are dispersed throughout the network, causing the system to become overloaded; this is especially true during DDoS attacks. As a result, determining the correct source IP address to determine the source of the attack is difficult.
- Furthermore, most systems in a network are given dynamic IP addresses, which means that at the time of an attack, they may have different IP addresses than they do now. This complicates determining the correct IP address for the right system at the right time. The aforementioned IP address issues make the system more expensive and difficult to use when an investigation is required in real time.

6. Data Extraction Location

- Network forensics is made more difficult by the distributed nature and virtualized characteristics of networks, which make it difficult to determine the best location and device for data extraction. A network with thousands of devices connected to each other via high-speed data links transmitting millions of packets per second is difficult to manage for each link and device individually.
- Extraction of data from the appropriate location of a large volume network for the purpose of analyzing network packets is a major challenge for network forensics, which should not jeopardize data privacy and integrity any further. Furthermore, routers, IDS, firewalls, network forensics analysis tools, protocol analyzers, packet sniffers, and other devices are used to collect and extract data for network forensics.
- Furthermore, it is difficult to place such devices in the appropriate locations to collect the maximum amount of data from the network for investigation and reconstruction of attack paths. It's critical to find the right location, use the right device, and collect the right evidence from the network at the right time.

7. Intelligent Network Forensic Tools

- Current network forensic analysis tools target complete packets to capture and record network traffic. Such tools have issues with storing large amounts of data with longer time delays. Depending on the investigational situation, an intelligent and smart network forensic tool is required to capture network traffic of choice.
- Capturing specific session data with a domain of interest, for example, which then records, analyses, and visualizes the data. This will alleviate storage issues, computational resources for investigation, bandwidth utilization, and time delays, resulting in rapid incident response in a real-time situation. The intelligent network forensic tool will provide a comprehensive visual representation of the network's ports, devices, channels, and protocols.

4.5 Tools used in Network Forensics

There are different types of tools available for network administrator or forensic. By using these tools one can perform remote shutdowns, monitor device use and more.

Windows Operating System Network Tools

- Sysinternals is a collection of freeware tools for examining windows products. These tools are created by Mark Russinovich and Bryce Cogswell and acquired by Microsoft.
- These tools are very helpful for monitoring the network traffic thoroughly and efficiently. You can monitor your network and shutdown machines or processes that could be harmful.
- Table 4.5.1 will give the information about the tools. All the tools mentioned in the tables are freeware.

Table 4.5.1

Tools	Description
RegMon	It Shows all registry data in real time.
Process explorer	Shows what files, Registry keys, and dynamic link libraries (DLLs) are loaded at a specific time.
Handle	Shows what files are open and which processes are using these files.
Filemon	Shows file system activity.
PsExec	Runs processes remotely.
PsGetSid	Displays the Security Identifier (SID) of a computer or user.
PsKill	Kills processes by name or process ID.
PsList	Lists detailed information about processes.

Tools	Description
PsLoggedOn	Displays who's logged on locally.
PsPasswd	Allows you to change account passwords.
PsService	Enables you to view and control services.
PsShutdown	Shuts down and optionally restarts a computer.
PsSuspend	Allows you to suspend processes.

UNIX/ Linux operating System Network Tools

- Knoppix Security Tools Distribution is a bootable Linux CD intended for computer and network forensics.
- Before using this tool one has to adjust the BIOS of the system you are using and make sure that it is booting from your CD.
- The Knoppix Security Tools Distribution is made by Klaus Knopper and maintained and updated by knoppix users.
- Knoppix offers tools of various categories like authentication, firewalls, password tools, wireless tools, encryption, IDS's, honeynets, forensics, packet sniffers, Vulnerability, assessment etc.

Table 4.5.2

Tools	Description
dcfldd	The U.S. DOD computer forensics lab version of the dd command.
memfetch	Forces a memory dump.
photorec	Retrieves files from a digital camera.
snort	A popular IDS that performs packet capture and analysis in real time.
oinkmaster	Helps manage snort rules so that you can specify what items to ignore as regular traffic and what items should raise alarms.
john	The latest version of John the Ripper, a password cracker.
chntpw	Enables you to reset passwords on a Windows computer, including the administrator password.
tcpdump and ethereal	Packet sniffers.

Using PACKET SNIFFERS

- "PACKET SNIFFERS" are device and/or software placed network to monitor traffic.
- Network administrators use sniffers for increasing security and tracking bottlenecks.
- Attackers use sniffers to obtain information illegally.
- On TCP/IP networks, sniffers examine packets. Thus termed as "Packet sniffers".
- In OSI model, Packet sniffers work at Layer 2 or Layer 3.
- Some sniffers perform packet captures. Sniffers are used for analysis. Some of the sniffers are used for both the purpose.
- Your organization needs to have policies about network sniffing to comply with new federal laws or digital evidence.
- As in windows, they have many sniffing tools capable of capturing and analyzing packets. But can't feed data (they collect directly into other tools).
- Most of tools can read anything captured in Pcap (Packet capture) format (LibPcap is for LINUX/UNIX and WinPcap is for Windows).
- As forensics experts, you must choose tools that best suit your purpose.
- **For Example :** If your network is being hit by SYN flood attacks. You need to find packet with SYN flag set.
- To find these packets, TCP dump Tethereal and SNORT can be programmed to examine TCP headers to SYN flag (Flag areas contains several flags and SYN flag is one of them).

Table 4.5.3

Tools	Description
Tcpslice	It is a good tool for extracting information from large Libpcap files; you specify the time frame you want to examine. Also Capable of combining files.
Tcpreplay	A suite of tools which can be used to replay network traffic recorded in libpcap format, this information used to test network devices such as routers, switches, etc.
Ngrep	It is used to examine Email headers or IRC logs. It collects and hashes data for Verification.
Ethereal	Tool used for viewing Network traffic graphically.

Tools	Description
Netdude	It's a GUI tool, which are designed as an easy-to-use interface for inspecting and analyzing large Tcpdump files.
Argus	It is a session data probe, collector and analysis tool.
Ethereal	It is used in a real-time environment to open saved trace files from packet capture. It also used to rebuild session.

Examining the Honeynet Project

- The main aim this project is to make the information available was developed to make the information available in an attempt to thwart internet and network attackers. Worldwide there are many people who participate in the project. The main aim behind it is to create awareness, information and tools.
- The first step is making people and organizations aware that threats exist and they might be targets.
- The second is to provide information on how to protect against these threats, including how attackers operate, how they communicate, and what tactics they use. Finally, for people who want to do their own research, the Honey net Project offers tools and methods.
- The recent major threats to a network are Distributed Denial-of-Service (DDoS) attacks and zero day attacks. In DDoS attacks, the attacker uses hundreds or even thousands of machines.
- These machines are known as zombies because they have unwittingly become part of the attack. When the first DDoS attacks began, the main concerns were the high monetary impact and the amount of time it took to track down these attacks.
- In **Zero day attacks** attackers look for holes in networks and OSs and try to exploit these weaknesses before patches are available.
- The honeynet project set up as a resource to help network administrators' deal with DDoS and other attacks. It involves installing honeypots and Honey walls at various locations in the world.
- A Honeypot is a computer set up to look like any other machine on your network; its purpose is to lure attackers to your network, but the computer contains no information of real value. In this way, you can take the Honeypot offline and not affect the running of your network.
- Honeywalls are computers set up to monitor what's happening to honeypots on your network and record what attackers are doing.
- The principle behind honey pots is that they aren't used on the network; they are simply set out to act as bait.

- The original machine is loaded with the standard software used on that part of the network, a forensic image of it is created, and then the machine is deployed on the network. If the machine is compromised, it's taken offline and another image of it is made.
- The software then compares the two images to determine what method of attack was used and what files were altered or added. Both images are stored in the database.

4.6 Self-Learning Topics : IDS Types and Role of IDS in Attack Prevention

Intrusion detection is a type of security management system for networks and computers. An ID identifies possible security breaches by gathering and analyzing information from various sources within a computer or a network. These breaches include both intrusions and misuse. Intrusion Detection uses a technology developed to access the security of a computer or network known as vulnerability assessment.

