Chapter 4

ETHICAL HACKING

4.1 CONCEPT OF HACKING AND TYPES OF HACKERS

- INTRODUCTION - HACKING
- TYPES OF HACKING
- TYPES OF HACKERS

4.2 BASICS OF ETHICAL HACKING

- WHAT IS ETHICAL HACKING?
- WHY ETHICAL HACKING?

4.3 HACKING TERMINOLOGIES

- BASIC HACKING TERMINOLOGIES
- VULNERABILITY, EXPLOIT, 0-DAY

4.4 STEPS OF HACKING PROCESS

- SECURE SOCKET LAYER
- TRANSPORT LAYER SECURITY

4.5 INFORMATION GATHERING

- INTRODUCTION - RECONNAISSANCE
- ACTIVE RECONNAISSANCE
- PASSIVE RECONNAISSANCE

4.6 INTRODUCTION TO KALI LINUX OPERATING SYSTEM

- INTRODUCTION – KALI LINUX OS
- INSTALLATION AND CONFIGURATION OF KALI LINUX OS
- BASIC COMMANDS IN KALI LINUX
- VULNERABILITY SCANNING
- VULNERABILITY BASED HACKING

4.7 PORT SCANNING

- WHAT IS PORT SCANNING?
- PORT SCANNING TECHNIQUES

4.1 CONCEPT OF HACKING AND TYPES OF HACKERS

4.1.1 Introduction

There are various definitions of the hackers in the literature of computer world. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. Originally the term was used to describe someone who could be a great programmer and had the ability to solve complex problems.

But now a days the term hacker refers as someone who finds loopholes and tries to gain access into the system to steal information that could be important for the victims. This is the negative aspect, but there is also a positive aspect. The positive aspect is that hackers are the people who exposes the vulnerabilities in the system and by this way protects organizations and multiple users.

Thus, ***"Hacking is an activity done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer."***

The computer experts who do the activity of hacking are known as **hackers.**

4.1.2 Types of Hacking

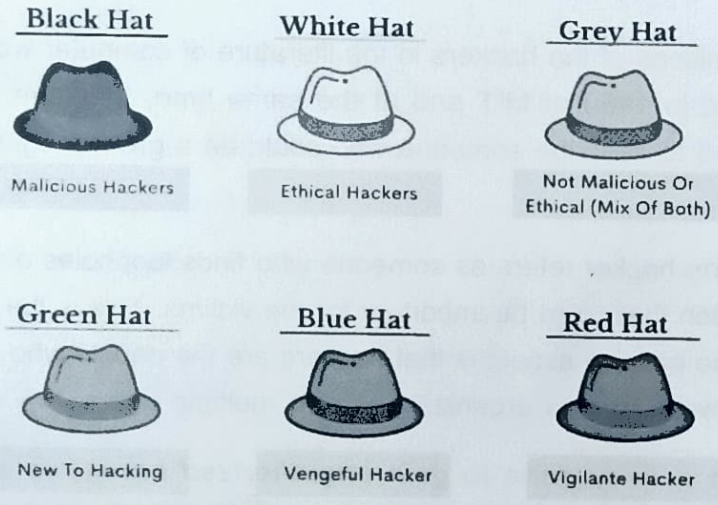
We can classify hacking into different categories, based on what is being hacked. These categories are as under:

- **Password Hacking** – This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** – This is the process of stealing login credentials of computer system like login ID and password by applying different hacking methods and getting unauthorized access to a computer system.

- **Network Hacking** – The word Network hacking refers to the gathering of information about a computer network by using network management and administration tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. using this information take the control over network with the intent to harm the network system and hamper its operation.
- **Website Hacking** – Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Email Hacking** – It includes getting unauthorized access on an Email account and using it without taking the consent of its owner. It may be also used to get other financial aids.
- **Ethical Hacking** – Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

4.1.3 Types of Hackers

Based on their intent of hacking a system, Hackers can be classified into different categories such as white hat, black hat, and grey hat hackers.



[Fig. 4.1 : Types of Hackers – Based on Intent]

- **Whites hat Hackers**

White hat hackers (sometimes also called ethical hackers). They employ their technical expertise to defend the planet against malicious hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

White hats are employed by businesses and government agencies as data security analysts, researchers, security specialists, etc. White hat hackers, with the permission of the system owner and with good motives, use the same hacking tactics that the black hackers use.

- **Black hat Hackers**

They are also known as crackers and always have a malicious motive and gain illegal access to computer system, networks and websites. The main goal of black hat hackers is getting financial gain like money loundering by stealing secret organizational data, stealing funds from online bank accounts, violating privacy rights, damaging the system, blocking network communication etc. In today's world, the majority of hackers fall into this category.

- **Grey hat Hackers**

Grey hat hackers are combined concept of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Apart from the above well-known categories of hackers, we have the following categories of hackers based on what they hack and how they hack.

1. **Red Hat Hackers**

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

2. **Blue Hat Hackers**

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term Blue Hat to represent a series of security briefing events.

3. **Elite Hackers**

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

4. **Script Kiddie**

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

5. **Neophyte**

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

6. **Hacktivist**

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial of-service attacks.

4.2 BASICS OF ETHICAL HACKING

4.2.1 What is Ethical Hacking?

Ethical Hacking is about identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

4.2.2 Why Ethical Hacking ?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.
- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

4.3 TERMINOLOGIES USED IN ETHICAL HACKING

4.3.1 Basic Hacking Terminologies

- **Adware** – Adware is software designed to force pre-chosen ads to display on your system.
- **Attack** – An attack is an action that is done on a system to get its access and extract sensitive data.

- **Back door** – A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.
- **Bot** – A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- **Botnet** – A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.
- **Brute force attack** – A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.
- **Buffer Overflow** – Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.
- **Clone phishing** – Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- **Cracker** – A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- **Denial of service attack (DoS)** – A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- **DDoS** – Distributed denial of service attack. In these types of attack instead of using single computer system for attack, an attacker uses multiple computer systems for attack. So, this kind of attack is more difficult to detect than simple DOS attack.
- **Firewall** – A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.
- **Keystroke logging** – Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/ human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- **Logic bomb** – A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.
- **Master Program** – A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

- **Phreaker** – Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines.
- **Rootkit** – Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
- **Shrink Wrap code** – A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.
- **Social engineering** – Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.
- **Spam** – A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.
- **Threat** – A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.
- **Spoofing** – Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- **Spyware** – Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- **Cross-site Scripting** – Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.
- **Zombie Drone** – A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

4.3.2 Vulnerability, Exploit, 0 – Day

- **Vulnerability** – A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

  These hackers can gain illegal access to the systems and cause severe damage to data privacy. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

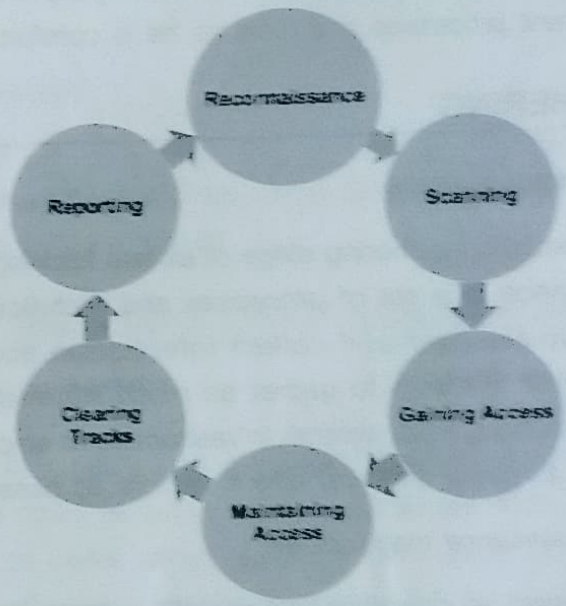
  The common source point for vulnerabilities are Misconfigurations, Unsecured APIs, Outdated or Unpatched Software, Zero-day Vulnerabilities, Weak or Stolen User Credentials, Access Control or Unauthorized Access, etc....

- **Exploit** – Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
- **Exploit Kit** – An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.
- **Zero-day Vulnerabilities** – A zero-day vulnerability refers to a security flaw that has been discovered by a threat actor but is unknown to the enterprise and software vendor. The term "zero-day" is used because the software vendor was unaware of their software vulnerability, and they've had "0" days to work on a security patch or an update to fix the issue. Meanwhile it is a known vulnerability to the attacker.

  Zero-day attacks are extremely dangerous for companies because they can be very difficult to detect.

4.4 STEPS OF HACKING PROCESS

Ethical hacking process is carried out with the number of phases. It helps hackers to make a structured hacking attack. Ethical hacking process can be described in different way, but here the ethical hacking process is explained with six phases as depicted in the below figure 4.2.



[Fig. 4.2 : Six phases of Hacking Process]

- **Reconnaissance (Information Gathering)**

  This is the first phase of Hacking process. During this phase the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

- **Scanning**

  During the scanning phase, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

- **Gaining Access**

  This procedure finds the vulnerability, which you then try to leverage to get access to the system. Metasploit is the main tool utilized in this process.

- **Access Maintaining**

  It is the procedure by which a hacker has previously entered a system. Once inside, the hacker installs backdoors so that, should the necessity arise in the future, he may re-enter the system. The recommended tool for this process is Metasploit.

- **Clearing Tracks**

  In actuality, this procedure is unethical. The removal of all activity logs from the hacking process is the reason for it.

- **Reporting**

  The final step in the ethical hacking is reporting. Here, the ethical hacker gathers information about the work completed, including the tools used, success rate, vulnerabilities discovered, and exploit procedures, and reports it with his results.

  The above-described process is not a standard. Different people can use different approach. One can use a set of different processes and tools as he is comfortable with it.

4.5 INFORMATION GATHERING

4.5.1 Introduction - Reconnaissance

Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

Data collected from reconnaissance may include:

- **Security policies**. Knowing an organization's security policies can help you find weaknesses in their system.
- **Network infrastructure**. A hacker needs to know what type of network the target is using (e.g., LAN, WAN, MAN), as well as the IP address range and subnet mask.
- **Employee contact details**. Email addresses, phone numbers, and social media accounts can be used to launch social engineering attacks.
- **Host information**. Information about specific hosts, such as operating system type and version, can be used to find vulnerabilities.

The reconnaissance process is generally carried out with below steps:

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

Reconnaissance takes place in two ways: Active Reconnaissance and Passive Reconnaissance

4.5.2 Active Reconnaissance

During this procedure, you will be interacting directly with the targeted computer system in order to obtain information. The data collected with this approach may be accurate and pertinent. However, if you are planning active reconnaissance without authorization, you run the danger of being discovered. The system administrator may take harsh measures against you and monitor your future actions if they find you.

4.5.3 Passive Reconnaissance

During this procedure, you won't be interacting directly (physically linked) to the target computer system in order to collect information from it. By using this method, vital data is gathered without ever having to communicate with the target systems.

4.6 INTRODUCTION TO KALI LINUX OPERATING SYSTEM

4.6.1 Introduction – Kali Linux OS

For the flawless working of a computer, the main responsible system software is an Operating System. Any operating system could be used for any task as we wish, but all they have some special tools or services available for its users which makes them a good OS for the specific purpose. E.g. Windows operating system for office work and gaming, mac OS for designing related purposes as most of the designing software are available with mac OS. In the same way, the Kali Linux is an OS for Network Security, Digital Forensics, Penetration testing, or Ethical Hacking.

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. Kali Linux is a specially designed OS for network analysts, Penetration testers, or in simple words, it is for cybersecurity and network analysis. The official website of Kali Linux is Kali.org. It was not designed to use it as general-purpose operating system, but it is for the professionals or the people who know how to operate Linux/Kali.

Advantages :

- It has 600+ Penetration testing and network security tools pre-installed.
- It is completely free and open source. So, you can use it for free and even contribute for its development.
- It supports many languages.
- Great for those who are familiar with Linux and Linux commands.
- Could be easily used with Raspberry Pi.

Disadvantages :

- It is not recommended for those who are new to Linux and want to learn Linux.
- It is a bit slower.
- Some software may malfunction.

Many people think that Kali is a tool for hacking or cracking. This is one of the biggest myths about Kali Linux. Kali Linux is just another Debian distribution with a bunch of networking and security tools which is used as a weapon to train or defend yourself not to attack anyone. It is a powerful tool and in case, not used properly, it may lead to losses even.

Kali Linux is an operating system for the professional penetration testers, cybersecurity experts, ethical hackers, or those who know how to operate it. In simple words, if you know how to use Linux and its terminal commands, architecture, system, and file management then Kali Linux is also for you.

4.6.2 Installation and Configuration of Kali Linux OS

Installing Kali Linux (single boot) on your computer is an easy process. In our example, we will be installing Kali Linux in a fresh guest VM, without any existing operating systems pre-installed.

System Requirements

The system requirements for installing Kali Linux may vary depending on what you would like to install and your setup.

- Kali Linux as a basic Secure Shell (SSH) server with no desktop,

  128 MB of RAM (512 MB recommended) and 2 GB of disk space.
- Install the default Xfce4 desktop and the kali-Linux-default **metapackage**,

  at least 2 GB of RAM and **20 GB of disk space**.
- When using resource-intensive applications, such as Burp Suite,

  At least **8 GB of RAM** (and even more for a large web application!).

Installation Prerequisites

This guide will make also the following assumptions when installing Kali Linux:

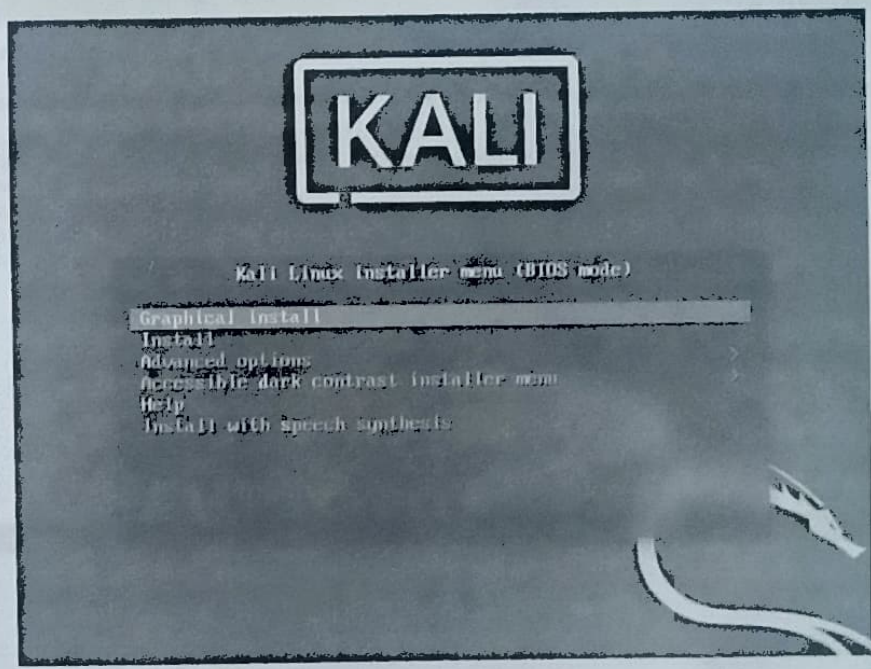
- Using the amd64 installer image.
- CD/DVD drive / USB boot support.
- Single disk to install to.
- Connected to a network (with DHCP & DNS enabled) which has outbound Internet access.

Preparing for the Installation

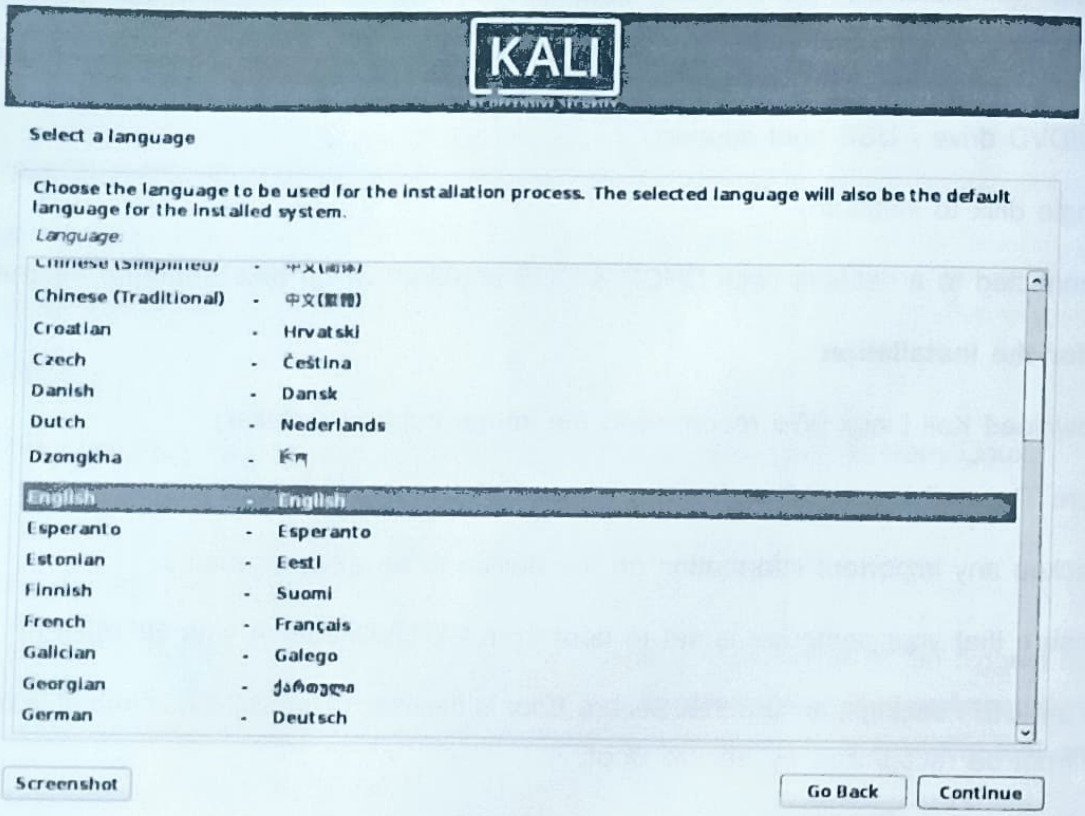
- Download Kali Linux (We recommend the image marked Installer).
- Burn The Kali Linux ISO to DVD or image Kali Linux Live to USB drive.
- Backup any important information on the device to an external media.
- Ensure that your computer is set to boot from CD/DVD/USB in your BIOS/UEFI.
- In the UEFI settings, ensure that Secure Boot is disabled. The Kali Linux kernel is not signed and will not be recognized by Secure Boot.