4.6.1 Intrusion Detection System

- IDS are security software which is designed to automatically alert the administrators when someone or something is trying to compromise information system through malicious activities or through security policy violation.
- It inspects all inbound and outbound network activities i.e., it monitors network traffic and identifies suspicious patterns. IDS may also respond to some malicious traffic by taking some particular actions like blocking the user.
- There are four elements of IDS :
  1. Events
  2. Analysis
  3. Counter measure
  4. Storage

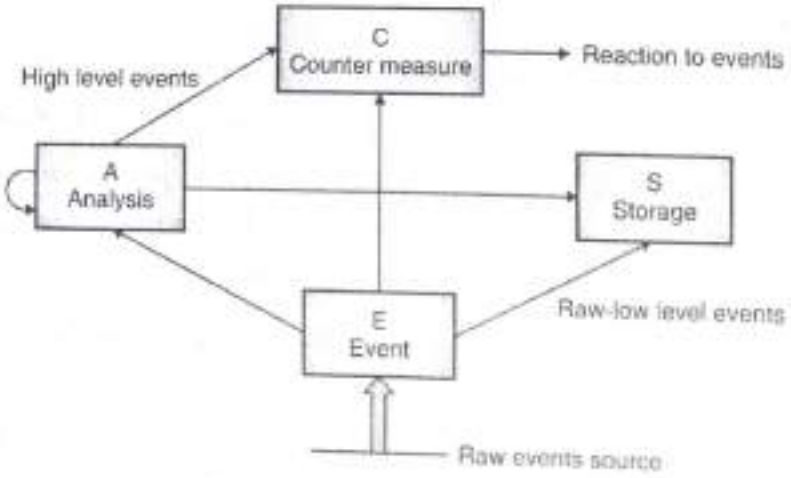


Fig. 4.6.1 : Components of IDS

- IDS get the input from the sensors. When an event happens; if it is a low-level event then IDS simply stores input and takes some control measures, and if a high level event occur then IDS first analyze it and then counter measures are taken and details are stored. An IDS performs different functions :
  1. It monitors the user and system activities.
  2. It audits the system configuration for the vulnerabilities and misconfiguration.
  3. It also corrects the system configuration errors.
  4. IDS also manage the audit trail.
  5. By using the statistical analysis, it identifies the abnormal activities.
  6. It accesses the integrity of critical system and data files.
  7. It identifies the known attack pattern in the system.

4.6.1(A) Types of IDS

The main types of Intrusion detection system are :

1. Network based Intrusion Detection System
2. Host based Intrusion detection System
3. Protocol-based Intrusion Detection System
4. Application Protocol-based Intrusion Detection System
5. Hybrid Intrusion Detection System

1. Network based Intrusion Detection System :

A network-based IDS consists of network devices with a network Interface Card (NIC) which is operated in promiscuous mode and a separate management interface. It does analysis for traffic on a whole subnet and makes a match to the traffic passing by to the attack already known in a library of known attacks.

2. Host based Intrusion detection System :

A host-based IDS is a software application which is usually installed on a system. This application monitors activities only of that local system. It doesn't have any knowledge of low-level network traffic since it directly communicates with operating system. Mostly these IDS rely on information they get from audit and system log files to detect intrusion. Some host-based IDS also monitor system files and system resources, and incoming applications.

3. **Protocol based Intrusion Detection System :** A protocol-based intrusion detection system includes a system that would constantly reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. This IDS tries to secure the web server by repeatedly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is unencrypted and before immediately entering its web presentation layer then this system would necessitate residing in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System :** An application Protocol-based Intrusion Detection System is a system that usually resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols.
5. **Hybrid Intrusion Detection System :** A hybrid intrusion detection system is prepared by the combination of two or more approaches of the IDS. In the hybrid intrusion detection system, host system data is combined with network information to build up a complete view of the network system. Hybrid intrusion detection system is more efficient in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

4.6.1(B) IDS Advantages and Disadvantages

IDS are evolving products. However, IDS mechanism continues to change as new research influences the design of the products.

Advantages

1. IDS recognize a constantly developing number of difficult issues. Furthermore, as we take in more about issues, we can add their signature to the IDS model. Subsequently, after some time, IDS proceed to improve. In the meantime, they are getting to be less expensive and simpler to control. IDSs are excellent addition to a network security.
2. Firewall part traffic to specific ports or addresses; they additionally compel certain protocols to restrict their effect. Firewalls need to permit some traffic to enter a protected zone. Watching what that traffic really does inside the protected region is an IDS's task.

Disadvantages

1. Avoiding IDS is dependably a first need for fruitful attackers. An ID that is not very much protected is futile. However, the stealth mode IDSs is troublesome even to discover on an inside network, IDS search for known shortcomings. Similar IDSs might have indistinguishable vulnerabilities, and their selection criteria might miss similar attacks.
2. Sensitivity is additionally the restriction of IDS, which is hard to guess and adjust. IDSs will never be flawless, so finding the best possible balance is critical.
3. IDD's does not run itself, somebody needs to monitor its record and react to its alarm.

4.6.2 Role of IDS in Attack Prevention

Intrusion detection systems monitor network traffic in order to detect when unauthorised entities are carrying out an attack. IDSes accomplish this by providing security professionals with some or all of the following functions :

- Other security controls aimed at detecting, preventing, or recovering from cyber attacks; monitoring the operation of routers, firewalls, key management servers, and files that are required by other security controls;
- Allowing administrators to tune, organise, and comprehend relevant os audit trails and other logs that would otherwise be difficult to track or parse;
- Providing a user-friendly interface so that non-expert employees can assist with system security management;
- Including a large attack signature database against which the system's data can be compared;
- When the ids detect that data files have been altered, it recognizes it and reports it;
- Alarming and informing the user that security has been breached; and
- Defending against intruders by blocking them or the server.

Review Questions

Q. 1 What is network forensics?

Q. 2 Explain Evidence Collection and Acquisition in network forensics.

Q. 3 What are network based evidence?

Q. 4 Explain the steps in router investigation.

Q. 5 Explain Analysis of network evidences in router.

Q. 6 List and explain Challenges in network forensics

Q. 7 Explain Tools used in network forensics.

❑❑❑

5 Mobile Forensics

Syllabus

Introduction, Evidence Collection and Acquisition, Analysis of Evidences, Challenges in mobile forensics, Tools used in mobile forensics

Self Learning Topics : Tools / Techniques used in mobile forensics.

Topics

5.1 Introduction

5.2 Evidence Collection and Acquisition

5.3 Analysis of Evidences

5.4 Challenges in Mobile Forensics

5.5 Tools used in Mobile Forensics

5.6 Self-Learning Topics : Tools / Techniques used in Mobile Forensics

5.1 Introduction

- Cell phone and mobile device forensics is a fast-changing field as maximum work is done by mobile device.
- In cell phone people save lots and lots of data, so if in case you lose your mobile phone, the data stored in the cell phone also get lost and it may be used for wrong purposes. It is observed that many people do not secure their cell phones, though they regularly lock and secure laptops or desktops.
- Now a day's maximum transactions are done via mobile like people log into their bank accounts and transfer the funds and perform other banking work. Your mobile phone contains the following information :
  - Incoming calls, outgoing calls, and missed calls
  - Text and Short Message Service (SMS) messages
  - E-mail
  - Instant Messaging (IM) logs like messenger and whatsapp messaging
  - Web pages
  - Photos and videos
  - Personal calendars
  - Address books
  - Songs
  - Voice recording
  - Banking details.
- Now a day's maximum people are storing more information on their cell phones than the computers, and it is resulting in crimes or cases. Recent days the mobile phone data is used in many cases as evidence. But it is very challenging to investigate the cell phones and mobile devices in computer forensics.
- The following are the challenges while investigating the mobile devices and cell phones :
  1. For storing the message no single standard id exist although many of the phones use same storage scheme.
  2. As technology is changing new phones are coming in the market about every 5 to 6 months and they are merely compatible with the previous model of the phone. In near future the cables and accessories may become obsolete in a short time.
  3. As cell phones are often combined with PDAs, which can make forensics investigations more complex.

5.1.1 Mobile Phone Basics

- In 1970, Motorola introduced cell phones, and it is developed rapidly. There were 3 generations of the mobile phones till 2008, and they are : analog, digital Personal Communications Service (PCS), and third-generation (3G).
- 3G gives the increased bandwidth, as compare to analog and PCS. It gives 384 Kbps for pedestrian use, 2 Mbps in fixed locations, such as office buildings and 128 Kbps in a moving vehicle.
- Digital networks for mobile phones :

1. Code Division Multiple Access (CDMA)
2. Global System for Mobile Communication (GSM)
3. Time Division Multiple Access (TDMA)
4. Integrated Digital Enhanced Network (IDEN)
5. Digital Advanced Mobile Phone Service (D-AMPS)
6. Enhanced Data GSM Environment (EDGE)
7. Orthogonal Frequency Division Multiplexing (OFDM)

1. Code Division Multiple Access (CDMA)

- CDMA is developed by Qualcomm. To define the channels CDMA uses complete radio frequency spectrum. Sprint and Verizon uses the CDMA networks.
- Many of the CDMA networks match to IS-95, which is created by the TIA (Telecommunications Industry Association). These systems are known as CDMA One, and when they go to 3G services, they will become CDMA2000.

2. Global System for Mobile Communication (GSM)

- GSM is used by AT&T and T-mobile. It is a standard in Asia and Europe.
- It uses Time Division Multiple Access (TDMA) technique, thus many phones get turns sharing a channel, a lot like token ring networks.

3. Time Division Multiple Access (TDMA)

- The TDMA network divides a radio frequency into timeslots. GSM also uses the same techniques. TDMA refers to the IS-136 standard, which introduced sleep mode to enhance battery life.
- TDMA can work in the cell phone with frequency 800 MHz to 1000 MHz) or PCS (1900 MHz) frequency, as a result it is compatible with a number of cell phone networks.

4. Integrated Digital Enhanced Network (IDEN)

It is a Motorola protocol which combines various services including data transmission, into one network.

5. Digital Advanced Mobile Phone Service (D-AMPS)

D-AMPS is a digital version of original analog standard for cell phone.

6. Enhanced Data GSM Environment (EDGE)

- EDGE digital network is used to deliver data and it is a faster version of GSM. It is specially designed for 3G.
- The 3G standard is developed by the International Telecommunication Union (ITU). It's compatible with CDMA, TDMA, and GSM.

7. Orthogonal Frequency Division Multiplexing (OFDM)

OFDM technology for 4G network utilizes energy more efficiently than 3G networks. It is more immune to inference.

4G networks can use the following technologies :

1. Orthogonal Frequency Division Multiplexing
2. Mobile WiMAX
3. Ultra Mobile Broadband (UTMS)
4. Multiple Input Multiple Output (MIMO)
5. Long Term Evolution (LTE)

1. Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing (OFDM) this techniques uses radio waves broadcast over dissimilar frequencies it uses power more resourcefully, and is more resistant to interference.

2. Mobile WiMAX

- This technology supports transmission speeds of 12Mbps. It is chosen by Sprint for its 4G network.
- This technology uses the OFDMA and IEEE 802.16e standard.

3. Ultra Mobile Broadband (UTMS)

- CDMA network provider use this technology to switch to 4G and to support the transmission speed of 100 Mbps.
- This technology also known as CDMA2000 EV-DO.

4. **Multiple Input Multiple Output (MIMO)**

- Airgo developed this technology and Qualcomm acquired it.
- It is expected to support 312 Mbps transmission speeds.

5. **Long Term Evolution (LTE)**

- LTE technology supports the transmission speed of 45 Mbps to 144 Mbps and is designed for UMTS and GSM technology, is expected to support 45 Mbps to 144 Mbps transmission speeds.
- The main components used for communication with these cells are : BTS, BSC and MSC.

(i) Base Transceiver Station (BTS)

- BTS is made up of radio transceiver equipment.
- It describes cells and communicates with mobile phones.

(ii)Base Station Controller (BSC)

- BSC is a combination of hardware and software.
- BSC manages BTSs and allots channels by connecting to the mobile switching center.

(iii) Mobile Switching Center (MSC)

- MSC connects calls by routing digital packets for the network and relies on a database to support subscribers.
- This central database has location data, account data, and other key information needed during an investigation. To access information from a carrier's central database warrant or subpoena is needed.

5.1.2 Inside Mobile Devices

- The hardware the Mobile devices consists of is ROM, RAM, a microprocessor, a digital signal processor, a microphone and speaker, a radio module, hardware interfaces (for example, cameras, keypads, and GPS devices), and an LCD display, removable memory cards (in some mobile), Bluetooth and Wi-Fi, Operating system (such as, Linux, Windows Mobile, Android, RIM OS, Palm OS, Symbian OS, Mac OS X).
- Usually, data is stored in the phone electronically Erasable Programmable Read-Only Memory (EEPROM).
- It allows the service providers to reprogram phones without accessing memory chips physically. Many users take advantage of this facility and reprogram their phone to add new features or switch to different service providers.

SIM Cards

- Subscriber Identity Module (SIM) cards are used in GSM devices and consist of a microprocessor and 16 KB to 4 MB EEPROM or more than that. SIM cards are like to standard memory cards, but the connectors are associated differently.
- To find the SIM card, open the panel covering GSM. GSM refers to mobile phones as mobile stations.
- The mobile station is divided into two parts : The SIM card and the Mobile Equipment (ME), which is the remainder of the phone. The SIM card is needed for the mobile equipment to work and serves these following additional purposes :

  To identify the subscriber to the network.

  - To store personal information.
  - To store address books and messages.
  - To store service-related information.
- You will get SIM cards in two sizes. The most standard size is 0.75 mm thick. SIM card is portable; simply by switching a SIM card between compatible phones, you can move your information to another phone.
- If you are travelling to neighboring countries then you have two SIM cards, one for your country and other is for foreign country, you can easily switch to new SIM card.

Inside PDAs

- Personal Digital Assistants (PDAs) are separate devices from mobile phones. The majority users carry them in place of a laptop to keep track of appointments, deadlines, address books, and so forth.
- Most of the PDAs have integrated phones. PDAs consists of RAM, microprocessor, flash ROM, and a variety of hardware components. You can retrieve the user's calendar, address book, Web access, and other items from PDA's.

  PDA's uses many peripheral memory cards :

  (i) Compact Flash (CF) : These cards are used for extra storage and work .

  (ii) Multi Media Card (MMC) : These cards are designed for mobile phones, but you can use with PDAs to give another storage area.

  (iii) Secure Digital (SD) : These cards are like MMCs, only extra security features are added to protect data.

5.2 Evidence Collection and Acquisition

- It is important to have proper search and seizure procedures for cell phones. The main fear with mobile devices is loss of power and synchronization with PCs. As all the mobile devices have volatile memory, so ensure that you retrieve the RAM data before the power off.
- If you are investing a scene then specify that mobile device is on or off. If the device is off then connect the charger as soon as possible or if it is on then check the LCD display for the battery's current charge level.
- As you know mobile devices are connected to the PC via cable cradle station should be disconnected immediately from the PC. It helps to prevent automatic synchronization that might occur on a fixed schedule and overwrite data on the device.
- Additionally, collect the PC and any peripheral devices that determine whether the hard drive consists of any information that's not on the mobile device.
- Based on the warrant, the time of seizure may be relevant. It may be possible that messages may be received after seizure that may or may not be admissible in court. If you are turning of the device to protect the battery power or attacks then note down the date and time when you have taken this step.
- The solution is to isolate the device from incoming signals by using any one of the following options :
  - Put the device in a paint can, preferably one that previously contained radio wave- blocking paint.
  - Make the use of the Paraben Wireless Stronghold Bag.
  - Make the use of eight layers of antistatic to block the signal.
- The disadvantage of using isolating options is that the mobile device is put into roaming mode, which speed ups battery drainage. The solution to this is using portable mean of power, like a battery-powered charger. Some mobile phones or devices shut themselves off or enter a "sleep state" after reaching a certain low battery level.
- In the forensic lab when you come back then you have to assess what can be retrieved. You have to check following 4 areas for critical information :
  - The SIM card
  - The internal memory
  - Any removable card or external memory cards
  - The system server.
- For checking the system server warrant is required, so to check the voicemail you need warrant. Help from service provider is also needed to discover the time of a call, to access backups of address books, and other.

- On mobile device, there is both, volatile and non-volatile memory available for storage. Volatile memory needs power to preserve its contents, but non-volatile memory does not.
- Though the exact locations of data differ from one phone model to the next, volatile memory typically contains frequently changed data like missed calls, text messages, and at times even user files. Non-volatile memory contains OS files and stored user data, for example, backed-up files and a Personal Information Manager (PIM).
- As you know memory resides in the phone itself and in the SIM card, if the device is equipped with one. SIM card's file structure is hierarchical structure. This file structure starts with the root of the system (MF).
- In the next level there are Directory Files (DF) and under DF there are files which contain elementary data (EF). In the Fig. 5.2.1, the EFs in the GSM and DCS1800 DFs have network data on different frequency bands of operation. The EFs in the Telecom DF contain service related data.

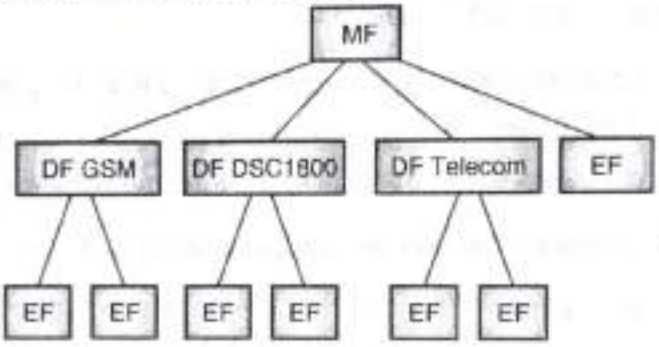


Fig. 5.2.1 : SIM file structure

- From SIM card you can recover moderately a little of data. The recovered information falls into four categories :
  - Service-related data, for example identifiers for the SIM card and subscriber.
  - Call data, like dialed numbers
  - Message information
  - Location information
- If power is lost, you require PINs or other access codes to view files. normally, users keep the original PIN assigned to the SIM card, so while collecting evidence at the scene, seek users' manuals and additional documentation that can help you access the SIM card. In many SIM cards you have 3 attempts of entering an access code before the device is locked, else you need to call the service provider or you have to wait for a certain amount of time before trying again.