Kali Linux Installation Procedure

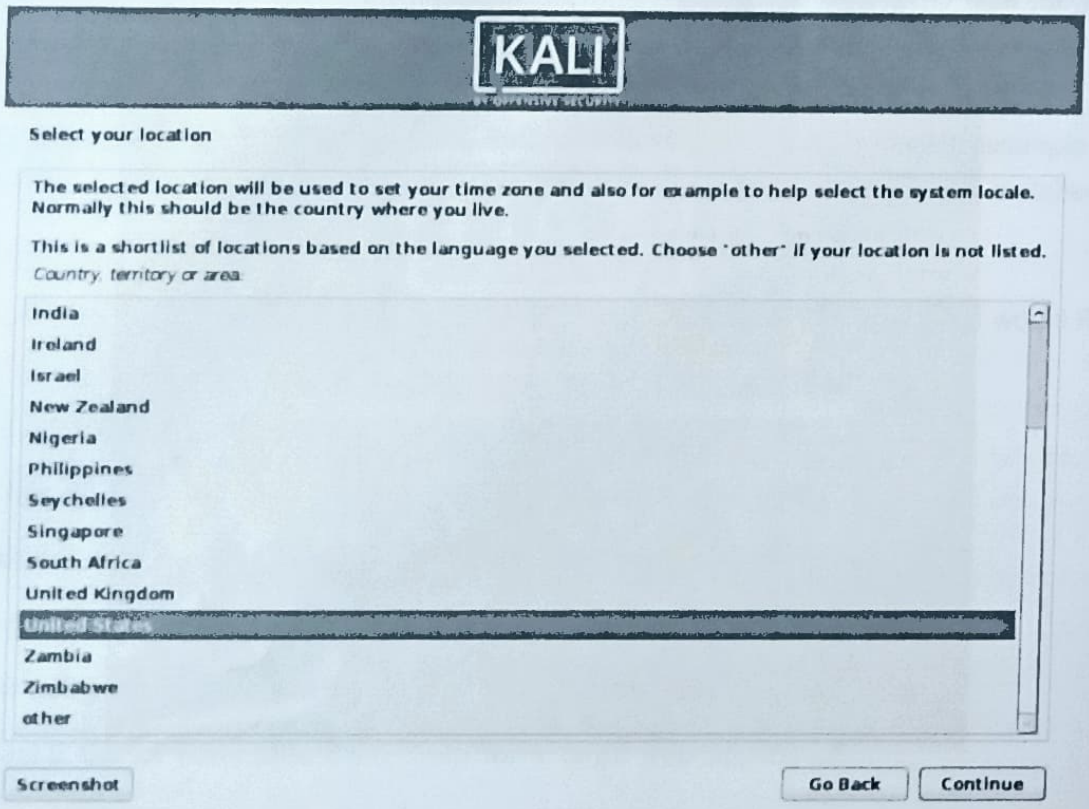
Step 1. To start your installation, boot with your chosen installation medium. You should be greeted with the Kali Linux Boot screen. Choose either Graphical install or Install (Text-Mode). In this example, we chose the Graphical install.



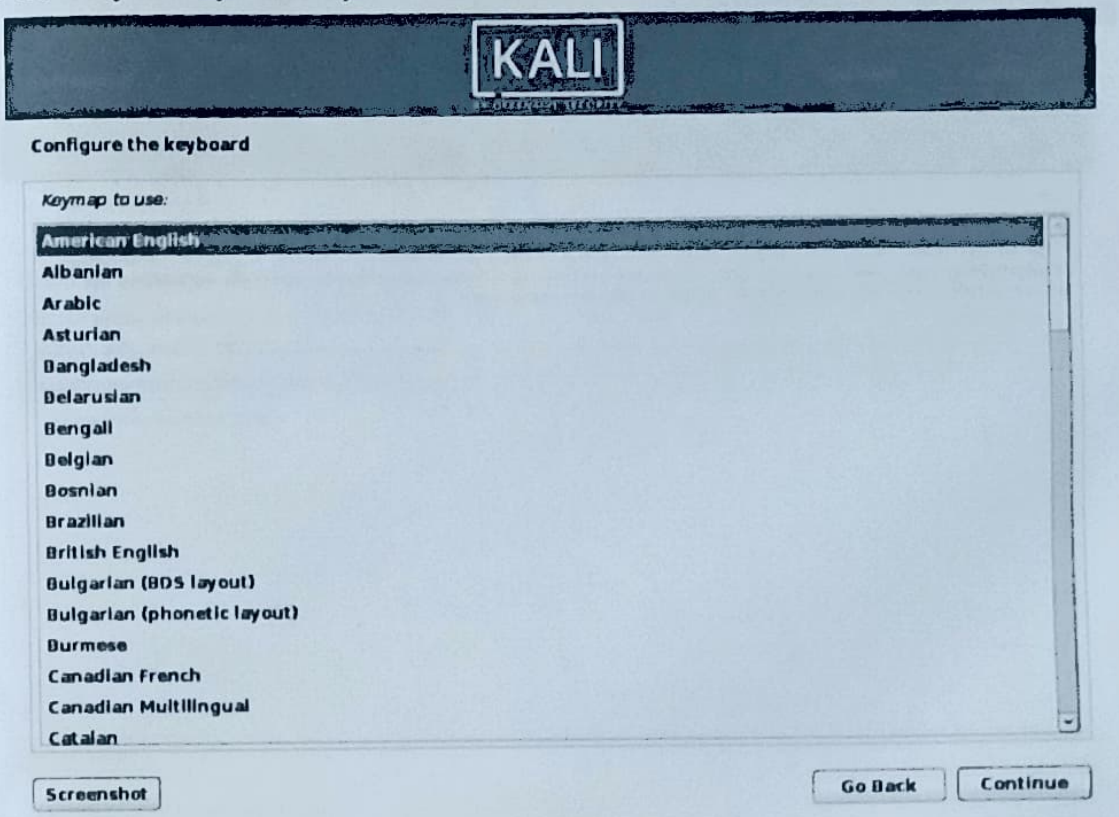
Step 2. Select your preferred language. This will be used for both the setup process and once you are using Kali Linux.



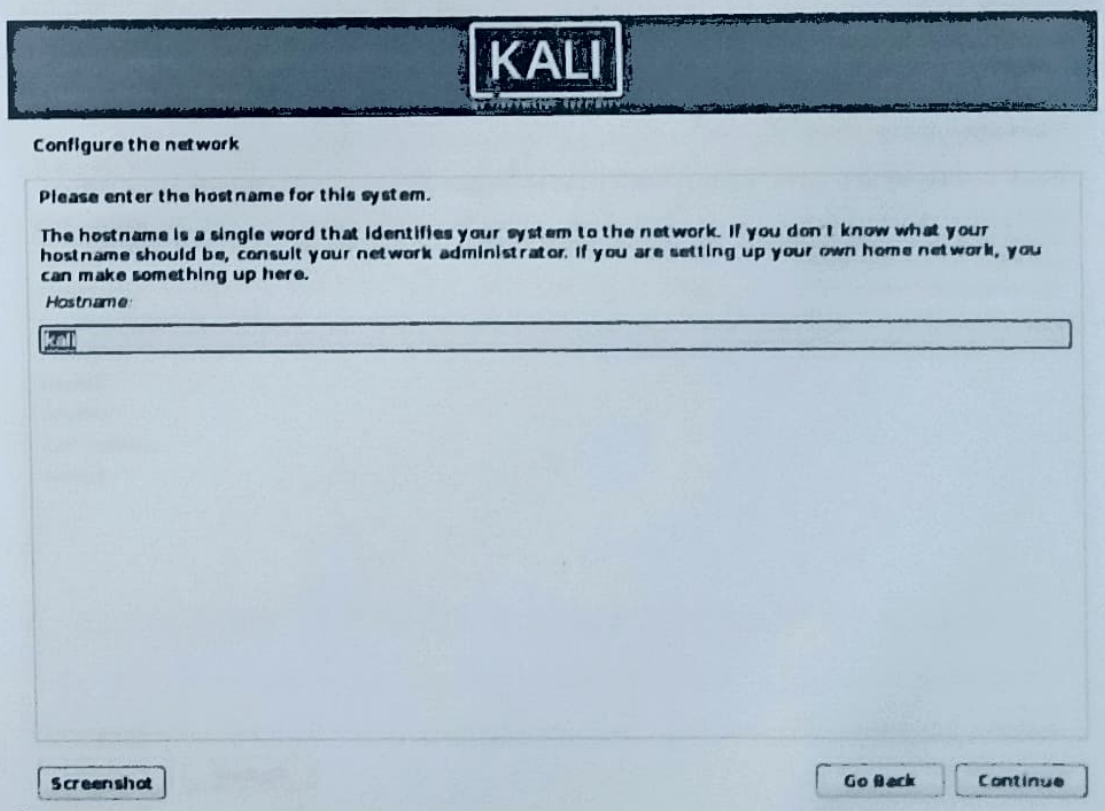
Step 3. Specify your geographic location.



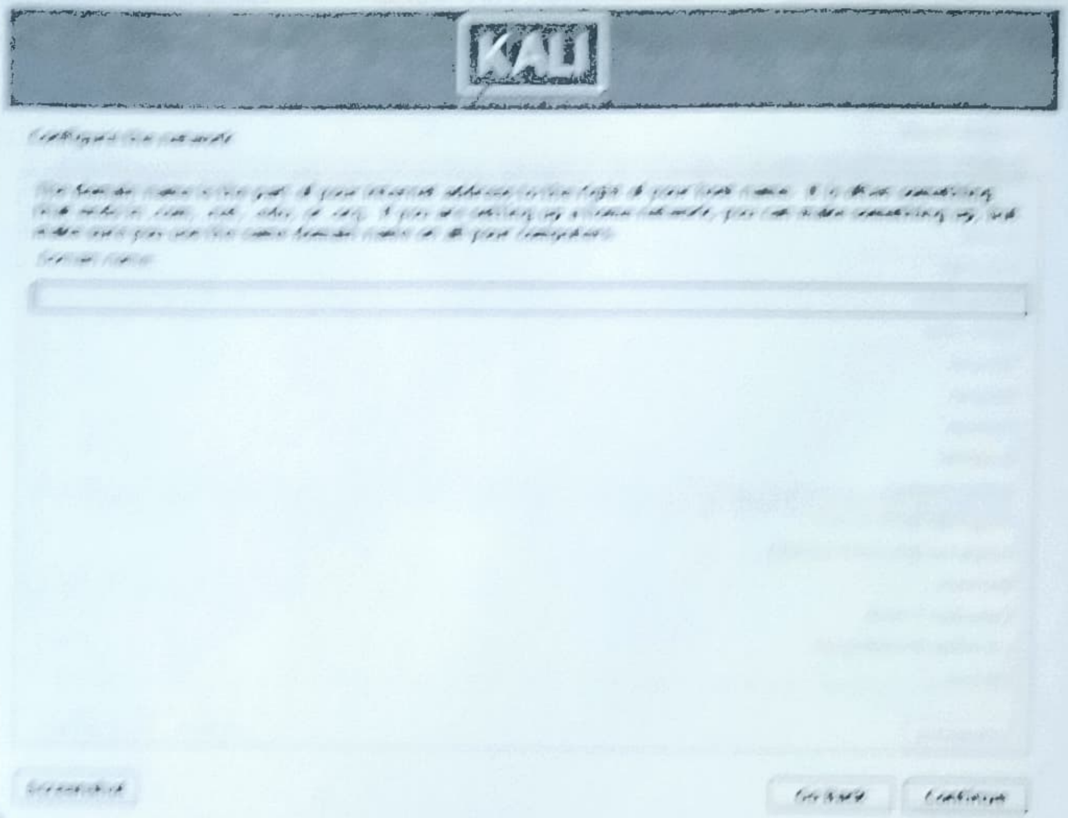
Step 4. Select your keyboard layout.



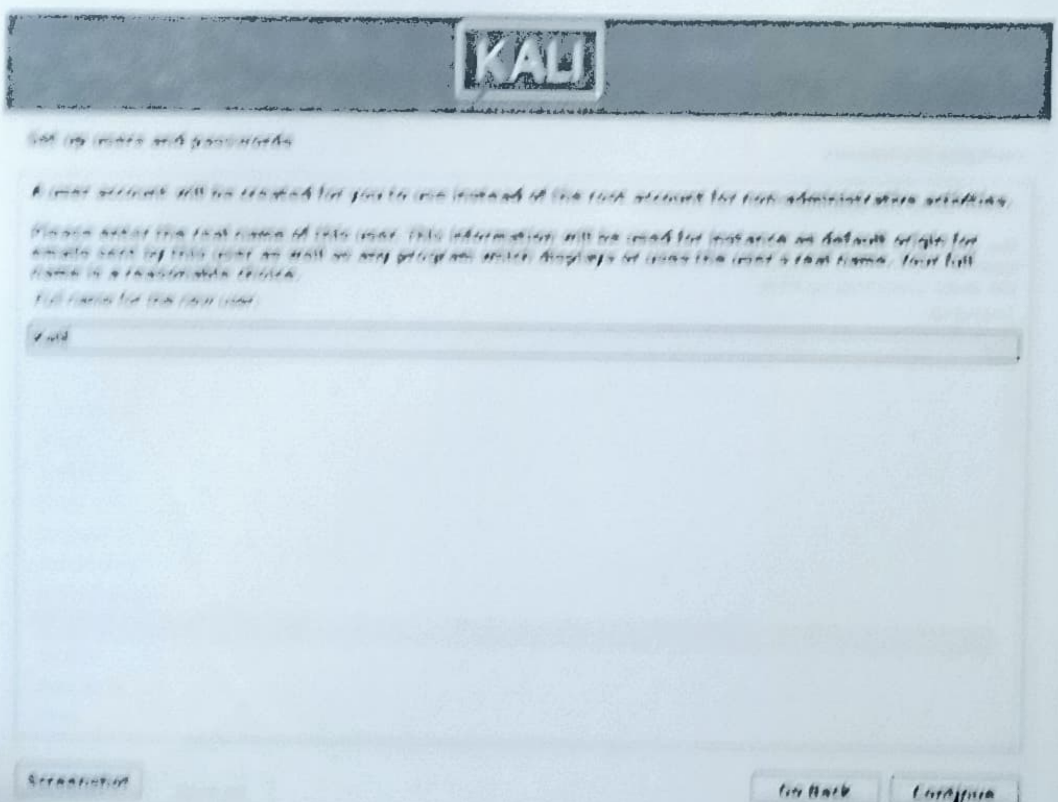
Step 5. The setup will now probe your network interfaces, looks for a DHCP service, and then prompt you to enter a hostname for your system. In the example below, we've entered **kali** as our hostname.

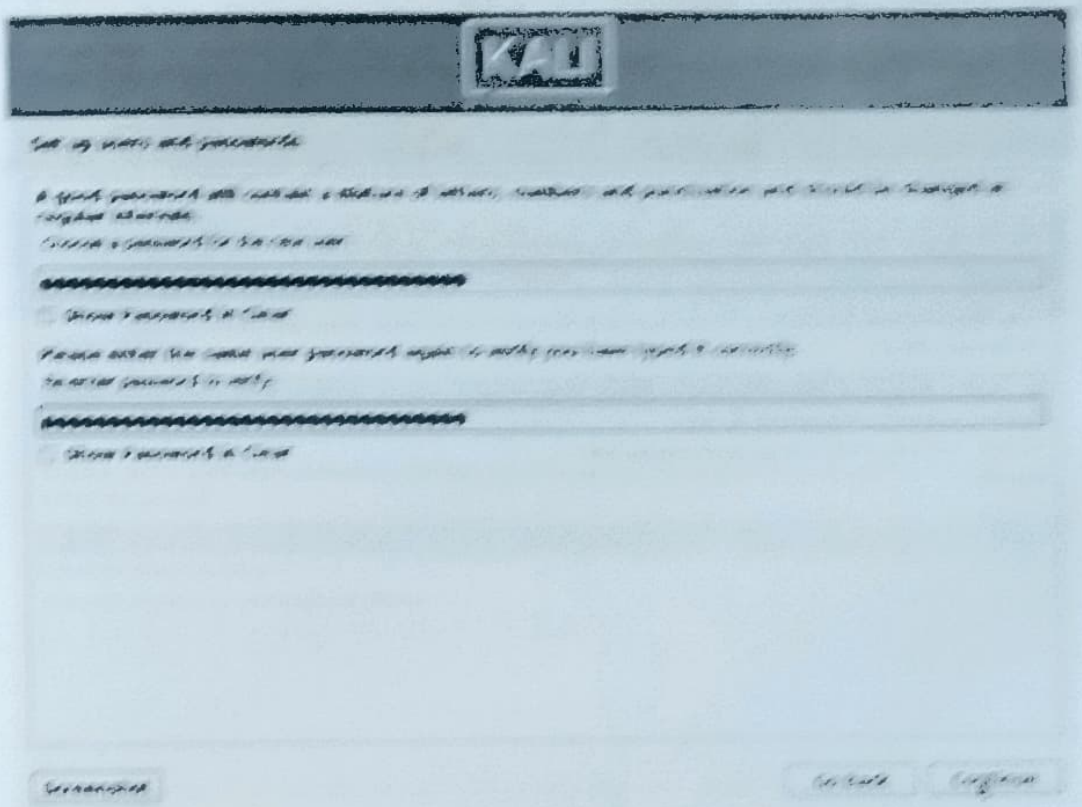


Step 6. You may optionally provide a default domain name for this system. (values may be pulled from DHCP or if there is pre-existing operating systems). select your keyboard layout.