Mobile Forensics

- In mobile forensics the biggest challenge is constantly changing models of cell phones and what works with the current cell phone model will not work with upcoming model.

- Like computer forensics we cannot recover deleted files in mobile forensics. In mobile forensics usually you are performing two tasks :

  (a) By synchronizing PC with the device

  (b) Reading the SIM card.

- The first step in mobile forensic is to identifying the mobile device. Many users do not change their device, but some users don't alter their devices, but some file off serial numbers, modify the display to show deceptive data, and so on.
- There are many online sources available to identify the phone, for example, www.phonescoop.com, www.cellphoneshop.com, and www.mobileforensicscentral.com.
- Second step is to ensure that mobile device software is installed on your forensic machine. Keep in mind that not all the services are equipped with the required software because many tools are expensive.
- Some tools simply take pictures of screens as you scroll through them. Forensically, translation it is not a good approach, but if no other alternative is available then you can use it.
- Third step is to attach the phone to its power supply and connect the correct cables. Use rig cables to connect to devices as cables for the model you're investigating may or may not be available.
- Lastly, after connecting the device, start the forensics program and start downloading the available information.

SIM Card Readers

With mobile devices, next step is to access SIM card using the hardware/ software device called a SIM card reader. To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you are ready to proceed to this step. The general procedure is as follows :

1. Take out the back panel of the device.
2. Take out the battery.
3. Under the battery, take out the SIM card from its holder.
4. Now into the card reader insert the SIM card.

Problems with SIM card Reader

1. To understand the data collection procedure or cell phones and mobile devices. There are many different types of SIM card readers available in market. Some SIM card readers are forensically sound and some are not; note down this feature of the device in your investigation log.

2. Second problem is related to the text and SMS messages. It is very difficult to document the unread message. In such situation use a tool that takes pictures of each screen can be important in this situation. These screen captures can provide extra documentation.

5.2.1 Evidence Acquisition

The ways in which data is retrieved from a mobile device are referred to as the acquisition phase of mobile forensics. Because evidence on mobile devices is so perishable, it's critical that appropriate techniques be used to collect it, regardless of the acquisition method. The following are the types of acquisition :

1. Manual acquisition

- The examiner investigates the contents of the phone's memory using the user interface. As a result, the device is used normally, with the examiner photographing the contents of each screen. This method has the advantage of not requiring the use of specialised tools or equipment to convert raw data into human-interpretable information due to the operating system.
- This method is commonly used with cell phones, PDAs, and navigation systems. The process is time-consuming, and only data visible to the operating system can be recovered. Additionally, all data is only available in the form of pictures.

2. Logical acquisition

- A bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical storage device is referred to as logical acquisition (e.g., a file system partition). The advantage of logical acquisition is that system data structures are easier to extract and organise for a tool.
- Using the original equipment manufacturer application programming interface for synchronising the phone's contents with a personal computer, logical extraction obtains information from the device. Because it does not produce a large binary blob, a logical extraction is generally easier to work with. A skilled forensic examiner, on the other hand, will be able to get far more information out of a physical extraction.

File system acquisition

- Due to the fact that deleted data is normally removed from the phone's file system, logical extraction rarely produces any deleted data. However, in some cases particularly with SQLite-based platforms like iOS and Android the phone may keep a database file of information that does not overwrite the data but simply marks it as deleted and available for overwriting later.
- It is possible to recover deleted data in such cases if the device allows file system access through its synchronisation interface. File system extraction is useful for understanding file structure, web browsing history, and app usage, as well as allowing the examiner to use traditional computer forensic tools to perform an analysis.

3. **Physical acquisition**

- Physical acquisition entails a bit-for-bit copy of an entire physical store (e.g. flash memory); as a result, it is the method most closely resembling a computer examination. A physical acquisition has the advantage of allowing for the examination of deleted files and data remnants. Physical extraction obtains data from the device by accessing the flash memory directly.
- This is generally more difficult to achieve because the device's original equipment manufacturer must protect memory from arbitrary reading; as a result, a device may be locked to a specific operator. Mobile forensics tool vendors often create their own boot loaders to get around this security, allowing the forensic tool to access the memory (and often, also to bypass user passcodes or pattern locks). The physical extraction process is usually divided into two stages: the dumping phase and the decoding phase.

4. **Brute force acquisition**

- Third-party passcode brute force tools that send a series of passcodes / passwords to the mobile device can be used to perform brute force acquisition. This is a time-consuming method, but it is still effective. This method employs trial and error to find the best password or PIN combination for authenticating access to a mobile device.
- Despite the fact that the procedure takes a long time, it is still one of the best options if the forensic expert is unable to obtain the passcode. With today's software and hardware, cracking the encryption on a mobile device's password file to obtain the passcode has become relatively simple.

5.3 Analysis of Evidences

- After acquisition the contents of (the HDD) image files are analysed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering (to hide data).
- During the analysis an investigator usually recovers evidence material using a number of different methodologies (and tools), often beginning with recovery of deleted material.
- Examiners use specialist tools (EnCase, ILOOKIX, FTK, etc.) to aid with viewing and recovering data. The type of data recovered varies depending on the investigation; but examples include email, chat logs, images, internet history or documents.
- The data can be recovered from accessible disk space, deleted (unallocated) space or from within operating system cache files.
- Various types of techniques are used to recover evidence, usually involving some form of keyword searching within the acquired image file; either to identify matches to relevant phrases or to parse out known file types.

- Certain files (such as graphic images) have a specific set of bytes which identify the start and end of a file, if identified a deleted file can be reconstructed.
- Many forensic tools use hash signatures to identify notable files or to exclude known (benign) ones; acquired data is hashed and compared to pre-compiled lists such as the Reference Data Set (RDS) from the National Software Reference Library On most media types including standard magnetic hard disks, once data has been securely deleted it can never be recovered.
- SSD Drives are specifically of interest from a forensics viewpoint, because even after a secure-erase operation some of the data that was intended to be secure erased persists on the drive.
- Once evidence is recovered the information is analysed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialist staff. Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon data and their own expert knowledge.

5.4 Challenges in Mobile Forensics

1. True Mobility

Data can be stored, shared, and retrieved from one platform to the next more easily than ever before thanks to today's devices. A document started on a smart phone can be sent to a computer, saved in the cloud, or deleted from a remote location in an instant. The fact that a user has complete control over the data they create or receive can be a major roadblock for investigators.

2. Resetting or wiping

You can see a real-life example of data being unintentionally wiped from a device in the beginning of our lesson. Investigators face the same challenges that you do when you delete a text, lose a calendar appointment, or accidentally delete a contact.

3. Variants in Software and Hardware

Smartphones used to come with one or two operating systems that were installed on three or fou different types of phones. Since the first iPhone was released in 2007, nearly two dozen different iPhone models have been released. That doesn't take into account Android phones, Google phones, Windows phones, and so on. Each of these has its own menus, settings, and features, which can make retrieving data a real pain.

4. Password Security

Many of us use passwords to secure our mobile devices. To help ensure that prying eyes don't access a user's personal data, phones are now equipped with fingerprint sensors and even facial recognition software programmes. Law enforcement faces an inherent challenge as a result of this. Although forensic tools exist to bypass these credentials, this requires additional time and money.

5. Altered Data

Investigators must take great care when gathering evidence to ensure that nothing on a mobile device has been tampered with. The simple act of an investigator turning on a phone that had previously been turned off or opening a smartphone app can cause data to be altered from how it was when the device was recovered. Even if a phone is connected to a cellular or Wi-Fi network, new calls or texts received, as well as apps running in the background, can affect it.

6. Mobile platform security features

Security mechanisms are implemented into modern mobile platforms to secure user data and privacy. These characteristics operate as a stumbling block during forensic collection and evaluation. Modern mobile devices, for example, include built-in encryption methods from the hardware to the software layers. To retrieve data from the devices, the examiner may need to break through various encryption techniques.

7. Lack of resources

As previously said, as the number of mobile phones grows, so will the instruments necessary by forensic examiners. In order to acquire those devices, forensic acquisition accessories such as USB cables, batteries, and chargers for various mobile phones must be kept.

8. Techniques that are anti-forensic

Data concealment, data obfuscation, data fabrication, and secure erasing are anti-forensic tactics that make digital media investigations more difficult.

9. Dynamic nature of evidence

Intentionally or inadvertently, digital evidence can be easily tampered with. Browsing an app on a phone, for example, could change the data stored by that app on the device.

10. Accidental reset

Mobile phones have capabilities that allow you to reset everything. Data may be lost if the device is unintentionally reset while being examined.

11. Modification of the device

Moving programme data, renaming files, and changing the manufacturer's operating system are all feasible ways to change devices. In this scenario, the suspect's knowledge and experience should be considered.

12. Recovering a password

If the device is password-protected, the forensic examiner must acquire access to the device without destroying the data on it.

13. Shielding communications

Cellular networks, Wi-Fi networks, Bluetooth, and Infrared are all used by mobile devices to connect. Because device communication has the potential to modify device data, the prospect of further contact should be ruled out once the device has been seized.

14. Lack of availability of tools

There is a large selection of mobile devices available, so there isn't a shortage of tools. Because a single tool may not be able to support all devices or execute all of the required operations, a combination of tools must be employed. It can be challenging to select the proper tool for a specific phone.

15. Malicious programs

Malicious software or malware, such as a virus or a Trojan, could be present on the device. These malicious programmes may attempt to spread to other devices via a wired or wireless link.

16. Legal issues

Criminals may use mobile devices to commit crimes that traverse national borders. To deal with these cross-jurisdictional concerns, the forensic examiner must understand the nature of the crime as well as regional legislation.

5.5 Tools used in Mobile Forensics

1. The AFLogical OSE

Open-source Android Forensics app and framework is an APK file that must be installed in the Android terminal first. Once the process is complete, various information (call log, contact list, list of installed applications, text messages, and multimedia) can be extracted to the SD card, which must then be recovered either by connecting the card to an external device or using the ADB.

2. Open Source Android Forensics

Open Source Android Forensics is a framework that is distributed as a virtual machine image and includes a number of tools for analysing mobile applications, including static and dynamic analysis, as well as forensic analysis.

3. Andriller

Andriller is a Windows application that combines various forensic utilities. It enables access to a wealth of interesting data, including that relating to social media and messaging apps, among other things (Skype, Tinder, Viber, WhatsApp, etc.).

4. FTK Imager Lite

FTK Imager Lite allows us to analyse and obtain evidence from memory dumps from mobile devices.

5. Now Secure Forensics Community Edition

Now Secure Forensics Community Edition is distributed as a virtual image that combines various tools for performing forensic analysis, and in its commercial version, it can perform various types of evidence extraction and even file carving.

6. LIME

Linux Memory Extractor is a piece of software that allows you to get a volatile memory dump from a Linux-based device, such as an Android phone.

7. Cellebrite Touch

One of the most well-known and comprehensive evidence extraction devices is the Cellebrite Touch. It enables us to work with over 6,300 terminals running the most popular mobile operating systems. It's also very easy to use and understand.

8. Encase Forensics

In addition to Cellebrite, Encase Forensics is a global leader in forensic analysis. It has a variety of features, including one that detects encrypted files and attempts to decrypt them using Passware Kit Forensic, a tool with specific algorithms for this purpose.

9. Oxygen Forensic Suite

Oxygen Forensic Suite can extract data from over 10,000 different mobile device models, as well as from cloud services and import backups or images.

10. MOBILedit

MOBILedit Forensic allows for the receipt of a large amount of data and the execution of advanced operations such as obtaining a complete memory dump, avoiding terminal-locking measures, and creating reports in a flexible manner.

11. The Elcomsoft iOS Forensic Toolkit

The Elcomsoft iOS Forensic Toolkit enables physical acquisition on iOS devices like the iPhone, iPad, and iPod Touch. Other useful features include deciphering the keychain that stores user passwords in the terminal under investigation, as well as registering each action taken throughout the process to keep track of them.

5.6 Self-Learning Topics : Tools / Techniques used in Mobile Forensics

- New approaches for extracting data from a variety of cellular devices are constantly being developed by forensic software applications. Physical and logical extractions are the two most popular methods. JTAG or cable connections are used for physical extraction, whereas Bluetooth, infrared, or cable connections are used for logical extraction.

- For mobile forensics, there are a variety of tools to choose from. There are three types of forensic tools : open source, commercial, and non-forensic. When it comes to interacting with a mobile device, both non-forensic and forensic tools usually use the same methodologies and standards.
- System of Classification for Tools : Forensic analysts must be familiar with a variety of forensic tools. The tools classification system provides forensic analysts with a framework for comparing the data collecting methodologies utilised by various forensic tools. Fig. 5.6.1 demonstrates the system.

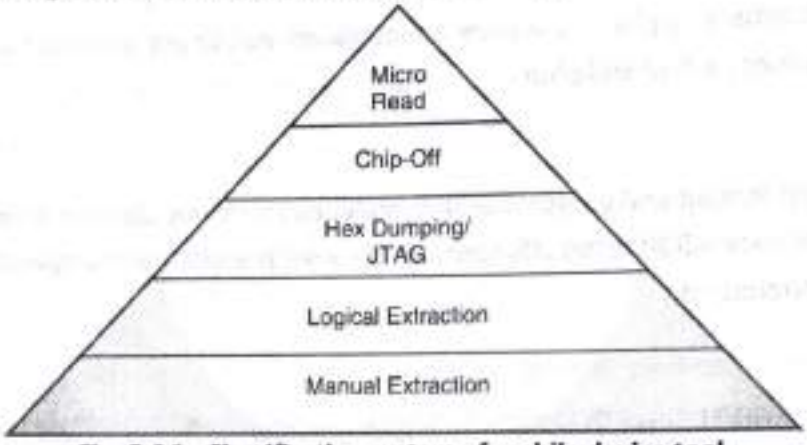


Fig. 5.6.1 : Classification system of mobile device tool

1. Manual extraction

Investigators can extract and view data using the device's touch screen or keyboard using the manual extraction technique. This information is later photographed and documented. Furthermore, manual extraction takes time and is fraught with the risk of human error. During the assessment, for example, the data could be mistakenly destroyed or updated.

The following are some of the most commonly used manual extraction tools :

- Fernico ZRT
- EDEC Eclipse
- Project-A-Phone

2. Logical extraction

The investigators use Bluetooth, Infrared, RJ-45 connection, or USB cable to link the cellular handset to a forensic workstation or hardware. The computer sends a sequence of orders to the mobile device using a logical extraction tool. As a consequence, the necessary information is extracted from the phone's memory and delivered to the forensic workstation for processing. The following are some of the tools that are used for logical extraction :

- Logical Oxygen
- Forensic Suite by XRY
- Lantern

3. Hex dump

A hex dump, also known as physical extraction, extracts the raw image from the mobile device in binary format. The forensic expert attaches the device to a forensic workstation and installs the boot-loader, which tells the device to dump its memory to the computer.

This method is less expensive and provides investigators with more information, including the recovery of deleted files and unallocated space on the phone. The following are some of the most commonly used hex dump tools :

- Pandora's Box
- XACT
- Cellebrite UFED Physical Analyzer

4. Chip-off

Examiners can extract data directly from the cellular device's flash memory using the chip-off approach. They take the phone's memory chip out and make a binary image of it. This procedure is pricey and necessitates extensive hardware knowledge. Improper handling may result in physical damage to the chip, rendering the data unrecoverable. Chip-off is commonly done with the following tools and equipment :

- Xytronic 988D Solder Rework Station
- FEITA Digital Inspection Station
- Chip Epoxy Glue Remover
- iSesamo Phone Opening Tool
- Circuit Board Holder

5. Micro read

This procedure entails deciphering and displaying data stored on memory chips. The researchers analyse the physical gates on the chips with a high-powered electron microscope, then transform the gate level into 1s and 0s to find the ASCII code. This is a costly and time-consuming procedure. It also necessitates a thorough understanding of hardware and file systems. For micro reading, there is no instrument accessible.

Review Questions

Q. 1 What is mobile forensics?

Q. 2 Explain evidence collection in mobile forensics.

Q. 3 Explain evidence acquisition in mobile forensics.

Q. 4 Explain analysis of evidences.

Q. 5 What are the challenges in mobile forensics? Explain.

Q. 6 Explain the tools used in mobile forensics.

❑❑❑

6 Report Generation

Syllabus

Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a forensic report.

Self Learning Topics : For an incident write a forensic report.

Topics

6.1 Goals of Reports

6.2 Layout of an Investigative Report

6.3 Guidelines for Writing a Report

6.4 Sample for Writing a Forensic Report

6.5 Self-Learning Topics : For an Incident Write a Forensic Report

6.1 Goals of Report

The investigation will not be effective if the documentation is terrible. A forensic report has to document facts and offer opinions with a style of communication that gives decision-makers with useful, accurate information. In other words, a poorly written report hinders the progress of your case.

Report Goals

- Your report should meet some standards established by the organization. So, it is necessary that your forensic report should achieve the following goals :
  1. Details of the incident should be accurately described.
  2. A report should be understandable to decision-makers.
  3. A report should withstand a barrage of legal examination.
  4. A report should be clear and not open to misunderstanding.
  5. A report should be easily referenced (using paragraph numbers for the report and Bates numbers for attached documents).
  6. A report should Contain all data needed to explain your conclusions.
  7. A report should Offer valid conclusions, opinions, or recommendations when required.
  8. A report should be created in a timely manner.
- When you write a report, that report should meet the given goals and it is a very difficult challenge of doing incident response and computer forensics.