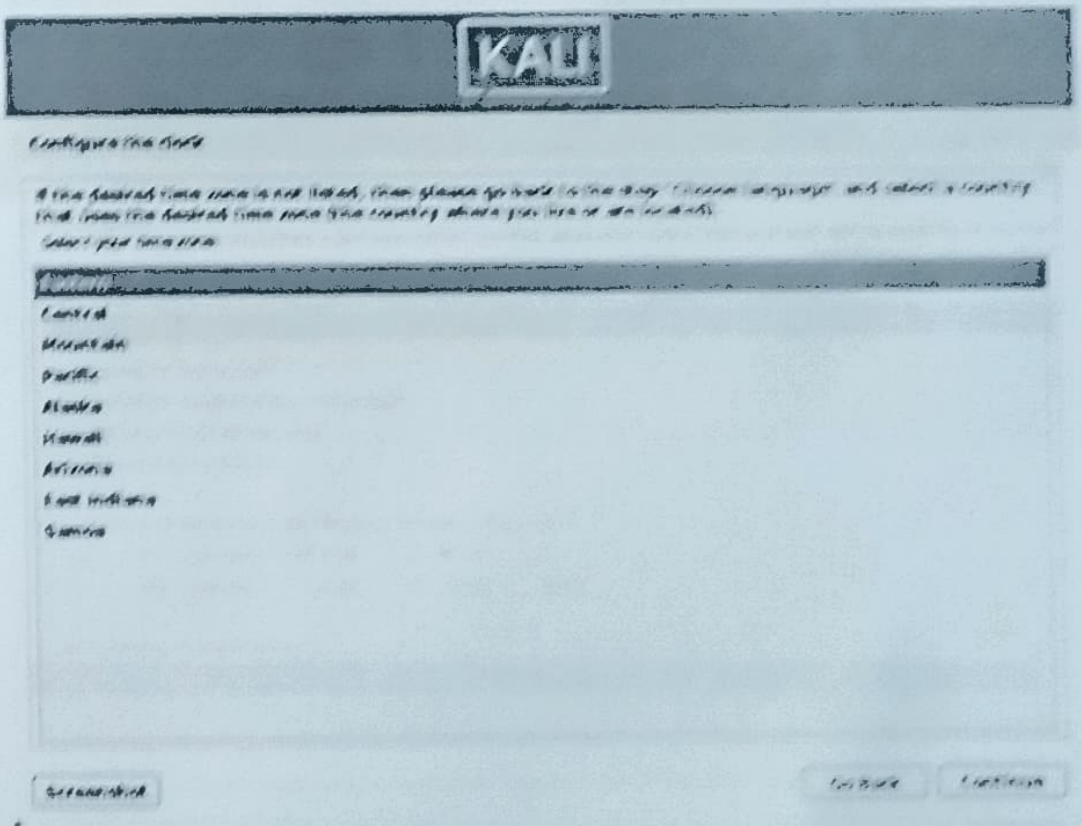


Step 7. Next, create the user account for the system (Full name, username and a password).

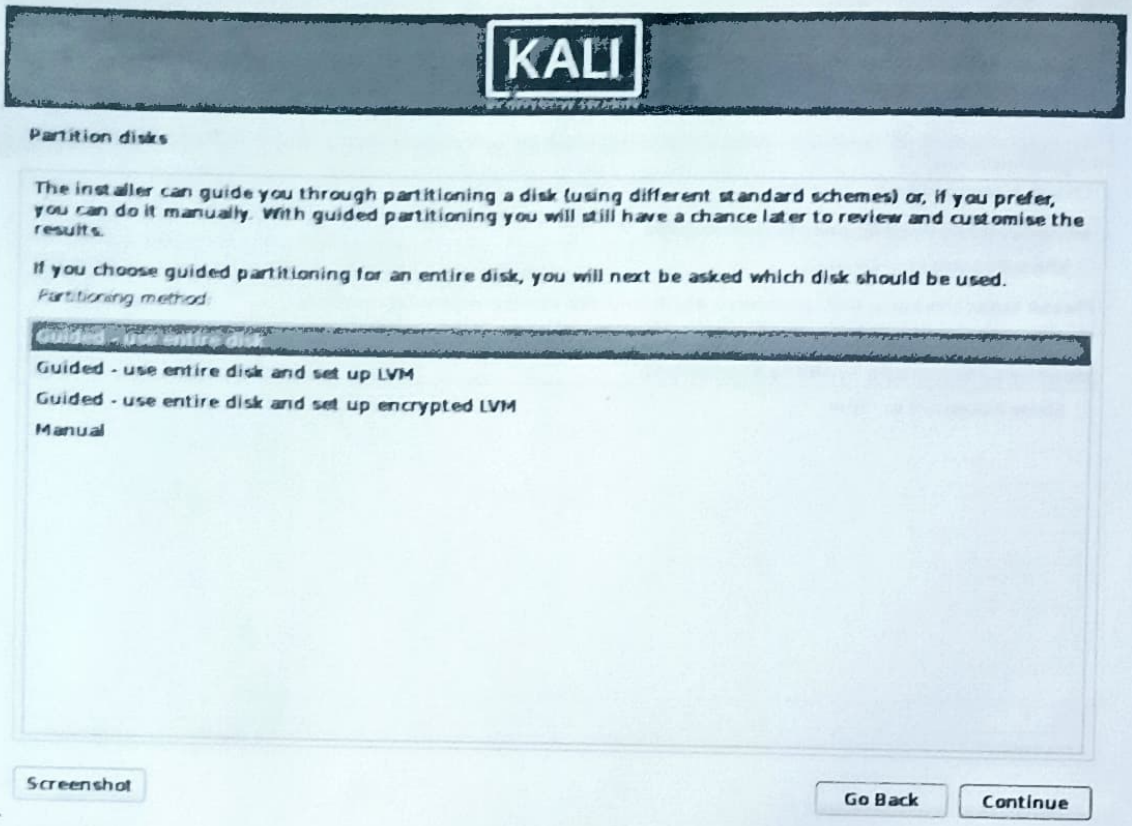




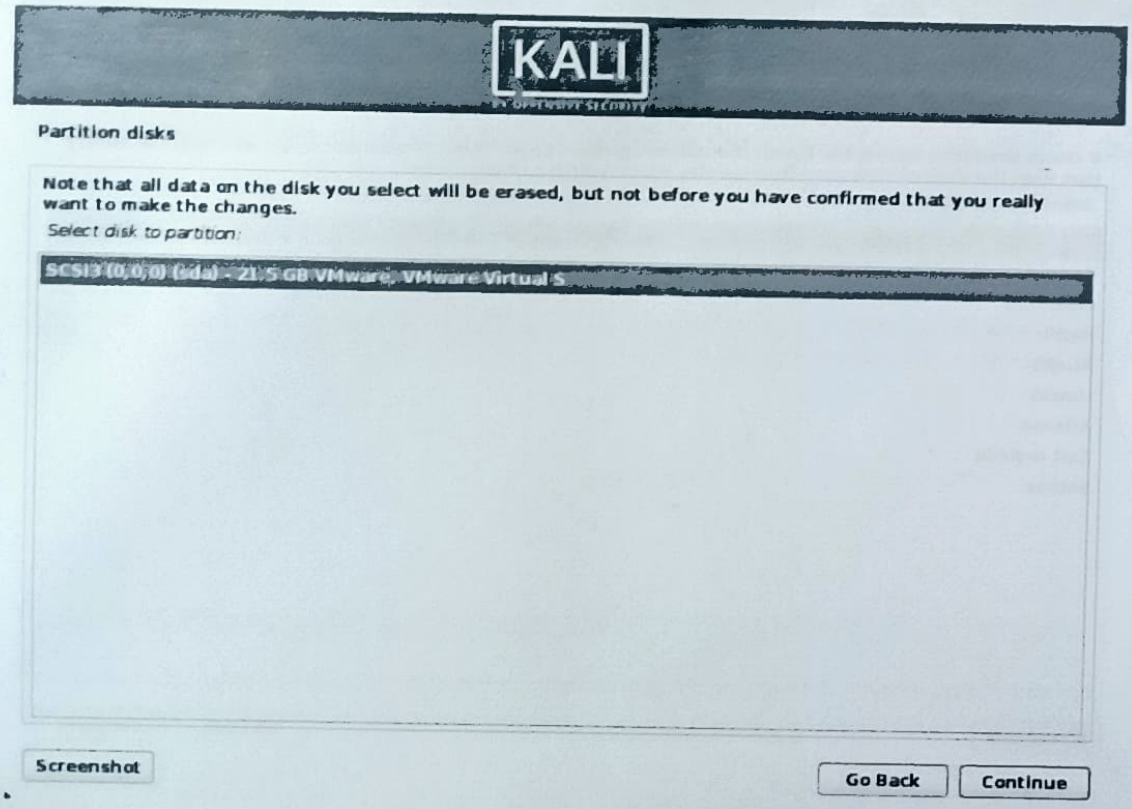
Step 2. Next, set your time zone.



Step 9. The installer will now probe your disks & offer you choices, depending on the setup.

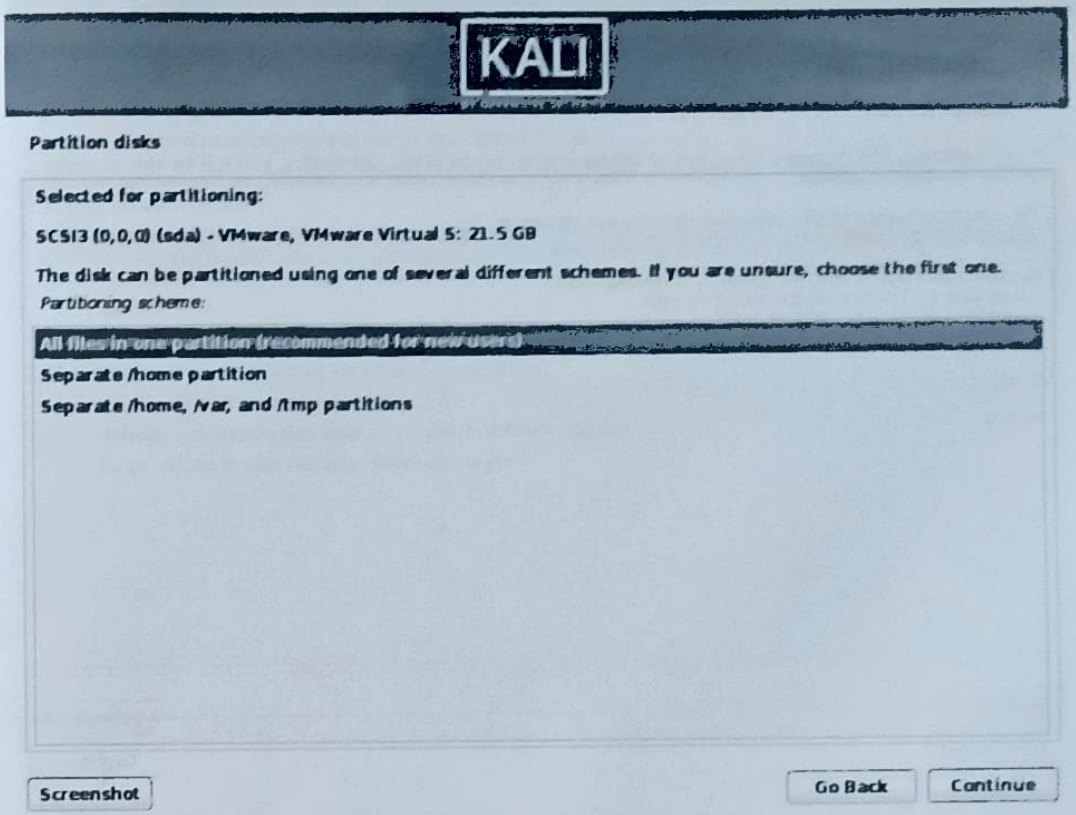


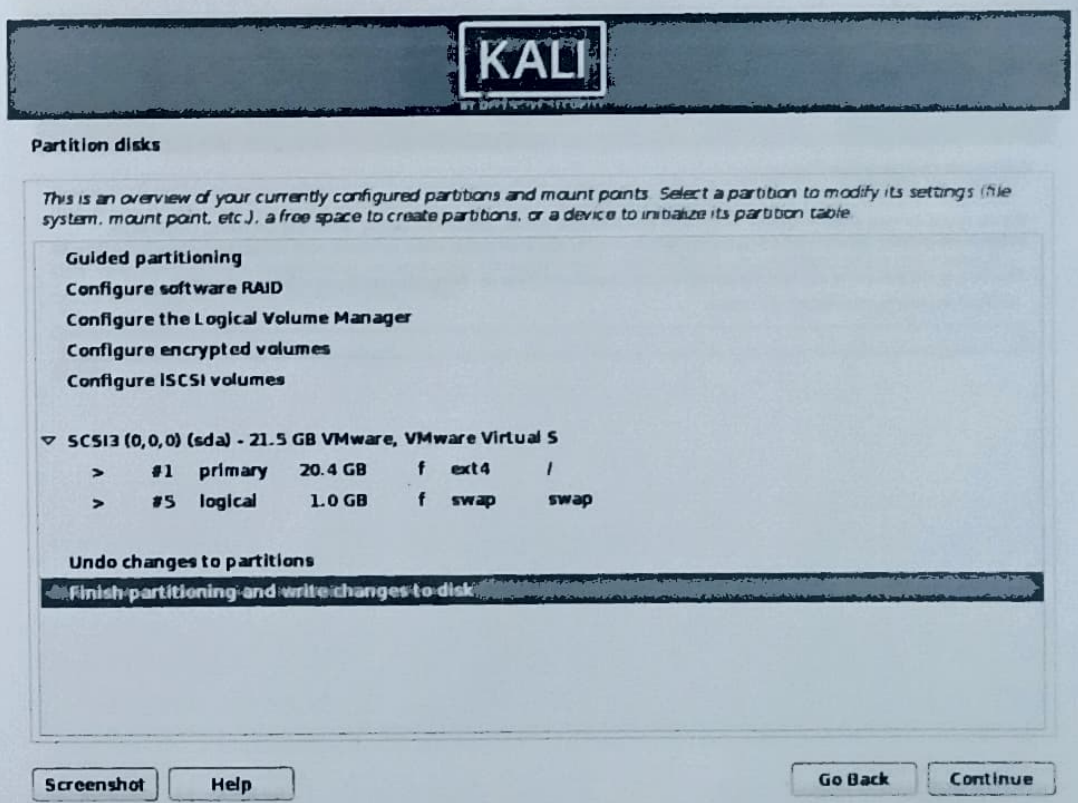
Step 10. Select the disk to be partitioned.



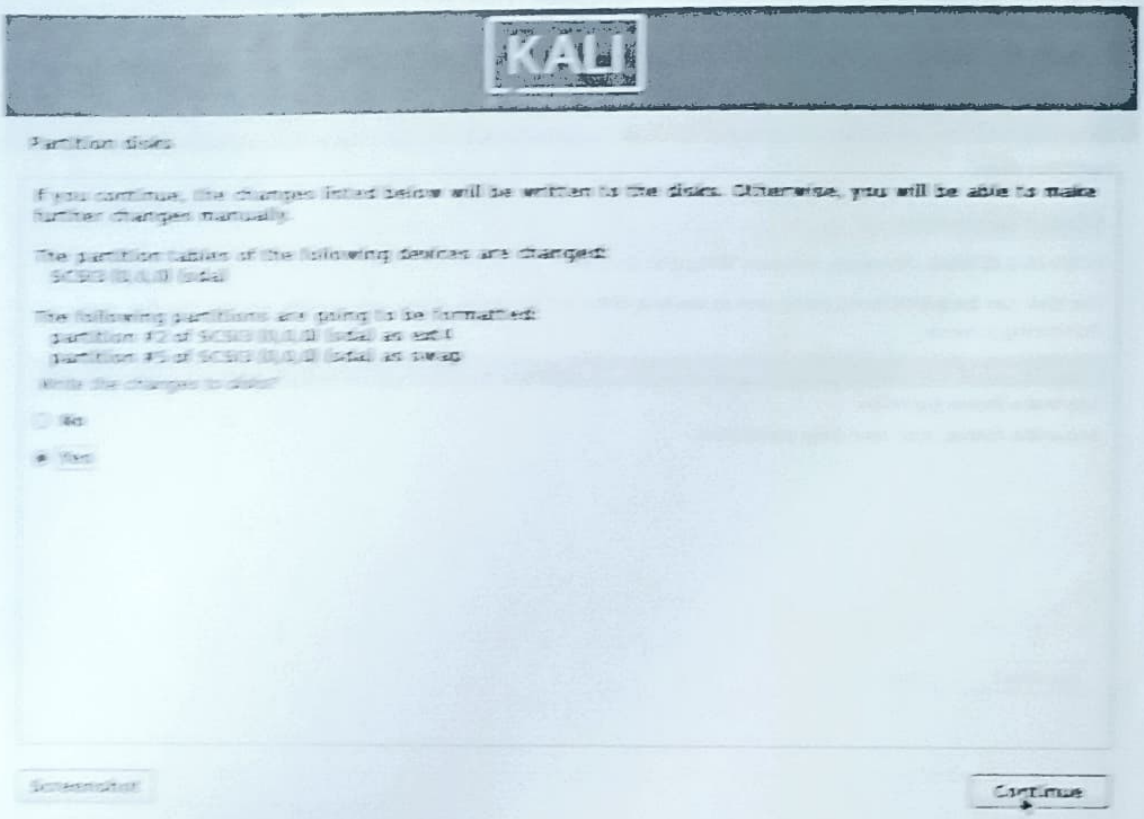
Step 11. Depending on your needs, you can choose to keep all your files in a single partition - the default - or to have separate partitions for one or more of the top-level directories.