6.2 Layout of an Investigative Report

The main goal of computer forensics is to conduct a structured investigation on a computing device in order to determine what occurred and who was responsible for it, all while maintaining a proper documented chain of evidence in a formal report. A Computer Forensic Report's syntax or template is as follows :

1. Executive Summary
2. Objectives
3. Computer Evidence Analyzed
4. Relevant Findings
5. Supporting Details
6. Investigative Leads

7. Additional subsections, such as Attacker Methodology, User Applications, Internet Activity, and Recommendations

1. Executive Summary

- The Executive Summary section gives the background data of the conditions that realized the requirement for an investigation. The senior management reads translation summary, they do not go into the detailed report. So, this section should include short details (under a page long) i.e. only the things that matter.
- The "Executive Summary" section is used to do the following :
  (i) Take account of who authorized the forensic examination.
  (ii) Describe why a forensic examination of computer media was necessary.
  (iii) List what the significant findings were (in short detail).
  (iv) Include a signature block for the examiner(s) who performed the work.
- Include the full and proper name of the all people who are involved in the case, a name of their employer, job titles, and the dates of initial communications.
- The following are the few examples of significant findings which are the part of an Executive Summary section :
  (i) Three days before to leaving employment, Employee C emailed ten company confidential documents to Company B, a competitor.
  (ii) Employee C did not have authorized access to these documents, but on his computer password cracking tools, along with "cracked" executive user passwords, were found.

2. Objectives

- In some cases, it may happen that the forensic examination may not do the full-scale investigation or fishing expedition when reviewing the contents of the media. The Objective section is used to outline all the tasks that our investigation planned to complete.
- The prepared plan list should be discussed and approved by legal counsel, decision-makers, the client before any forensic analysis. The task list should include the tasks undertaken and the method undertook by an examiner for each task and the status of each task at the end of the report.

3. Computer Evidence Analyzed

In the Computer Evidence Analyzed section, all the collected evidence and their interpretations are introduced. This section gives detailed information about the assignment of evidence tag numbers, media serial numbers, and descriptions of the evidence.

4. Relevant Findings

- The Relevant Findings section gives a summary of the findings of probative value. The answers to the questions are given, like "What related items were found in the investigation?"
- The relevant findings have to list in order of relevance to the case. In this section, findings are described in a logical and organized way. This section gives quick reference needed to high-level decision-makers and it is used at the time of describing the results of the investigation.

5. Supporting Details

- The in-depth analysis of the relevant findings is done in supporting details section. This section outlines how we found the conclusions outlined in the Relative Findings section. This section contains the table of important files with the full pathname, number of files reviewed, results of string searches, Emails/ URLs reviewed, and any other significant information.
- The Supporting Details section is used to outline all the tasks undertook to meet the objectives. In this section, we go into technical depth. It includes charts, tables, and illustrations as it conveys much more than written text.
- Many subsections are also included to meet the outlined objectives. This section is the longest section of our report.
- The supporting details section always starts by giving background details of the actual media analyzed. It is difficult to report the number of files reviewed and the size of the hard drive in human understandable language. So, your client must have to know how much information you wanted to review to arrive at your conclusions.
- The following table shows, how to report the size of the media inspected :

Size	6.8 GB
Files	~9828
Directories	~500

- The geometry of the evidence media is also given in the report. The Table 6.2.1 illustrates it.

Table 6.2.1

Partition	File system	Size	Logical drive
1	FAT32	3.00GB	C:\
2	Extended	12.15GB	N/A
5	NTFS	3.1GB	D:\
6	NTFS	5.6GB	E:\

- We also include a table of string search results in the report. The Table 6.2.2 illustrates it.

Table 6.2.2

Keyword	Number of hits reviewed
pornography	0
Client name	456
Source code	988
Rotation Raja	14

6. **Investigative Leads**

- This section outlines action items that could be carried out to discover additional information related to the investigation. Investigator performs all the outstanding tasks if more time and extra information resources are there.
- The investigative leads section is very critical to law enforcement. It is also necessary to document which is beyond the scope o forensic report for more generating compelling evidence and successful resolution of a case. This section is also important to a hired forensic consultant.
- The investigative leads section suggests the extra tasks that discover the information needed to move on the case. The example of investigative leads is, finding out whether there are any firewall logs that date far enough into the past to give a correct picture of any attacks that took place.

7. **Additional Report Subsections**

- There are numerous additional subsections included in forensic reports.
- The following subsections are useful in specific cases. These subsections are depended on the need and want of the client.

8. **Attacker Methodology**

This section gives the additional briefing to help the reader understand the general or exact attacks performed. This section is useful in computer intrusion cases. Here, you can inspect how the attacks are done and what the bits and pieces of the attacks look like in standard logs.

9. **User Applications**

- It is observed that in many cases the applications present on the system are very relevant, so in this section, we discuss the relevant applications that are installed on the media analyzed.
- Outline where the applications were found and what they do. If you are investigating any system that is used by the attacker then give a title to this section, for example, "Cyber-Attack Tools". This section is used in cases like accounting software on frauds, credit card number generation software on credit card fraud, and image viewing applications on a child pornography.

10. Internet Activity or Web Browsing History

- This section gives the web surfing history of the user of the media analyzed. This section included in administrative cases where an employee all day surfing the web.
- The browser history is also useful to suggest intent, downloads of malicious tools, unallocated space, and online research, downloads of secure delete programs, or evidence-removal type programs that wipe files slack, and temporary files that often harbor evidence very important to an investigation.

11. Recommendations

- Recommendation section gives the recommendation to posture the client to be more prepared and trained for the next computer security incident.
- To reduce or eliminate the risk of incident security we investigated, some host-based, network-based and procedural countermeasures are given to the clients.

6.3 Guidelines for Writing a Report

Report Writing Guidelines

There are following incident reports writing guidelines :

1. Document Investigative Steps Immediately and Clearly
2. Know the Goals of Your Analysis
3. Organize Your Report
4. Follow a Template
5. Use Consistent Identifiers
6. Use Attachments and Appendices
7. Have Co-workers Read Your Reports
8. Use MD5 Hashes
9. Include Metadata

1. **Document Investigative Steps Immediately and Clearly**

   - This step needs discipline and organization for successful report writing. Write everything down in a way that it is understandable to you and others; do not use shorthand or shortcuts. Such unclear notations, incomplete scribbling, or unclear documentation will eventually lead to redundant efforts, forced translation of notes, confirmation of notes, and a failure to comprehend notes by yourself or others.
   - Writing something clearly and concisely at the moment you discover evidence saves time and promotes accuracy. It also ensures that the details of the investigation can be communicated more clearly to others at any moment, which is critical should new personnel become involved or assigned to lead the investigation. This is known as the "write it tight" philosophy.

2. **Know the Goals of Your Analysis**

   - It is important to know what the goals of your examination are before you begin your analysis. It helps to foster a focused report. For law enforcement examiners, every crime has elements of proof. Your report should unearth evidence that confirms or dispels these elements. It means that the more focused your reports are, the more effective they are.
   - While hashing out the objectives of your forensic examination, you should also address issues such as the following :
     - Does the client of your report need a single forensics report for each piece of media examined or a report of the investigation that encompasses all media analyzed?
     - How does the client wish you to communicate your findings : verbally or in written form?
     - How often does the client want a status report of your forensic examination?
     - Should the interim status reports be verbal or written?
     - Which examiner should sign as the provider or author of the forensic report?

3. **Organize Your Report**

   - Write "macro to micro." Organize your forensic report to start at a high level, and have the complexity of your report increase as your audience continues to read it. This way, the high-level executives need to read only the first page or so to get the idea of your conclusions, and they should not need to understand the low-level details that support your claims. Include a table of contents for your longer reports.
   - The table of contents enforces a logical approach to documenting your findings, and it helps the reader understand what your report accomplishes.

4. Follow a Template

Follow a standardized report template. The template makes your report writing scalable, establishes a repeatable standard, and saves time.

5. Use Consistent Identifiers

- In a report, instead of referring to an item in a different way like referring to the same computer as a system, PC, box, web server, victim system, and so on can create confusion. Developing a consistent, unwavering way to reference each item throughout your report is critical to eliminate such ambiguity or confusion. P:\010Comp\Hacking\696-x\ch17.vp Monday, June 23, 2003, 2:09:13 PM Color profile : Generic CMYK printer profile Composite Default screen It is a good idea to create a unique identifier or reference tag for each person, place, and thing (nouns) referred to repeatedly in your report. That label will identify the corresponding item for the remainder of the report.
- For example, if the report is a summary of your forensic analysis of a laptop system belonging to a suspect named John, you could reference the items in capital letters in the following manner : "We performed a forensic duplication to the laptop system belonging to John (JOHN), an employee of ABC Corporation. The system was a Dell laptop, SN 141607, hereafter referred to as the JOHN LAPTOP. An in-depth review of the JOHN LAPTOP revealed ...." We have reviewed expert forensic reports that refer to items in the report as tag 1 or evidence tag 2. Using descriptive labels such as JOHN LAPTOP the reader know precisely which piece of evidence you're talking about.