If you're not sure which you want, you want **"All files in one partition"**.

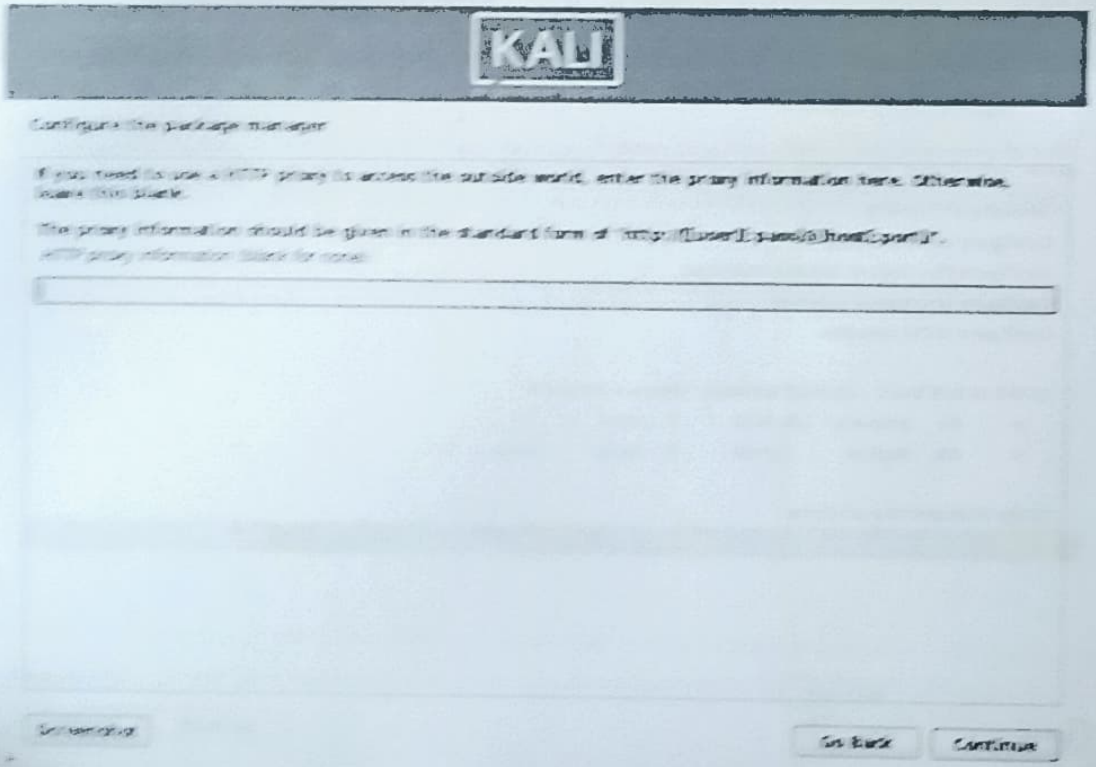




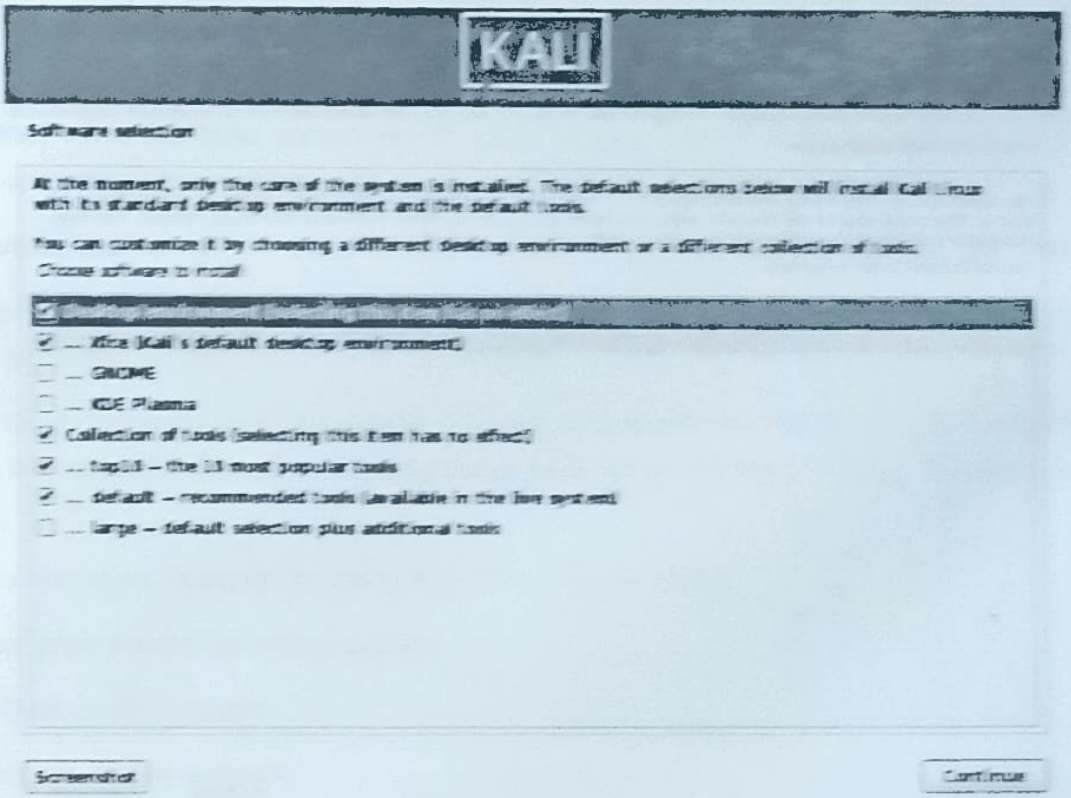
Step 12. Next, you'll have one last chance to review your disk configuration before the installer makes irreversible changes. After you click Continue, the installer will go to work and you'll have an almost finished installation.



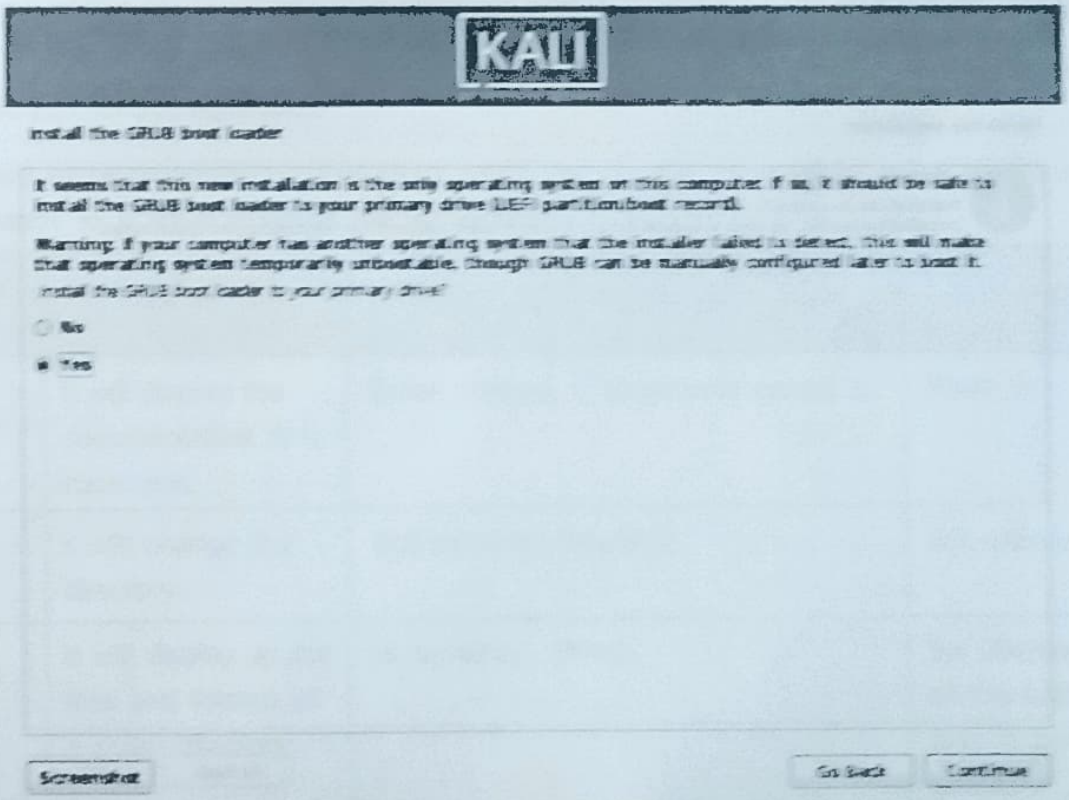
Step 13. Kali Linux uses a central repository to distribute applications. You'll need to enter any appropriate proxy information as needed.



Step 14. Next you can select which metapackages you would like to install. The default selections will install a standard Kali Linux system.

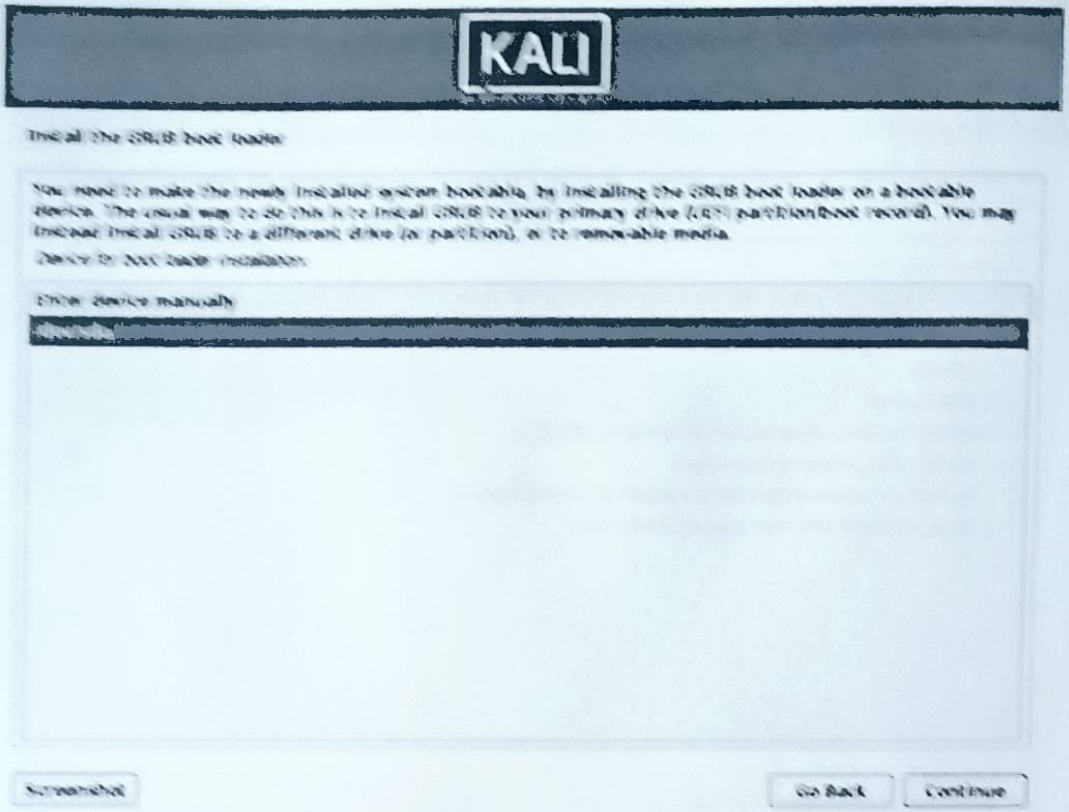


Step 15. Next confirm to install the GRUB boot loader.

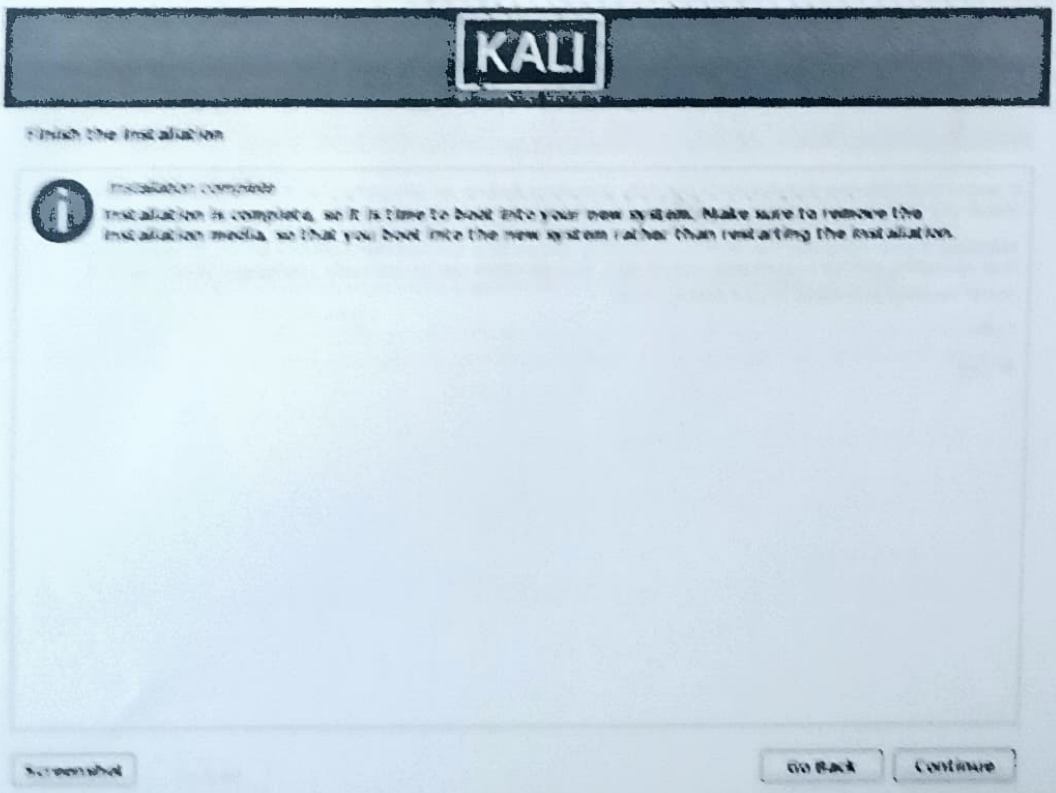


Step 16. Select hard drive to install the GRUB bootloader in

(By default, it does not select any drive).



Step 17. Finally, click Continue to reboot into your new Kali Linux installation.



4.6.3 Basic commands in Kali Linux

Kali Linux is an open-source operating system. All system hardware and resources, such as CPU, memory, and storage, are directly managed by the operating system. Kali Linux is similar to Unix, but Kali Linux can work on a large number of devices, from mobiles to supercomputers. Linux includes:

- **Kernel :** It is the base component of any operating system. It manages system resources and makes users communicate with hardware by using Kali Linux commands.
- **System userspace :** It contains all the codes of the applications that the user interacts with.
- **Applications :** It consists of all the utilities and software that are used while working. They can be accessed by using Kali Linux commands.

Kali Linux is primarily used by ethical hackers. It contains hundreds of cyber security tools and applications for various information security tasks such as penetration testing, forensics, and reverse engineering.

Some of the more reasons for using Kali Linux are as under:

- Free open-source operating system
- Multi-language support
- Wireless device support
- Completely customizable

Kali Linux – Command Line Essentials

Command-line plays an important role when we are working with Kali Linux. While executing a command in Kali Linux we enter a command on the terminal emulator and it gives us the appropriate output after the execution of the command.

There are some commands in Kali Linux which we use too frequently. So, we should be aware of those commands as it could increase our productivity.

Command Name	Description	Syntax	Example
man	It will display the documentation of ls command	$man [option] ... [command name] ...	$man ls
cd	It will change the directory	$cd [options] directory]	$cd Desktop
ls	It will display all the files and folders in a given directory.	ls [options]... [files] ..	$ls DesktopShows all the folders and files in the Desktop directory

Command Name	Description	Syntax	Example
cat	Reads the contents of all files that are in a terminal.	$cat [options].... [filename(s)] ...	$cat text.txt
touch	Creates new files without writing any content in it.	$touch [Option]... [Filename]...	$ touch test1.txtIt creates a file with a text name.
mkdir	Create a new directory in the present directory	$mkdir [Option]..<Directory Name>..	$mkdir testcreates a test folder.
pwd (print working directory)	It shows you the working directory	$pwd [Option]	$pwd
echo	Displays any text as arguments	$echo [Option] [String]	$ echo -e "Welcome"
rm	Used to remove or delete any directory.	$rm [Option] [File]	$rm test123.txt
rmdir	Deletes or removes empty directories.	$rmdir [Option] [Directory_Name]	$ rmdir test
mv	It can move files from one folder to another.	$mv [Source] [Destination]	$mv t1.txt t2.txt
cp	Copies files from one location to another.	$cp [Options] [Source].. [Destination]	$cp t1.txt t2.txt
tree	Lists of contents of a director in the tree fashion.	$tree [Options]	$tree
grep	Searches for word in files and prints lines with that word.	$grep [Options] [Pattern] [Filename]	$grep -ihkp t1.txt
vi	Allows the users to edit the text in the Vim editor.	$vi [Options] [Filename]	$vi t1.txt

Command Name	Description	Syntax	Example
head	Prints the first given number of lines from a file.	$head [Option] [Filename]	$head -n 2 t1.txtIt will print first 2 lines of t1.txt
tail	Prints the last given number of lines from a file.	$ tail -n <number><Filename>	$tail -n 2 t1.txt It will print last 2 lines of t1.txt
wc (word count)	It shows the number of lines, words, bytes and characters.	$wc [Option]... [File]...	$wc t1.txt
history	shows history of commands that you have typed and executed.	$history	$history

4.6.4 Vulnerability Scanning

The practice of finding security holes and weaknesses in the software and systems that run on them is known as vulnerability scanning. It is a component of an organization-protecting vulnerability management program that guards against data breaches.

Vulnerability scanning technologies are used by IT departments or outside security service providers to check for vulnerabilities. By doing this, the effectiveness of countermeasures against a danger or assault can be predicted.

NIS defines vulnerability scanning as:

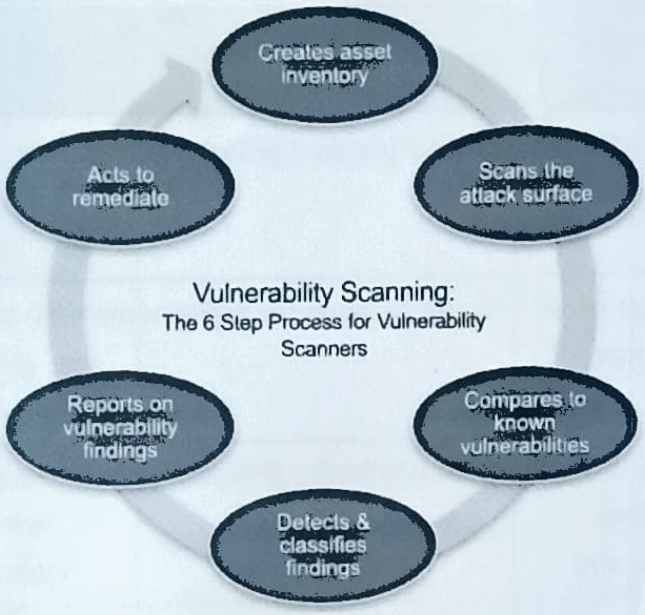
"A technique to identify hosts/host attributes and associated vulnerabilities."

Software for vulnerability scanning can identify a company's weaknesses, provide assistance in fixing them, and assist in setting priorities for repair activities.

How vulnerability scanning operates:

Regular vulnerability scanning keeps businesses ahead of new vulnerabilities and emerging threats. Vulnerability scanning is a continuous process. Here's a detailed breakdown of how it operates:

- **Generates an asset inventory :** Every system linked to a network is found and listed by the vulnerability scanner. It lists the software, open ports, operating system, and user accounts for every device.
- **Examines the attack surface :** In order to find potential risk exposures and attack routes, the scanner then examines the networks, hardware, software, and systems.



[Fig. 4.3 : Six Step Process of Vulnerability Scanning]

- **In contrast to vulnerability databases :** The vulnerability scanner searches the target attack surface for known vulnerabilities, such as CVEs, and possible routes to sensitive data.
- **Identifies and categorizes :** The scanner finds and categorizes vulnerabilities in systems that an attacker could use against you.
- **Reports:** To assist businesses in setting priorities, the scanner generates reports that detail vulnerabilities and associated fixes.
- **Takes corrective action :** Organizations can take action to address the vulnerabilities found based on the information from the vulnerability scans. Patching, updating software, resetting systems, and putting other security measures in place can all be part of this.

4.6.5 Vulnerability Based Hacking

Hacking can be classified into different categories as described below.

- **Foot printing**

Foot printing is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information like Domain name, IP Addresses, Namespaces, Employee information, Phone numbers, E-mails, Job Information etc...

For example, we can use **http://www.whois.com/whois** website to get detailed information like domain name information with its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Another example is to use of **ping command to find out an IP Address.** $ping ambajitemple.com

- **Scanning**

Vulnerability scanning is a specific type that focuses on identifying security flaws and vulnerabilities in systems and software. Scanning software can show a company where its vulnerabilities are, offer support to fix them and help you prioritize remediation efforts.

- **Password Cracking**

Password cracking refers to the act of attempting to uncover or crack passwords that are encrypted or hashed.

The main objectives of password cracking are as :

1. *Recover forgotten passwords* : Password cracking can be used for legitimate purposes, such as helping individuals recover forgotten passwords
2. *Penetration Testing* : Password cracking is sometimes used by security professionals and ethical hackers during authorized penetration testing engagements. By attempting to crack passwords, they can assess the strength of security measures and identify vulnerabilities within an organization's systems and networks. This helps organizations improve their overall security posture by addressing weaknesses.
3. *To gain access* : Another objective of the password cracking is to gain unauthorised access to the system or computer network or server.

Password crackers are tools or programs used by individuals or attackers to recover or crack passwords that have been encrypted or hashed. These tools utilize various methods and techniques to guess or obtain passwords through brute force attacks or exploiting vulnerabilities.

- **Brute Force Attacks**

Brute force attacks involve systematically trying every possible combination of characters until the correct password is found. Password crackers automate this process by attempting different combinations of characters, including letters, numbers, and symbols, until the password is successfully cracked. Brute force attacks can be time-consuming, especially for complex and longer passwords.

- **Injection Attacks**

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. SQL injection is a code injection technique that might destroy your database.

It occurs when the web application does not properly validate or sanitize user-supplied input, allowing an attacker to inject malicious SQL statements into the application's database queries.

For example, we have an application which selects the user from usermaster table in the database based on userid.

The frontend design for this application is as below.

ENTER USER ID [ ]

The backend logic (SQL statement) for this application is as below.

```
txtuserid = getRequestString("userid");
txtSQL = "SELECT * FROM usermaster WHERE userid = " + txtuserid;
```

In this application, user is required to enter his userid in the above textbox. Then SQL statement written above will be executed and gives the detail for that user as the userid supplied in the textbox.

ENTER USER ID [101 OR 1=1]

SQL Injection statement based on 1=1 always true.

When attacker enters input as written in textbox. The backend SQL statement will be executed as

```
SELECT * FROM usermaster WHERE userid = 105 OR 1=1;
```

The SQL statement above is valid and will return ALL rows from the "usermaster" table, since **OR 1=1** is always TRUE. What if the "usermaster" table contains names and passwords? A hacker might get access to all the user names and passwords in a database.

With the use of various techniques like Parameterized queries, Input Validation and Sanitization, Least Privilege Principle, Secure Coding Practices, Web Application Firewalls, and Regular Security Testing we can prevent from the SQL Injection Attack.

- **Phishing Attacks**

Phishing is a type of cybercrime in which criminals pose as a trustworthy source online to lure victims into providing personal information such as usernames, passwords, or credit card numbers. The goal of any phishing scam is always **stealing personal information**, there are different types of phishing attacks as described.

1. Email Phishing : It is the most common type of phishing which often involves a "spray and pray" technique in which hackers impersonate a legitimate identity or organization and send **mass emails** to as many addresses as they can obtain.

These emails are often written with a sense of urgency, informing the recipient that a personal account has been compromised and they must respond immediately. Their objective is to elicit a certain action from the victim such as clicking a malicious link that leads to a fake login page. After entering their credentials, victims unfortunately deliver their personal information straight into the scammer's hands.

2. Spear Phishing : Rather than using the "spray and pray" method as described above, spear phishing involves sending malicious emails to specific individuals within an organization. Rather than sending out mass emails to thousands of recipients, this method targets certain employees at specifically chosen companies. These types of emails are often more personalized in order to make the victim believe they have a relationship with the sender.

3. **Whaling :** Whaling closely resembles spear phishing, but instead of going after any employee within a company, scammers specifically target senior executives (or "the big fish," hence the term whaling). This includes the CEO, CFO or any high-level executive with access to more sensitive data than lower-level employees. Often, these emails use a high-pressure situation to hook their victims, such as relaying a statement of the company being sued. This entices recipients to click the malicious link or attachment to learn more information.

4. **Smishing :** SMS phishing, or smishing, leverages text messages rather than email to carry out a phishing attack. They operate much in the same way as email-based phishing attacks: Attackers send texts from what seem to be legitimate sources (like trusted businesses) that contain malicious links. Links might be disguised as a coupon code (20% off your next order!) or an offer for a chance to win something like concert tickets.

5. **Vishing :** Vishing—otherwise known as voice phishing—is similar to smishing in that a phone is used as the vehicle for an attack, but instead of exploiting victims via text message, it's done with a phone call. A vishing call often relays an automated voice message from what is meant to seem like a legitimate institution, such as a bank or a government entity.

6. **Business Email Compromise (CEO Fraud) :** CEO fraud is a form of phishing in which the attacker obtains access to the business email account of a high-ranking executive (like the CEO). With the compromised account at their disposal, they send emails to employees within the organization impersonating as the CEO with the goal of initiating a fraudulent wire transfer or obtaining money through fake invoices.

7. **Clone Phishing :** This method of phishing works by creating a malicious replica of a recent message you've received and re-sending it from a seemingly credible source. Any links or attachments from the original email are replaced with malicious ones. Attackers typically use the excuse of re-sending the message due to issues with the links or attachments in the previous email.

- **Block chain Attacks**

Blockchain attacks refer to malicious activities aimed at disrupting or compromising the integrity, availability, or confidentiality of blockchain networks and associated assets. Blockchain technology, which underpins cryptocurrencies like Bitcoin and Ethereum, is designed to be secure through its decentralized and distributed nature. However, various attack vectors can still pose risks to blockchain systems. Here are several types of blockchain attacks:

1. **51% Attack :** In a 51% attack, a single entity or group controls more than 50% of the computational power (hash rate) of a blockchain network. This enables the attacker to manipulate transaction confirmations, reverse transactions, or double-spend coins.

2. **Sybil Attack :** A Sybil attack occurs when an attacker creates multiple fake identities or nodes to gain control or influence over a blockchain network. This can lead to network manipulation, denial of service (DoS) attacks, or undermining the consensus mechanism.

3. Denial of Service (DoS) Attack : A DoS attack aims to disrupt the availability of a blockchain network by overwhelming it with a high volume of malicious traffic or transactions. This can prevent legitimate users from accessing the network or executing transactions.

4. Eclipse Attack : In an eclipse attack, an attacker isolates a targeted node by controlling its network connections and surrounding it with malicious nodes. This allows the attacker to manipulate the node's view of the blockchain network, potentially leading to double-spending or other fraudulent activities.

5. Double-Spending : Double-spending occurs when a user spends the same cryptocurrency units more than once. While blockchain technology is designed to prevent double-spending through its consensus mechanism, certain vulnerabilities or attacks, such as 51% attacks, can enable double-spending.

4.7 PORT SCANNING

4.7.1 What is Port Scanning ?

A port scanning is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals to find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

When hackers send a message to a port, the response they receive determines whether the port is being usedand if there are any potential weaknesses that could be exploited.

Businesses can also use the port scanning technique to send packets to specific ports and analyse responses for any potential vulnerability. They can then use tools like IP scanning, Network mapper (Nmap), and Netcat to ensure their network and systems are secure.

Port scanning can provide information such as:

- Services that are running
- Users who own services
- Whether anonymous logins are allowed
- Which network services require authentication

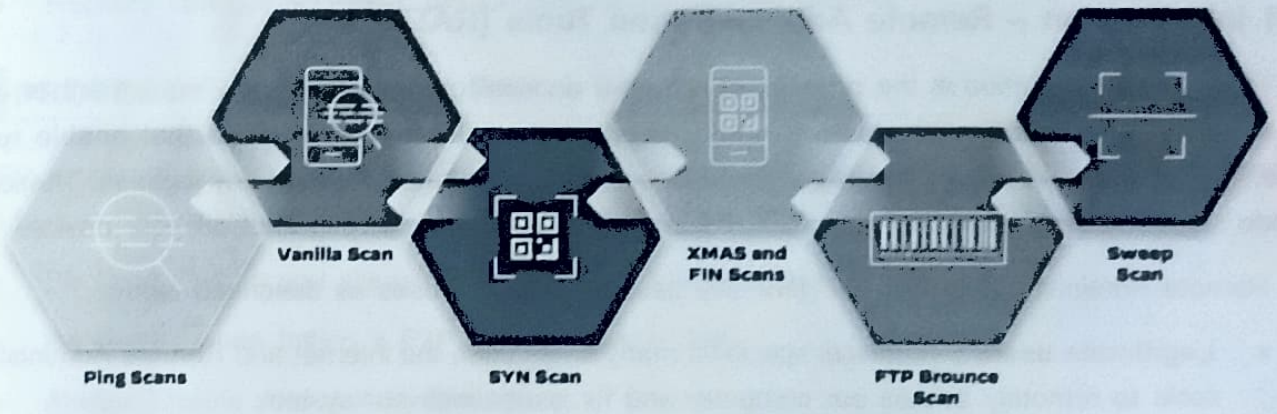
4.7.2 Port Scanning Techniques

A port is a point on a computer where information exchange between multiple programs and the internet to devices or other computers takes place. To ensure consistency and simplify programming processes, ports are assigned port numbers. This, in conjunction with an IP address, forms vital information that each internet service provider (ISP) uses to fulfil requests.

Some of the most popular and most frequently used ports include :

- Port 20 (UDP): File Transfer Protocol (FTP) used for transferring data
- Port 80 (TCP): The World Wide Web Hypertext Transfer Protocol (HTTP)

The various port scanning methods are described under :



[Fig. 4.4 : Port Scanning Methods]

1. **Ping scans :** A ping scan is considered the simplest port scanning technique. They are also known as internet control message protocol (ICMP) requests. Ping scans send a group of several ICMP requests to various servers in an attempt to get a response. A ping scan can be used by an administrator to troubleshoot issues, and pings can be blocked and disabled by a firewall.

2. **Vanilla scan :** Another basic port scanning technique, a vanilla scan attempts to connect to all of the 65,536 ports at the same time. It sends a synchronize (SYN) flag, or a connect request. When it receives a SYN-ACK response, or an acknowledgment of connection, it responds with an ACK flag. This scan is accurate but easily detectable because a full connection is always logged by firewalls.

3. **SYN scan :** Also called a half-open scan, this sends a SYN flag to the target and waits for a SYN-ACK response. In the event of a response, the scanner does not respond back, which means the TCP connection was not completed. Therefore, the interaction is not logged, but the sender learns if the port is open. This is a quick technique that hackers use to find weaknesses.

4. **XMAS and FIN scans :** Christmas tree scans (XMAS scans) and FIN scans are more discrete attack methods. XMAS scans take their name from the set of flags that are turned on within a packet which, when viewed in a protocol analyser like Wireshark, appear to be blinking like a Christmas tree. This type of scan sends a set of flags, which, when responded to, can disclose insights about the firewall and the state of the ports. A FIN scan sees an attacker send a FIN flag, often used to end an established session, to a specific port. The system's response to it can help the attacker understand the level of activity and provide insight into the organization's firewall usage.

5. **FTP bounce scan :** This technique enables the sender to disguise their location by using an FTP server to bounce a packet.

6. **Sweep scan :** This preliminary port scanning technique sends traffic to a port across several computers on a network to identify those that are active. It does not share any information about port activity but informs the sender whether any systems are in use.

4.8 REMOTE ADMINISTRATION TOOL (RAT)

4.8.1 Introduction – Remote Administration Tools (RAT)

Remote administration is the process of remotely accessing or operating any equipment or device like computer from a different place. Remote Administration Tools are software that enable remote administration. Thus, RAT allows someone to access your device remotely from any location. These tools provide someone else access to your files, camera, and even the ability to shut off your device.

Remote Administration tools are generally used for two purposes as described below.

- **Legitimate users :** Technical specialist many times uses the internet and Remote Administration tools to remotely access our computer and fix issues with our system.
- **Hackers :** However, a lot of these remote administration solutions are utilized by hackers to get access to your computer, damage your data, and take crucial data. Hackers typically include a malicious code inside a game or movie that you download, which allows them to quickly get access to your computer.

4.8.2 How one can use – Remote Administration Tools (RAT)

The internet connection on both devices is a basic need if you need to access a system remotely.

With RAT software, the user can establish a remote connection to the host machine located over any other location. When you are online, hackers establish a connection with you and carry out destructive actions such as deleting files, adding data, stealing data, and so on.

Remote Administration tools can be installed in two different ways as described below.

- **Manually :** If you know how to install it, you can manually add a valid RAT to your machine. On the other hand, hackers might install RAT on your system using unique methods. Generally, this approach is used by legitimate users like technicians.
- **Stealthy :** Cybercriminals affix these viruses with an online file, such as a game or movie. The malicious software is also downloaded and installed on your system, giving you access to it.

With the use of these RAT software the below activities can be performed.

- Hackers can create, delete, rename, copy, or edit any file.
- The attacker can also use RAT for executing various commands, changing system settings, running, and controlling applications on the victim's PC.
- Hackers can install optional software or worms.
- Hackers can control hardware, shutdown, or restart a computer without asking the user's permission.
- Hackers can steal passwords, login names, personal documents, and other credentials.