6. Use Attachments and Appendices

- Use attachments or appendices to maintain the flow of your report. Any information, files, and file fragments that you cite in your report that are over a page long should be included as appendices or attachments. Then, you can include a brief reference to the appendix in the report. For example, you might say, "A printout of the information is included as Appendix A."
- Consider including every file that contributes to your conclusions as an appendix to your report. It is also a great idea to Bates number any files you reference in your report so that every document that you cite in your report has a unique reference number.
- You should also provide an electronic copy of every file or file fragment you cite in your report which is too big or simply impossible to provide in a printed format. For example, large database files, lengthy source code files, and spreadsheets. For this type of reference, we provide an electronic copy instead of the printed copy and call it an eAppendix (electronic appendix).
- Simply burn a CD-ROM that contains all files that we cited in the report, and we append it as the last attachment in the report.

7. **Have Co-workers Read Your Reports**

- Employ other co-workers to read your forensic reports. This helps develop reports that are comprehensible to nontechnical personnel who have an impact on your incident response strategy and resolution. Write your reports at the appropriate level of the client of your report.
- Take into consideration the technical capability and knowledge of your audience. For example, if you are providing a computer forensics report to a nontechnical lawyer, it is a good idea to provide a glossary of terms tailored specifically for that report.

8. **Use MD5 Hashes**

- Create and record the MD5 hashes of your evidence, whether it is an entire hard drive or specific files.
- Performing MD5 hashes for all evidence provides support to the claim that you are diligent and attentive to the special requirements of forensic examination. If your evidence is handled properly and remains tamper-proof, the MD5 hashes calculated for a given set of data will always remain the same. By recording these MD5 values, your audience becomes confident that you are handling the data in the appropriate manner.

9. **Include Metadata**

- Record and include the metadata for every file or file fragment cited in your report. This metadata includes the time/date stamps, full path of the file, the file size, and the file's MD5 sum.
- This will help to remove any ambiguity about which files you reference during testimony. For example, the Table 6.3.1 shows the files cited in the report. Specifically, it provides the file metadata for a Windows IIS web access log found on the C: partition (C:\WINNT\system32\LogFiles\W3SVC3\ex001215.log).

Table 6.3.1

File Created	12/15/00 09:16:26AM
Last Accessed	11/14/01 08:47:11AM
Last Written	04/06/01 04:26:05AM
Logical Size	2,034,833
Hash Value	eb40d0678cd9cdfbf22d2ef7ce093273

- We frequently add a Comment field to our file tables to provide a quick reference and reminder of why we cited the file in the report. It is shown in Table 6.3.2.

Table 6.3.2

File Created	02/14/01 01:24:02AM
Last Accessed	11/14/01 04:41:11AM
Logical Size	208,144
Hash value	25d1ee046ebf4a758148f92cc39a8e7e
Comment	A copy of cmd, exe in a browser accessible directory. The MD5 sum is identical to c:\winnt\system32\cmd.exe.

- When a single report includes data from multiple pieces of media (evidence), we need to include additional data in our file tables. Table 6.3.3 includes an extra row illustrating the source media for the file.

Table 6.3.3

Item :	Foundstone Evidence Tag#1, JOHN LAPTOP		
Directory :	\hda1\var\log		
File Name	Messages		
Creation Date :	N/A	Time :	N/A
Modification Date :	02/04/00	Time :	02:32:42 AM
Access Date :	01/29/00	Time :	09:39:00 AM
File Size :	2,400,995		
MD5 Checksum :	Afdf51b0af89efa754ff646626b55ba0		

- There are chances of complexity to the metadata if the file you are citing was originally contained within a zip file or some other archive file. So in such cases provide the metadata for both the original zip file and the metadata for the cited file contained within that zip file.

6.4 Sample for Writing a Forensic Report

The following is the sample for forensic report writing :

APTITUDE BUSINESS SYSTEMS

Network Security Incident Report

DATE:

SECURITY INCIDENT ID:

OFFICE CODE:

FROM

NAME

DEPARTMENT

PHONE NUMBER

An IT security incident was detected/ observed/ discovered on

Date/Time:

Location:

Priority (1=low, 5=high):

System Identification

System Description:

Software systems involved:

Type of Security Incident:

The nature of this security incident was (choose all that apply):

- Unauthorized access to computing resources
- Unauthorized disclosure or use of personal password
- Improper use of computing resources
- Alteration of data or computer systems
- Other (Explain):

Sensitivity of Data:

- Not sensitive (routine correspondence, little to no strategic value)
- Business Confidential/ Proprietary Data
- Business Sensitive/ Financial Data
- Business Sensitive/ Personnel Data
- Business Sensitive/ Other:

Impact of Security Incident:

The effect of the security violation included the following (check all that apply):

- Not sensitive (routine correspondence little to no strategic value)
- Business Confidential/ Proprietary Data
- Business Sensitive/ Financial Data
- Business Sensitive/ Personnel Data
- Business Sensitive/ Other:

6.5 Self-Learning Topics : For an Incident Write a Forensic Report

Sample Forensics Report

Overview / Case Summary

On April 11, 2011, Paul Ceglia filed an Amended Complaint seeking a share of Facebook. Mr. Ceglia based his claim on a purported contract between Mr. Ceglia and Mark Zuckerberg (the "Work for Hire Document"). In addition, the Amended Complaint included excerpts of purported emails between Mr. Ceglia and Mr. Zuckerberg (the "Purported Emails").

Objectives

- This report is a summary of Stroz Friedberg's findings regarding the authenticity of the Work for Hire Document and the Purported Emails based on its analysis of the media produced by Mr. Ceglia pursuant to data received as part of expedited discovery. This report is not intended to detail each and every aspect of Stroz Friedberg's work in this engagement.
- Evidence Analyzed Pursuant to the Court Order, Stroz Friedberg collected digital media made available by Mr. Ceglia. Stroz Friedberg inspected the data on the following media for analysis according to the terms of the Court-ordered Protocol :
  - A Compaq Presario SR5413WM desktop computer with a 250 gigabyte hard drive.
  - An eMachines ET1161-05 desktop computer with a 160 gigabyte hard drive.
  - A Toshiba Satellite L305-55968 laptop computer with a 320 gigabyte hard drive.
  - A 200 gigabyte Maxtor Personal Storage 3200 external hard drive.
  - A 500 gigabyte Western Digital internal hard drive 174 floppy disks.
- Using widely-accepted digital forensic techniques and procedures, digital forensic personnel from Stroz Friedberg made bit-for-bit, verified forensic copies or images of : the hard drive within the Compaq Presario desktop computer; the hard drive within the eMachines desktop computer; the hard drive within the Toshiba Satellite laptop computer; the Maxtor external hard drive; the Seagate Hard Drive; and 173 of the 174 floppy disks.
- The digital forensic copying process captured the entire contents of each piece of media, including the active user-accessible files, the deleted files, and the unallocated space, which may contain deleted content. Because the forensic image created by Plaintiff's Expert is a forensic image file, Stroz Friedberg used a forensically-sound copy method to copy the forensic image file on that drive to preservation media.

Investigation Steps

- Stroz Friedberg conducted its analysis of the Ceglia media pursuant to the Protocol issued by the Court. Stroz Friedberg searched and analyzed the Ceglia Media "to identify only documents, data, fragments, and artifacts that reasonably appear[ed] to be related to the authenticity of the [Work for Hire Document] attached to the Amended Complaint and the [P]urported [E]mails described in the Amended Complaint".
- The documents, data, fragments, and artifacts found by Stroz Friedberg that reasonably appeared to be related to the authenticity of the Work for Hire Document or the Purported Emails first were produced to Mr. Ceglia's attorneys for a privilege review.
- The material was turned over to attorneys from Gibson Dunn only if no privilege objection was raised, an asserted privilege objection was withdrawn by Mr. Ceglia or his attorneys, or an assertion of privilege was overruled by the Court. Stroz Friedberg has followed the terms of the Protocol for all data found on the Ceglia Media and any other data subject to the Protocol during its analysis, including the procedures for privilege review and production set forth above and the maintenance of a search log.
- During this analysis, Stroz Friedberg employed a methodology tailored to the particular facts of this case. Stroz Friedberg's methodology included : (1) conducting keyword and other searches of the digital forensic copies of the Ceglia Media and other data, including webmail accounts, to identify responsive documents or fragments of documents; (2) manually reviewing the documents containing keyword hits, certain unsearchable file types, such as image files with no text, and other documents to determine whether they were relevant to the authenticity of the Work for Hire Document or the Purported Emails; and (3) reviewing the digital forensic copies of the Ceglia Media for digital forensic artifacts relevant to the authenticity of the Work for Hire Document or the Purported Emails.