- Hackers can capture screenshots and track a user's activity.
- Hackers can get access to the Camera of the victim's system.

4.9 PROTECT SYSTEM FROM RAT

For protecting your system from RAT software, the system administrator should keep below points in mind.

- Be careful when you are using the internet and downloading files online.
- Be careful when taking a P2P file from other users.
- Always Enable your Anti-Viruses.
- Don't allow any malicious file to your system.
- Update your anti-virus from time to time.
- Regularly update your software
- Restrict the access through the use of Firewall
- Limit users who can log in using Remote Desktop

Top Remote Administration Tools

- DarkComet: Dark Comet is the best RAT and a free RAT as well as the old one as well. This tool has astounding graphical UI that causes the client to control the system. It is best used on windows and can control any windows device very smoothly.
- BlackShades: This is the super RAT shockingly better than DarkComet and it is steady, reliable, and easy to use It's likewise the speediest RAT at any point made on .net and helps Windows.
- JSpy: Jspy Rat is the same as Pussy RAT as created by the same person, with some improvements and in 2013 this was free. It is a decent RAT and one of the safest RAT.
- NJRat: It is an amazing RAT to hack into different systems. It gives us a large number of choices that make it different from others. It is very simple to use. It has the malware to use the camera, microphones getting and deleting files, and many more.
- Plasma Remote Administration Tools: Plasma RAT is a capable remote administration tool (RAT) which is a customer service application. It's not just a conventional standard remote administrator tool, it is intended to control a mass measure of PCs without a moment's delay.

4.10 SNIFFING AND MECHANISM OF SNIFFING

4.10.1 Introduction - Sniffing

"Sniffing is the technique of utilizing sniffing tools to monitor and record every packet that passes over a certain network." It is a method of "tapping phone wires" to listen in on the discussion. Another name for it is computer network "wiretapping."

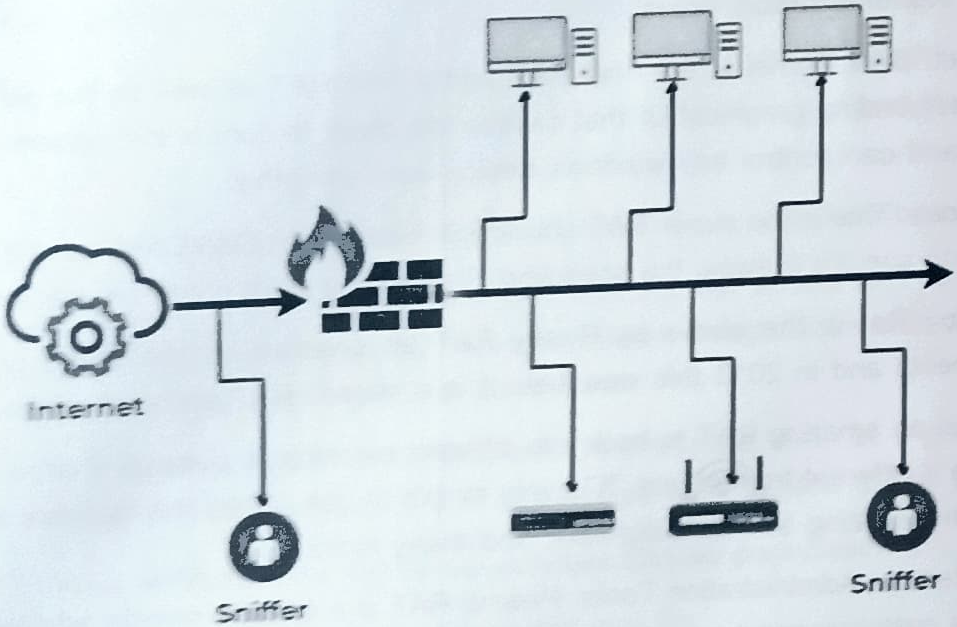
Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyse all of the network traffic.

Sniffing techniques can be used to collect information like email traffic, FTP passwords, Web traffics, Telnet passwords, Router configuration, Chat sessions, DNS traffic etc... All these collected information can be used for other kind of attacks.

How Sniffing Works

Normally, a sniffer sets the system's network interface card (NIC) to promiscuous mode, which allows it to listen to all data transmitted on its segment.

The term promiscuous mode describes the special feature of Ethernet hardware, namely network interface cards (NICs), which enables a NIC to receive any network traffic, even if it is not addressed to it. By comparing the hardware address, also known as the MAC, of the device with the destination address of the Ethernet packet, a NIC may determine by default what traffic is not directed to it. Non-promiscuous mode makes it challenging to employ network monitoring and analysis tools for traffic accounting or diagnosing connectivity problems, even though it makes perfect sense for networking.



[Fig. 4.5 : Working of sniffing]

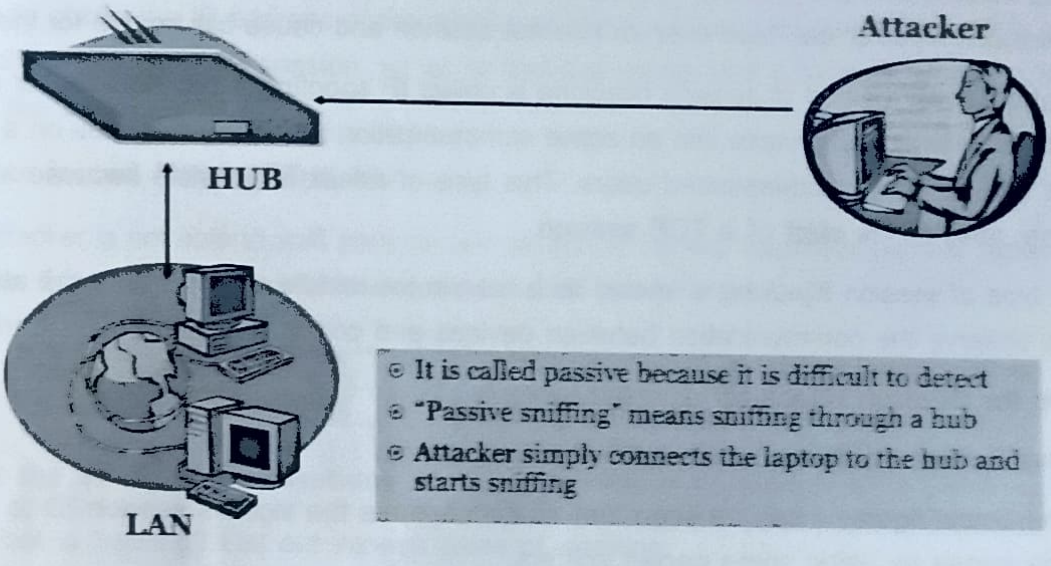
A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

4.10.2 Types of sniffing

Sniffing attacks can be classified in either Passive sniffing or Active sniffing based on sniffing method used.

Passive Sniffing:

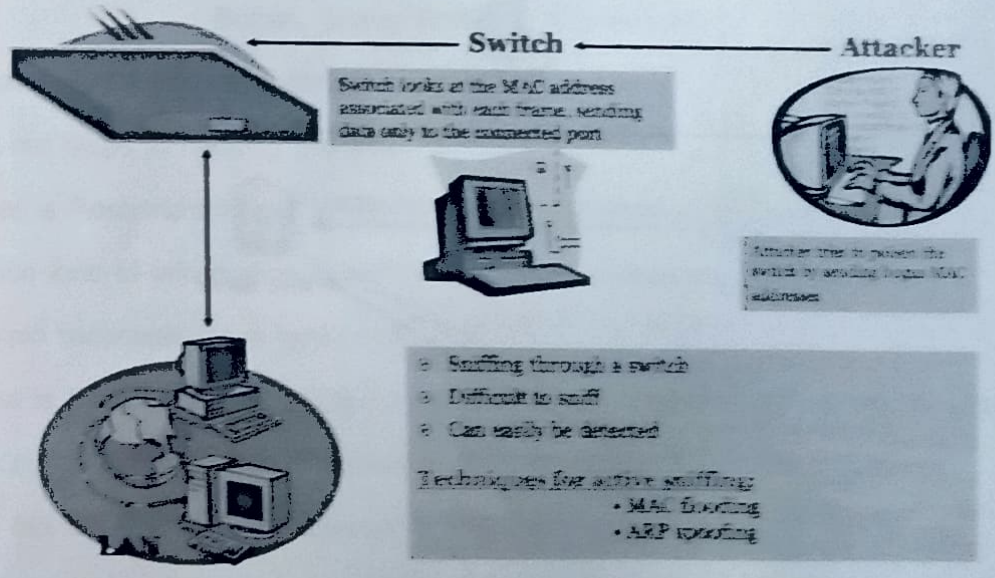
In passive sniffing, an attacker only monitors traffic without any alteration. Passive sniffing works on networks with Hub devices as central device. Hub is a device which works on broadcasting communication technique that is hub accepts packet from one computer and send it to all other computers in the network. But the computer which is intended, will only accept the packet and other computers just ignores packet received from hub. In this kind of communication traffic is visible to all the ports. So, it becomes very easy for an attacker to sniff the traffic and such kind of attack is difficult to discover.



[Fig. 4.6 : Passive Sniffing]

Active Sniffing :

In active sniffing, the traffic is not only monitored, but it may also be altered in some way as the case of attack. Active sniffing is used to sniff a switch-based network. The different kind of techniques used for Active Sniffing are MAC Flooding, DHCP Attacks, DNS Poisoning, Spoofing Attacks, ARP Poisoning etc...



[Fig. 4.7 : Active Sniffing]

The active sniffing techniques are difficult to sniff and easy to detect.

4.10.3 Session Hijacking

A session hijacking attack happens when an attacker takes over your internet session. For instance, while you're checking your credit card balance, paying your bills, or shopping at an online store. Session hijackers usually target browser or web application sessions.

A session hijacking attacker can then do anything you could do on the site. In effect, a hijacker fools the website into thinking they are you. Just as a hijacker can commandeer an airplane and put the passengers in danger, a session hijacker can take over an internet session and cause big trouble for the user.

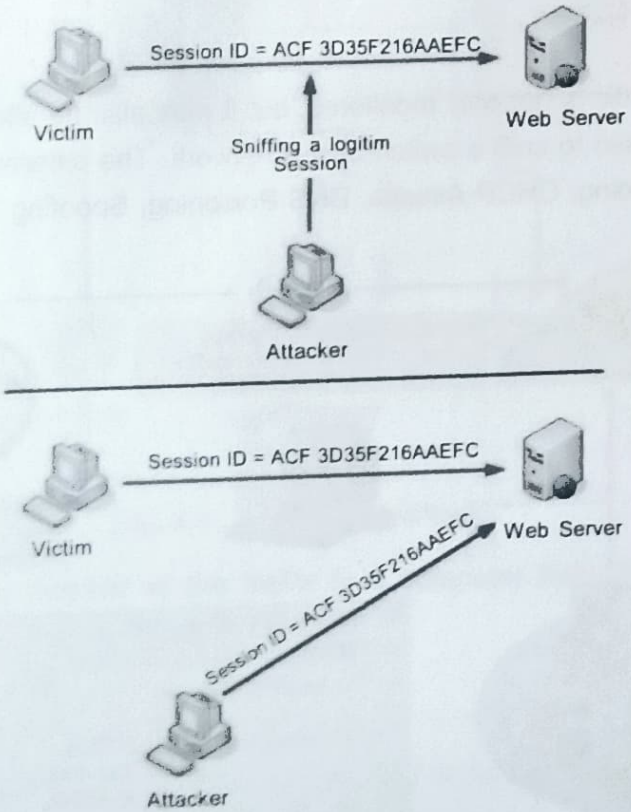
The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Methods for Session Hijacking :

- **Using Packet Sniffers**

  In the below figure, it can be seen that attack captures the victim's session ID to gain access to the server by using some packet sniffers.



[Fig. 4.8 : Session Hijacking with Packet Sniffing]

- **Cross Site Scripting (Malware Scripting)**

  Attacker can also capture victim's Session ID using XSS attack by using javascript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

- **IP Spoofing**

  Spoofing is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.

- **Brute forced Attack (Blind Attack)**

  If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What is hacking? List out various types of Hacking.

(2) Define the term: Hacking. List out the types of Hackers.

(3) Differentiate: White hat V/s Black hat V/s Grey hat hackers.

(4) What is Ethical hacking? Why ethical hacking is important?

(5) Define the Terms : Attack, Threat, Keystroke logger.

Botnet, Spam, Phishing, Vulnerability

(6) What is 0- Day vulnerability?

(7) List out steps in hacking process.

(8) What is Reconnaissance? Write down steps in Reconnaissance process.

(9) Which kind of information is gathered in Reconnaissance process.

(10) Explain reconnaissance types briefly.

(11) What is KALI Linux Operating System? Why it is important in Ethical hacking?

(12) List out advantages and disadvantages of using Kali Linux OS.

(13) List out any six basic commands of Kali Linux with its uses.

(14) What is Vulnerability Scanning? List out steps in Vulnerability scanning process.

(15) Define the terms : Foot printing, Scanning, Brute force attack

(16) What is password cracking? List out main objectives of password cracking.

(17) What is Phishing? List out various types of Phishing attacks.

(18) What is Port Scanning? List out various Port scanning methods.

(19) What is Remote Administration Tool (RAT)? Which kind of activities can be performed by hackers using RAT Tools.

(20) Write down the points by which we can protect our system from RAT.

(21) What is Sniffing? Differentiate: Active V/s Passive Sniffing

(22) What is Session Hijacking? List out various Session Hijacking methods.

Q. 2 Explain the below questions:

(1) What is hacking? Explain various types of hacking.

(2) Define the term: Hacking. Explain various types of hackers in detail.

(3) Short note on: Ethical Hacking and its importance

(4) Explain hacking process in detail with all is steps.

(5) Explain information gathering in detail with its types.

(6) Explain installation and configuration of Kali Linux with all necessary steps.

(7) Explain any 12 commands of Kali Linux with suitable example.

(8) What is Vulnerability Scanning? Explain vulnerability scanning process in detail.

(9) What is SQL Injection Attack? Explain with one simple example.

(10) What is phishing? Explain different types of phishing attacks.

(11) What is port scanning? Explain various port scanning methods in detail.

(12) Short note on: Remote Administration Tools (RAT).

(13) What is sniffing? Explain its working process.

(14) Differentiate: Active sniffing V/s Passive Sniffing

(15) What is session hijacking? Explain various methods of session hijacking in detail.

***

Chapter 5

DIGITAL FORENSICS

5.1 INTRODUCTION TO DIGITAL FORENSICS

- INTRODUCTION
- WHAT IS DIGITAL FORENSIC?
- ADVANTAGES AND DISADVANTAGES OF DIGITAL FORENSICS

5.2 LOCARD'S PRINCIPAL OF EXCHANGE IN DIGITAL FORENSICS

- LOCARD'S PRINCIPLE IN FORENSIC SCIENCE
- LOCARD'S PRINCIPLE OF EXCHANGE IN DIGITAL FORENSICS
- LIMITATIONS OF LOCARD'S PRINCIPLE OF EXCHANGE

5.3 BRANCHES OF DIGITAL FORENSICS

- TYPES OF DIGITAL FORENSICS
  - ➲ COMPUTER FORENSICS
  - ➲ MEMORY FORENSICS
  - ➲ NETWORK FORENSICS
  - ➲ DATABASE FORENSICS
  - ➲ SOFTWARE FORENSICS
  - ➲ EMAIL FORENSICS
  - ➲ MALWARE FORENSICS
  - ➲ MOBILE FORENSICS

5.4 PHASES OF DIGITAL FORENSIC INVESTIGATION

- OBJECTIVES OF DIGITAL FORENSIC INVESTIGATION
- DIGITAL FORENSIC INVESTIGATION PROCESS MODEL

5.5 METHODS OF PRESERVING DIGITAL FORENSIC EVIDENCE

- WHY SHOULD WE PRESERVE DIGITAL EVIDENCE
- DIGITAL EVIDENCE PREVERSATION METHODS

5.1 INTRODUCTION TO DIGITAL FORENSICS

5.1.1 Introduction

We know that once a cyberattack has been occurred on our organization, it may create extreme confusion about cyberattack. You may need to answer some of the questions like how the attack happened, how it affects your data, and how to move forward from here. This information is vital to help both the criminal investigation and to increase your network security and prevent new attacks.

A digital forensics investigation is the first step toward the direction of answering these questions and also helped hundreds of organizations navigate the rough waters of a cyberattack.

5.1.2 What is Digital Forensics ?

"Digital forensics, also known as **computer forensics** or **cyber forensics**, is a branch of forensic science that deals with the investigation, collection, preservation, analysis, and presentation of digital evidence."

It involves the application of scientific methods and techniques to extract and interpret information from digital devices, networks, and online platforms for legal purposes. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases. A digital forensic investigation can help you answer any questions you might have about the attack, including

- What networks, systems, files, or applications were affected?
- How did the incident occur? (Tools, attack methods, vulnerabilities, etc.)
- What data and information were accessed or stolen?
- Are hackers still on my network? Is the incident finished, or is it ongoing?
- Where did the attack come from?

Example Uses of Digital Forensics

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

The goal is to establish a chain of custody for the digital evidence, ensuring its integrity and admissibility in legal proceedings.

5.1.3 Advantages and Disadvantages of Digital Forensics

Advantages of Digital Forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal actions in the court.

Disadvantages of Digital Forensics

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result.