Findings

- No exact copies of the Work for Hire Document were found on the Ceglia Media, which comprised hundreds of pieces of media - including computers, hard drives and floppy disks. Stroz Friedberg used a methodology that would have identified any copies of the Work for Hire Document on the Ceglia Media if they had been present. Instead of the purported Work for Hire Document, Stroz Friedberg found on the Ceglia Media seven unsigned versions of the Work for Hire Document that are very similar but not identical to the purported Work for Hire Document.
- All seven of those electronic documents contain metadata anomalies indicative of backdating and document manipulation. Mr. Ceglia's Amended Complaint purports to quote from or otherwise reference 22 Purported Emails between Mr. Ceglia and Mr. Zuckerberg. During the litigation, Mr. Ceglia acknowledged that he did not keep the Purported Emails referenced in the Amended Complaint in their original native form, that is to say, as individual files in message format. Rather, he claimed to have copied-and-pasted the text of the Purported Emails into Microsoft Word documents saved to floppy disks in order to maintain copies of these messages.

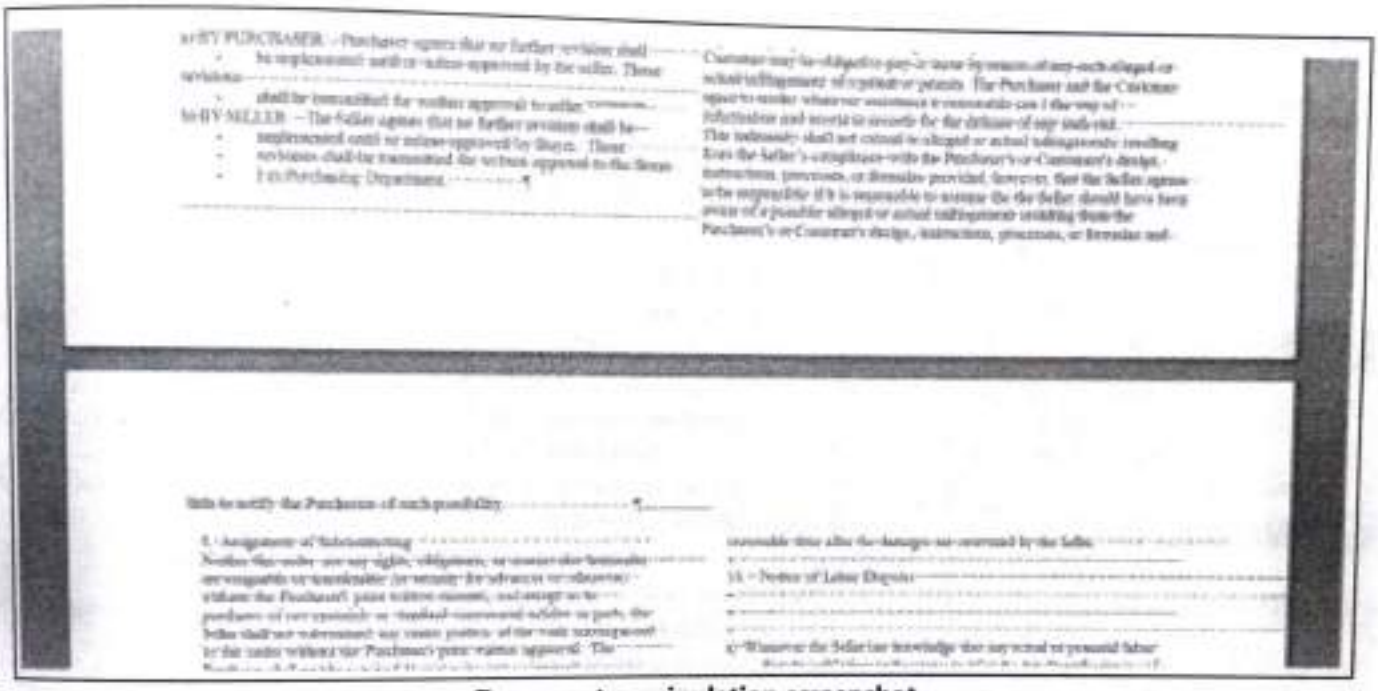
- Stroz Friedberg found substantial evidence that all three of the Word documents containing the purported emails are backdated. The effect of backdating is to obscure the true date and time at which computer activity, such as the creation or modification of documents, occurred. Backdating can be accomplished by setting the system clock on a computer hard drive to an earlier date, such that activity that occurs on the hard drive while the computer is in a backdated state will appear to have occurred at that earlier time.
- Moreover, the last printed date of the document is February 15, 2011, while the document's last modified date is April 25, 2003. As discussed above, absent backdating or manipulation of the system clock, it is not possible for a file's last printed date to post-date its last modification date. Therefore, this document was fabricated on or after February 15, 2011. This date is years after the Work for Hire Document was allegedly signed and months after Mr. Ceglia filed this lawsuit.

Conclusion

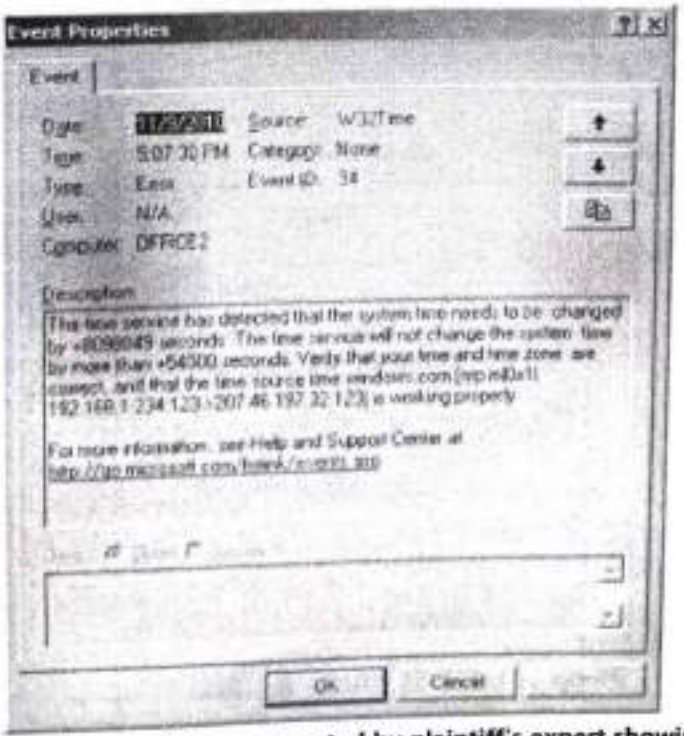
- Stroz Friedberg found direct and compelling digital forensic evidence that the documents relied upon by Mr. Ceglia to support his claim are forged. Stroz Friedberg also found what it believes to be the authentic contract between Mr. Ceglia and Mr. Zuckerberg. That contract contains no references to Facebook. As described more fully in this report, Stroz Friedberg made the following findings bearing on the authenticity of the Work for Hire Document and the Purported Emails : Stroz Friedberg did not find any exact copies of the Work for Hire Document on the hundreds of pieces of media produced by Mr. Ceglia, including three computers, three hard drives, 174 floppy disks, and 1,087 CDs (hereinafter, the "Ceglia Media"). Stroz Friedberg did find a signed copy of an April 28, 2003 contract between Mr. Ceglia and Mr. Zuckerberg, though it concerns only Mr. Zuckerberg's work on the StreetFax project and includes no references to Facebook.
- Stroz Friedberg identified seven unsigned electronic documents on the Ceglia Media that are variants of the Work for Hire Document. All of these electronic documents were backdated to appear as if they were created at earlier dates. They appear to be part of an effort to create a fraudulent contract. Stroz Friedberg did identify the Microsoft Word documents into which Mr. Ceglia claims to have copied-and-pasted the text of the Purported Emails. All of these Word documents were backdated to appear as if they were created at earlier dates.
- The Purported Emails themselves, which Mr. Ceglia has proffered as authentic communications with Mr. Zuckerberg, are fabricated. Many of the Purported Emails reflect the wrong time zone. For example, all of the Purported Emails purportedly sent from October 26, 2003 to April 4, 2004 contain the "-0400" time zone stamp that reflects Eastern Daylight Time. However, Eastern Daylight Time was not in effect during this time. There is no place in the Continental United States from which Mr. Ceglia could have sent these Purported Emails with an accurate "-0400" time zone stamp. The Purported Emails have formatting differences in the email headers that are inconsistent with Mr. Ceglia's explanation that he copied-and-pasted the emails into Word documents.

- These formatting differences indicate that the Purported Emails were typed or edited manually and were not solely the result of a copy-and-paste operation. There is no digital forensic evidence on the Ceglia Media supporting a conclusion that the Work for Hire Document or the Purported Emails are authentic documents dating from 2003 and 2004. To the contrary, the digital forensic evidence strongly indicates that these documents were fabricated by Mr. Ceglia at a later date.

Exhibits :



Document manipulation screenshot



System event log from forensic image created by plaintiff's expert showing backdating.

Review Questions

Q. 1 What are the goals of report ?

Q. 2 Explain the report writing guidelines ?

Q. 3 Explain template for computer forensic report ?

❑❑❑