5.2 LOCARD'S PRINCIPLE OF EXCHANGE IN DIGITAL FORENSICS

5.2.1 Locard's Principle of exchange in Forensic Science

Forensic science has changed the way crime investigations are handled. By examining and analysing the physical evidence and reconstructing the circumstances of the crime, forensic investigators are able to come up with scientific information that they can present in court. A person who is responsible for one of the most important principles in forensic science is Edmond Locard. He came up with the Locard's exchange principle or Locard's theory which states that

"Any action of an individual, and obviously, the violent action constituting the crime, cannot occur without leaving a trace."

A devout viewer of crime investigative series on television will be able to understand the importance of this principle. Haven't we all observed how the investigator goes to the site of a grisly murder and examines the crime scene, to check for blood stains, footprints or fingerprints, murder weapons and even the slightest of traces of blood in the nails? This is known as trace evidence, and according to Locard's principle whenever a crime is committed, trace evidence no matter how small or less, will always be present.

Locard's exchange principle is an important part of forensic science investigation.

"It states that any criminal leaves behind a trace when committing a violent crime. It is the investigator's duty to find this trace evidence and reconstruct the events of the crime."

The trace evidence can be divided into:

- Physical (clothing, glass fragments, paint chips etc)
- Biological (DNA, fingerprints, hair)
- Natural evidence (soil, pollen, seeds and plants)
- Digital evidence (Images, audio, video, files, hard disks etc...)

5.2.2 Locard's Principle of exchange in Digital Forensics

In digital forensics, Locard's Principle of Exchange is still applicable, and it emphasizes the idea that whenever two digital entities come into contact, there will be an exchange of materials or information. This principle serves as a foundational concept in digital investigations and highlights the importance of analysing the traces and artifacts left behind during digital interactions.

Here's how Locard's Principle of Exchange can be applied specifically to digital forensics:

1. **Digital Contact**
   - Whenever there is interaction between digital devices, systems, or users, there is a potential for an exchange of digital information.
   - Examples include file transfers, communication over networks, logins, data access, and other digital transactions.

2. **Exchange of Digital Evidence**
   - During digital interactions, data is created, modified, or deleted, leaving behind a trail of digital evidence.
   - This digital evidence can include files, logs, metadata, timestamps, network activity records, images, audio, video and other artifacts that reflect the nature of the interaction.
3. **Analysis of Digital Artifacts**
   - Digital forensics experts analyse these digital artifacts to reconstruct events, understand the series of actions, and identify relevant information for an investigation.
   - It involves examining file structures, computer system logs, network traffic, and other digital traces to piece together the timeline and details of a digital incident.
4. **Chain of Custody and Integrity**
   - Locard's Principle reinforces the importance of maintaining a secure chain of custody for digital evidence. This involves documenting the handling, storage, and transfer of digital evidence to ensure its integrity and admissibility in legal proceedings.
5. **Specialized Tools and Techniques:**
   - Digital forensics professionals use specialized tools and techniques to acquire, preserve, and analyse digital evidence.
   - These tools help investigators extract information from digital devices without altering the original data, maintaining the integrity of the evidence.

Overall, Locard's Principle of Exchange remains a guiding principle in digital forensics, emphasizing the inevitability of data exchange during digital interactions and highlighting the importance of skilful analysis of digital evidence in investigations.

5.2.2 Limitations of Locard's Principle of Exchange

One of the greatest drawbacks of Locard's exchange theory lies in evidence dynamics. This refers to the alteration of physical evidence before it has been examined by investigators.

There are many factors that can lead to the tampering and destruction of evidence.

- Staging (manipulation of objects in crime scene) by the offender
- Secondary transfer of evidence
- Actions of the victim before the crime
- Witness actions
- Natural factors like animal or insect activity, weather, decomposition.
- Fire suppression efforts
- Actions of police, scene technicians and medical personnel.

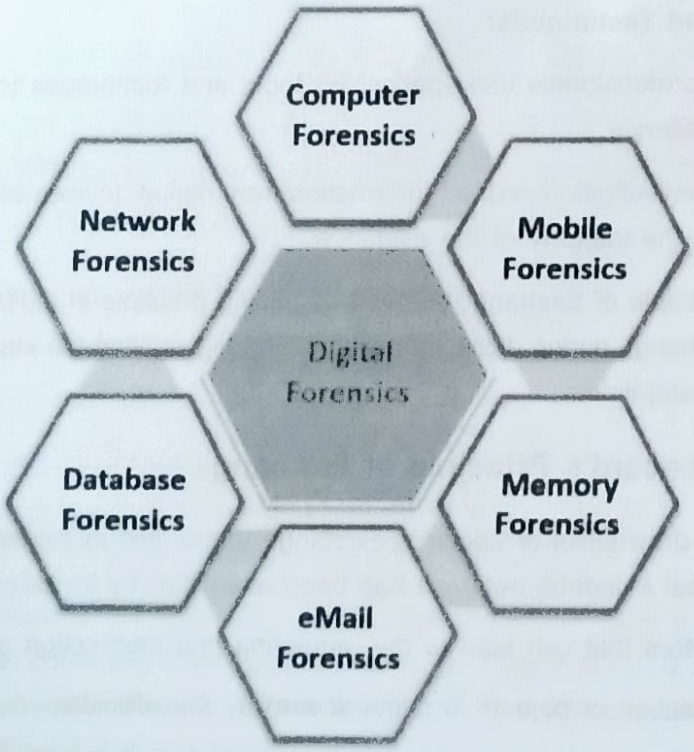
These factors can lead to the removal or obliteration of the evidence. They can often mislead the investigators and cause problems with crime reconstruction. Misinterpretations or misleading evidence can lead to inaccurate crime reconstruction. To avoid this, the investigator needs to make sure that the crime scene investigation and reconstruction is carried out with care.

5.3 BRANCHES OF DIGITAL FORENSICS

Digital forensics, also known as **computer forensics** or **cyber forensics**, is a branch of forensic science that deals with the investigation, collection, preservation, analysis, and presentation of digital evidence. Digital forensics plays a crucial role in modern criminal investigations and is often relied upon in legal proceedings. It helps in identifying perpetrators, proving guilt or innocence,recovering lost or deleted data, protecting digital evidence from tampering, and enhancing the overall integrity of the justice system in the digital age.

5.3.1 Types of Digital Forensics

Digital forensics encompasses various types or sub-disciplines based on the specific areas of focus and the nature of the investigation. Here are some common types of digital forensics:



[Fig. 5.1 : Branches of Digital Forensics]

Computer Forensics

This is the most well-known and widely practiced type of digital forensics. It involves the analysis and investigation of computer systems, including desktops, laptops, servers, and storage devices. Computer forensics aims to recover and examine digital evidence such as files, documents, emails, internet browsing history, and system logs to establish a timeline of events or support legal cases.

When conducting an investigation and analysis of evidence, computer forensics specialists use various techniques; here are some examples:

- **Deleted file recovery**

  This technique involves recovering and restoring files or fragments deleted by a person—either accidentally or deliberately—or by a virus or malware.

- **Reverse steganography**

  The process of attempting to hide data inside a digital message or file is called steganography. Reverse steganography happens when computer forensic specialists look at the hashing of a message or the file contents. A hashing is a string of data, which changes when the message or file is interfered with.

- **Cross-drive analysis**

  This technique involves analysing data across multiple computer drives. Strategies like correlation and cross-referencing are used to compare events from computer to computer and detect anomalies.

- **Live analysis**

  This technique involves analysing a running computer's volatile data, which is data stored in RAM (random access memory) or cache memory. This helps pinpoint the cause of abnormal computer traffic.

Memory Forensics

Memory forensics focuses on the analysis of a computer's volatile memory (RAM) to extract valuable information. Memory forensics is crucial in uncovering malicious activities or detecting sophisticated malware that may not be present on disk.

This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a **memory dump**. This file can then be taken offsite and searched by the investigator. It involves examining the contents of the memory at a given time to identify running processes, network connections, open files, passwords, encryption keys, and other volatile data.

This is useful because of the way in which processes, files and programs are run in memory, and once a snapshot has been captured, many important facts can be ascertained by the investigator, such as :

- Processes running
- Executable files that are running
- Open ports, IP addresses and other networking information
- Users that are logged into the system, and from where
- Files that are open and by whom

Memory forensics can be thought of as a current snapshot of a system that gives investigators a near real time image of the system while in use. Hard drive forensics is normally focused on data recovery and decryption, usually made from an image of the drive in question.

Network Forensics

Most of the attacks move through the network before hitting the target and they leave some trace. According to Locard's exchange principle, "every contact leaves a trace," even in cyberspace.

Network forensics deals with the examination of network traffic and data packets to investigate network-based security incidents or cybercrimes. It involves capturing, analysing, and interpreting network traffic to identify potential threats, unauthorized activities, or evidence of malicious actions. Network forensics can provide insights into network intrusions, data breaches, or other network-related offenses.

There are **two methods** of network forensics :

- **"Catch it as you can" method :** All network traffic is captured. It guarantees that there is no omission of important network events. This process is time-consuming and reduces storage efficiency as storage volume grows.
- **"Stop, look and listen" method :** Administrators watch each data packet that flows across the network but they capture only what is considered suspicious and deserving of an in-depth analysis. While this method does not consume much space, it may require significant processing power.

Investigators focus on **two primary sources**:

- **Full-packet data capture :** This is the direct result of the "Catch it as you can" method. Large enterprises usually have large networks and it can be counterproductive for them to keep full-packet capture for prolonged periods of time anyway
- **Log files :** These are the files which reside on web servers, proxy servers, Active Directory servers, firewalls, Intrusion Detection Systems (IDS), DNS and Dynamic Host Control Protocols (DHCP). Unlike full-packet capture, logs do not take up so much space.

Database Forensics

Database forensics is a branch of digital forensics that focuses specifically on the investigation and analysis of databases to uncover evidence related to cybercrimes, security breaches, or other malicious activities. It involves the systematic examination of database systems, structures, contents, and logs to identify, preserve, analyse, and present digital evidence that may be relevant to an investigation.

The different kind of activities performed during database forensics are as under:

- **Data Collection :** The process begins with the collection of data from the database systems under investigation. This may include capturing disk images, memory dumps, transaction logs, and database backups.
- **Data Preservation :** It's crucial to preserve the integrity of the data during the forensic investigation. This involves creating forensic copies of the original data to prevent any alterations or modifications that could compromise its evidentiary value.

- **Data Analysis and Reconstruction :** Forensic analysts examine the database contents and structures to reconstruct events, transactions, and user activities that may be relevant to the investigation. This may involve examining tables, records, metadata, and transaction logs to identify anomalies, unauthorized access, or suspicious activities.

- **Timeline Analysis :** Establishing a timeline of events is essential in database forensics. Analysts correlate timestamps from database logs, transaction records, and system logs to reconstruct the sequence of activities leading up to a security incident or data breach.

- **User and Access Analysis** : Investigators analyse user accounts, permissions, and access logs to determine who had access to the database, what actions they performed, and whether any unauthorized or suspicious activities occurred.

- **Data Recovery and Reconstruction :** In cases where data has been deleted, altered, or corrupted, forensic analysts may employ specialized techniques and tools to recover and reconstruct the original data or transactional history.

- **Documentation and Reporting :** Forensic findings are documented in detail, including the methods used, analysis results, conclusions, and recommendations. A forensic report is prepared to present the findings in a clear and understandable manner, which may be used as evidence in legal proceedings.

- **Legal Considerations :** Database forensics must adhere to legal and regulatory requirements governing the handling, preservation, and admissibility of digital evidence. This may involve obtaining proper authorization, maintaining chain of custody, and ensuring compliance with relevant privacy laws and regulations.

Overall, database forensics plays a crucial role in uncovering digital evidence, identifying perpetrators, and mitigating the impact of cyber incidents on organizations. It requires a combination of technical expertise, analytical skills, and adherence to legal standards to conduct thorough and effective investigations.

Mobile Device Forensics :

The term "mobile devices" encompasses a wide array of gadgets ranging from mobile phones, smartphones, tablets, and GPS units to wearables and PDAs. What they all have in common is the fact that they can contain a lot of user information.

Mobile devices are right in the middle of three booming technological trends: Internet of Things, Cloud Computing, and Big Data.

Nowadays, mobile device use is as pervasive as it is helpful, especially in the context of digital forensics, because these small-sized machines amass huge quantities of data on a daily basis, which can be extracted to facilitate the investigation. These machines allow digital investigators to glean a lot of information.

Information that resides on mobile devices :

- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related data, Wi-Fi information
- User dictionary content
- System files, usage logs, error messages
- Deleted data from all of the above

Mobile device forensics focuses on the extraction and analysis of digital evidence from smartphones, tablets, and other mobile devices. It involves the recovery of data such as call logs, text messages, multimedia files, location information, social media activity, and app usage. Mobile device forensics is particularly relevant in cases involving mobile-related crimes or when mobile devices are potential sources of evidence.

E mail Forensics

Due to the rapid spread of internet use all over the world, email has become a primary communication medium for many official activities. Not only companies, but also members of the public tend to use emails in their critical business activities such as banking, sharing official messages, and sharing confidential files. However, this communication medium has also become vulnerable to attacks.

The primary evidence in email investigations is the email header. The email header contains a considerable amount of information about the email like From, To Cc, Bcc, Subject, Date Reply-to, Message-id, References, and Received. This information becomes very vital for the email investigation activity.

Email forensics refers to analysing the source and content of emails as evidence. Investigation of email related crimes and incidents involves various approaches as discussed below.

- **Header Analysis :** Email header analysis is the primary analytical technique. This involves analysing metadata- data like sender, receiver, sending time etc. in the email header. It is evident that analysing headers helps to identify the majority of email-related crimes. Email spoofing, phishing, spam, scams and even internal data leakages can be identified by analysing the header.

- **Server Investigation :** This involves investigating copies of delivered emails and server logs. In some organizations they do provide separate email boxes for their employees by having internal mail servers. In this case, investigation involves the extraction of the entire email box related to the case and the server logs.
- **Network Device Investigation :** In some investigations, the investigator requires the logs maintained by the network devices such as routers, firewalls and switches to investigate the source of an email message. This is often a complex situation where the primary evidence is not perfect.
- **Software Embedded Analysis :** Some information about the sender of the email, attached files or documents may be included with the message by the email software used by the sender for composing the email. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF).
- **Sender Mail Fingerprints :** The "Received" field includes tracking information generated by mail servers that have previously handled a message, in reverse order. The "X-Mailer" or "User-Agent" field helps to identify email software. Analysing these fields helps to understand the software, and the version used by the sender.
- **Use of Email Trackers :** In some situations, attackers use different techniques and locations to generate emails. In such situations it is important to find out the geographical location of the attacker. To get the exact location of the attacker, investigators often use email tracking software embedded into the body of an Email.

When a recipient opens a message that has an email tracker attached, the investigator will be notified with the IP address and geographical location of the recipient. This technique is often used to identify suspects in murder or kidnapping cases, where the criminal communicates via email.

Malware forensics and Malware Analysis

Malware forensics is the process of examining the traces and artifacts left by malware on a compromised system or network. The goal of malware forensics is to identify the source, nature, and impact of the malware infection, and to collect evidence for legal or investigative purposes. Malware forensics typically involves acquiring and analysing disk images, memory dumps, network traffic, registry entries, logs, and other data that can reveal the malware's behaviour, origin, and targets. Malware forensics requires a thorough knowledge of operating systems, file systems, network protocols, and digital forensics tools and techniques.

Difference between Malware Forensics and Malware Analysis

Malware forensics and malware analysis are two related but distinct skills that can help you understand and counter malicious software. The differences between them are based on their goals, methods,tools and techniques used. These differences are discussed as under

1. **Working and Objectives :** Malware analysis is the process of dissecting and understanding the inner workings of a malware sample or code. The goal of malware analysis is to determine the

functionality, capabilities, and purpose of the malware, and to find ways to detect, remove, or mitigate it. Malware analysis typically involves reverse engineering, debugging, decompiling, or disassembling the malware code, and observing its execution in a controlled environment. Malware analysis requires a solid background in programming, assembly, binary formats, and malware analysis tools and frameworks.

2. **Type of analysis method used :** One of the main differences between malware forensics and malware analysis is the type of analysis they perform: static or dynamic. Static analysis refers to examining the malware without running it, while dynamic analysis refers to observing the malware while it is running.

   Malware forensics often relies on static analysis, as it can provide valuable information about the malware's characteristics, indicators, and persistence mechanisms without risking further infection or damage. Malware analysis often uses dynamic analysis, as it can reveal the malware's behaviour, logic, and communication patterns under different conditions and inputs.

3. **Tools and Techniques used :** Another difference between malware forensics and malware analysis is the tools and techniques they use. Malware forensics uses tools such as FTK Imager, EnCase, Autopsy, Volatility, Wireshark, and RegRipper to acquire and analyze various types of data from infected systems or networks. Malware analysis uses tools such as IDA Pro, Ghidra, OllyDbg, x64dbg, Radare2, Cuckoo Sandbox, and VirusTotal to examine and manipulate malware code or samples.

4. **When they are used ?** Malware forensics is often used in response to a malware incident, such as a ransomware attack, a data breach, or a cybercrime investigation. Malware analysis is often used in research or development of malware detection or mitigation solutions, such as antivirus software, firewall rules, or threat intelligence.

5. **Outcome of the technique :** The outcome of malware forensics is to provide a comprehensive report of the incident, including the timeline, scope, impact, attribution, and recommendations for recovery and prevention. The outcome of malware analysis is to provide a detailed description of the malware's features, functions, and weaknesses, and to develop signatures, patches, or countermeasures.

Both malware forensics and malware analysis also use techniques such as hashing, signature scanning, code obfuscation, encryption, unpacking, and sandboxing to deal with different challenges and scenarios.

Software Forensics

Software forensics is a branch of science that investigates computer software text codes and binary codes in cases involving patent infringement or theft. Software forensics can be used to support evidence for legal disputes over intellectual property, patents, and trademarks.

Software forensics is especially important in patent and trade cases. In these cases, someone might have copied another person's code, but rewritten that code in a way to hide the theft.

Cloud Forensics

Cloud forensics focuses on the investigation of digital evidence stored in cloud computing environments. It involves extracting and analysing data from cloud storage, virtual machines, and other cloud-based services. Cloud forensics addresses the unique challenges of investigating data stored remotely in shared environments and requires specific expertise in handling cloud-based evidence.

Multimedia Forensics

Multimedia forensics deals with the analysis and authentication of digital images, audio recordings, video recordings, and other forms of multimedia. It involves techniques such as image analysis, video forensics, audio forensics, and steganography analysis to determine the authenticity, integrity, or origin of multimedia files.

These are just a few examples of the different types of digital forensics. Depending on the nature of the investigation and the specific digital artifacts involved, other specialized areas of digital forensics may include email forensics, social media forensics, IoT forensics, and more. Each type requires specialized tools, techniques, and expertise to effectively analyse and interpret digital evidence within its respective domain.

5.4 PHASES OF DIGITAL FORENSIC INVESTIGATION

Digital forensics, also known as **computer forensics** or **cyber forensics**, is a branch of forensic science that deals with the investigation, collection, preservation, analysis, and presentation of digital evidence.

It involves the application of scientific methods and techniques to extract and interpret information from digital devices, networks, and online platforms for legal purposes.

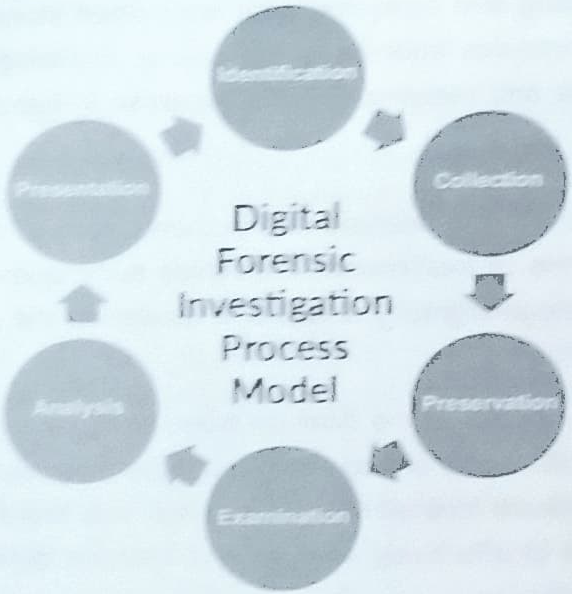
5.4.1 Objectives of Digital Forensic Investigation

The **objectives** of the Digital Forensics Investigation are as under:

- The primary goal of digital forensics is to identify, preserve, and analyse digital evidence to support investigations and legal proceedings.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim.
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

5.4.2 Digital Forensic Investigation Process Model

The Digital Forensic investigation process is carried out as the model shown in the figure 5.2.



[Fig. 5.2 : Digital Forensic Investigation Process Model]

- **Identification and Collection :** The first step is to identify the purpose of investigation, identify the required resources, and to identify potential sources of digital evidence and collect relevant data from the identified sources.

  This includes to find out what evidence is present, where it is stored and lastly how it is stored. It also includes seizing and imaging digital devices, making backups, and capturing network traffic.

- **Preservation :** Digital evidence is fragile and can be easily modified or destroyed. Preservation involves taking measures to protect the integrity and original state of the evidence. So, data is isolated, secured, and preserved.

  This includes creating forensic images, hashing, and storing the evidence in a secure and controlled environment and preventing people from using the digital device so that digital evidence is not tampered with.

- **Analysis :** In this phase, the collected digital evidence is analysed using specialized tools and techniques. This can involve recovering deleted files, examining system logs, analysing network traffic, decrypting encrypted data, and reconstructing digital activities to establish a timeline of events.

- **Examination (Interpretation) :** The analysis results are interpreted to draw conclusions and establish the significance of the evidence. This includes identifying relevant information, establishing links between different pieces of evidence, and identifying potential suspects or leads.

- **Presentation (Documentation and Reporting) :** A comprehensive report is prepared detailing the findings of the investigation. This report is often presented in a clear and concise manner to assist legal professionals, law enforcement agencies, or other stakeholders in understanding the technical aspects of the case.

Digital forensics plays a crucial role in modern criminal investigations and is often relied upon in legal proceedings. It helps in identifying perpetrators, proving guilt or innocence, recovering lost or deleted data, protecting digital evidence from tampering, and enhancing the overall integrity of the justice system in the digital age.

It requires specialized knowledge, skills, and tools to ensure accurate and reliable results. Forensic investigators need to stay updated with the latest technologies, encryption methods, and forensic techniques to address the ever-evolving landscape of digital crimes.

5.5 METHOS TO PRESERVE DIGITAL EVIDENCE

5.5.1 Why Should We Preserve Digital Evidence ?

One of the greatest drawbacks of Locard's exchange theory lies in evidence dynamics. But there are many factors that can lead to the tampering and destruction of evidence.

- Staging (manipulation of objects in crime scene) by the offender
- Secondary transfer of evidence
- Actions of the victim before the crime
- Witness actions
- Natural factors like animal or insect activity, weather, decomposition
- Fire suppression efforts
- Actions of police, scene technicians and medical personnel.

These factors can lead to the removal or obliteration of the evidence. They can often mislead the investigators and cause problems with crime reconstruction. Misinterpretations or misleading evidence can lead to inaccurate crime reconstruction. To avoid this there is a need to preserve the digital evidence. Due to this fundamental importance of digital evidence preservation, it is necessary to preserve digital evidences in well-structured manner.

5.5.2 Digital Evidence Preservation Methods

In this section, we'll go over three techniques that forensics specialists might employ to protect any evidence before the analysis process begins.

Drive Imaging

Forensic investigators must first produce an image of the evidence before they can start examining it from a source. A forensic procedure called "drive imaging" involves an analyst making a bit-by-bit copy of the original disk.

The following considerations should be made by forensic professionals when examining an image:

- It is possible for crucial and recoverable data to remain on even erased drives

- Using forensic procedures, experts in the field of forensics can recover all erased files.
- Never examine the original media through forensic examination. Utilize the duplicate image for all operations.

Forensic investigators should construct the image for analysis using a "write blocker," which is a piece of hardware or software that aids in the forensic image's legal defensibility.

Hash Values

Cryptographic hash values such as MD5, SHA1, and others are produced when a forensic investigator prepares a picture of the evidence for analysis. Hash values are important because:

- They are used to confirm that the image is an exact reproduction of the source media and that it is authentic and intact.
- Hashing values are essential when introducing evidence in court since even the smallest change to the data will result in an entirely new hash value.
- A new hash value is generated for any modifications you make to a file on your computer, such as adding new content or changing an already-existing one.
- Analysts can use specialized software to obtain information that is not available in a standard file explorer window, such as the hash value and other file metadata.

In court, it could be questioned whether the evidence was tampered with if the hash values of the image and the original evidence do not match.

Chain of Custody

When forensic investigators gather and transfer media from the client, they should record all actions taken throughout the transfer of media and evidence on Chain of Custody (CoC) forms. They should also get signatures, the time and date of the media handoff. For the following reasons, completing CoC paperwork is imperative:

- The Certificate of Consistency (CoC) serves as proof that the image has been in known possession since its creation.
- A breach in the CoC renders the image's legal value and the analysis it contains void.
- It is troublesome if there are any gaps in the procession record, such as instances where the evidence was left unsupervised in an unguarded area or in plain sight.

5.5.3 Issues with Maintaining Digital Evidence

Some of the issues that arise with preserving evidence are as under.

- **Legal Admissibility**

  This poses the greatest risk. Digital media evidence should be placed under the CoC right away and quarantined if it is a piece of criminal evidence; an investigator can subsequently make an image.

- **Evidence Destruction**

  Future forensic analysis will depend on the program remaining accessible and not being removed from the system in the event that threat actors have installed an application on a server.

- **Media is still in Service?**

  If so, the longer it has been since the occurrence, the greater the chance is that important evidence will be destroyed.

5.6 CRITICAL STEPS IN PRESERVING DIDITAL EVIDENCE

Misinterpretations or misleading evidence can lead to inaccurate crime reconstruction. So, we need to follow a series of steps in order to preserve digital evidence, as even a small inattentive move could lead to a loss of evidence and the break of a case.

5.6.1 Critical Steps in Preserving Digital Evidence

This section will cover the essential actions that must be taken in order to prevent digital evidence loss before delivering the it to the forensic specialists. When it comes to digital evidence preservation, time is crucial.

1. **Do not change the current state of the device :** If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
2. **Power down the device :** In the case of mobile phones, If it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
3. **Do not leave the device in an open area or unsecured place :** Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
4. **Do not plug any external storage media in the device :** Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
5. **Do not copy anything to or from the device :** Copying anything to or from the device will cause changes in the slack space of the memory.
6. **Take a picture of the piece of the evidence :** Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
7. **Make sure you know the PIN/ Password Pattern of the device :** It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry their job seamlessly.
8. **Do not open anything like pictures, applications, or files on the device :** Opening any application, file, or picture on the device may cause losing the data or memory being overwritten.

9. **Do not trust anyone without forensics training :** Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.

10. **Make sure you do not Shut down the computer, If required Hibernate it :** Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

5.6.2 Key Points to Remember to Speed Up Preserving Evidence

For the evidence to be professionally acquired by forensics investigators, the device is either seized or a forensic copy is created at the site of the "crime" scene.

The important key points to remember to speed up the process of preserving digital evidence and ease out the process for the authorities:

- Prepare yourself to share your authentication codes like screen patterns and passwords.
- You may also need to share the device manuals, chargers, cables.
- Device interactions will the Internet can also be analysed to build a complete and most appropriate picture of overall activity.
- Have ownership of the device that you plan to submit to the police. In case you do not have the authority or you're not voluntarily submitting the device, then, in that case, Police may need to seize the device under their lawful powers.
- It is easier to share external memory storage than your devices with the police instead of giving your phone away every time, so it is recommended that you have an external memory configured for your phone.
- Regularly back-up your phone data and retain copies of these back-ups for future use. These will help you restore another handset or your phone if needs be at a later today, and also can help to log a trail of incidence.

5.7 ROLE OF DEVICES AS EVIDENCE IN DIGITAL FORENSICS

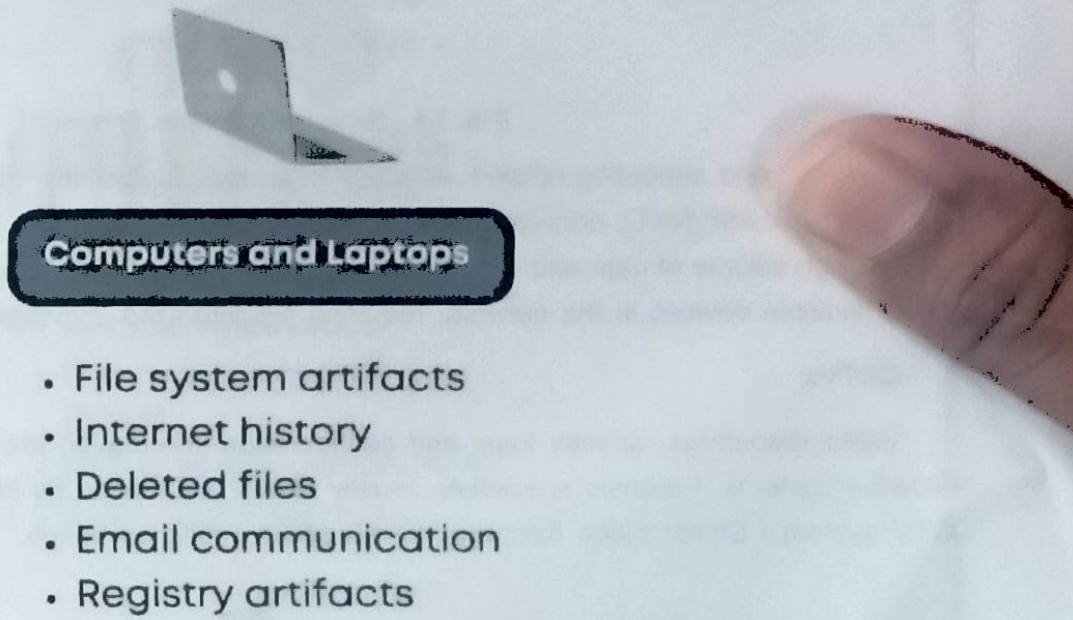
Digital forensic investigators must be adept at extracting evidence from an array of devices, each with unique structures, operating systems, storage capabilities, and security features. A case involving a desktop computer, for example, may require an understanding of operating systems, file systems, and data recovery techniques. Conversely, a case involving a smartphone may call for expertise in mobile operating systems, encryption, GPS technologies, and app data extraction. In network or cloud-based investigations, understanding data transmission, network protocols, cloud architectures, and multi-tenancy environments becomes critical. Thus, the device or system at the centre of the investigation often shapes the strategy and methodologies employed by the investigators.

5.7.1 Types of Devices

Digital forensics is not a single-size-fits-all discipline; it branches out into several areas, each addressing a specific kind of device or system. Some of them are as discussed under.

Computing Devices (Computers and laptops) :

Data preservation is the first step in computer forensics, and it is accomplished by making a forensic image of the system's storage devices. To guarantee data integrity, this procedure is usually carried out with the use of a write-blocking device. Next, the forensic picture is examined for files (both deleted and present), surfing history, email conversations, system logs, information (such as timestamps and file ownership), and metadata. These components may offer vital proof of the ownership, usage, and intent of the gadget.



[Fig. 5.3 : Computing Devices Forensics]

The main sources of difficulty in computer forensics are anti-forensic methods and encryption. Full-disk encryption is a common feature of modern computers that might keep investigators from accessing the data if they don't have the right encryption key.

Anti-forensic techniques, such as data wiping, data hiding, and obfuscation, can also be employed to complicate the investigation. Tools and strategies such as file carving, keyword searching, and hash comparison can help overcome these challenges.

Network Devices and Servers

Network forensics focuses on monitoring and analysing network traffic. Investigators can capture network packets in real-time or from saved logs, using tools like Wireshark or tcpdump. Analysing these packets can reveal suspicious activities, data exfiltration, or malicious network anomalies. Network devices also store log files, providing a record of network events, while servers may contain user data, website logs, and databases.

Network Devices and Servers

- Log files
- Network traffic
- Configuration files
- User account information
- System artifacts

[Fig. 5.4 : Networking Devices Forensics]

Tracking and attributing network activities to specific individuals can be challenging due to network address translation (NAT), proxies, VPNs, or anonymizing networks like Tor. Another challenge is dealing with the high volume of data and isolating relevant information. Furthermore, evidence might be distributed across multiple devices in the network, requiring synchronized investigation.

CCTVs

Video recordings, access logs, and configuration information are all available from closed-circuit television systems. Forensic specialists usually obtain information by taking off the hard drive from the CCTV system's Digital Video Recorder (DVR) and creating an Image.

Closed-Circuit Television Systems (CCTVs)

- Video footage
- System configuration
- Log files
- Timestamps and metadata
- Motion detection and alerts

[Fig. 5.5 : CCTV Forensics]

CCTV systems come with their own set of difficulties. For example, video footage is frequently recorded again and over again, making it more difficult to access older data. It may require sophisticated methods to retrieve overwritten or erased video. Moreover, video footage processing and analysis can take a long time, particularly in high-resolution systems where large amounts of data may be involved.

Automobiles:

Several onboard computers, referred to as Electronic Control Units (ECUs), are installed in modern cars and are in charge of multiple operations, including engine control, navigation, communications, and more. A portion of them, known as Event Data Recorders (EDRs), are able to offer vital event data before to, during, and following a collision, such as vehicle speed, brake application, airbag deployment, and seatbelt usage.

- Infotainment systems
- Vehicle telematics
- Event data recorders (EDRs)
- GPS and navigation data
- Connected services

[Fig. 5.6 : Vehicle Forensics]

In order to interface with these ECUs via the onboard diagnostics (OBD) port and other interfaces and understand the data that is collected, vehicle forensics requires specialist tools. The process is made much more difficult by the fact that these car systems are proprietary and there are many different manufacturers and models. For security reasons, a lot of car systems encrypt communications as well, which makes forensic extraction difficult.

Other than above discussed devices some other devices are also there like Smartphones and Tablets, Internet of Things (IoT) Devices, Wearables, Drones, Medical Devices, Device Memory, Gaming Consoles, Cloud Storage.

With the varied types of devices and systems involved in digital forensic investigations, a singular approach often proves insufficient. A more encompassing, holistic approach is necessary to conduct an effective and thorough investigation. This involves considering all the digital devices and systems relevant to the case and understanding how data from each device contributes to the overall picture.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What is Digital Forensic? List out information we collect by digital forensics.

(2) List out the examples of Digital Forensics uses.

(3) Write down Locard's principle of exchange in Digital Forensics.

(4) Write down limitations of Locard's principle of exchange.

(5) List out classification of trace evidence.

(6) Write down various branches of Digital Forensics.

(7) Write down objectives of Digital Forensic investigation.

(8) List out various phases of Digital Forensic Investigation process model.

(9) Why should we preserve Digital Evidence? List out three methods for preserving Digital Evidence.

(10) Write down issues which arise for maintaining Digital Evidence.

(11) List out essential actions which require to preserve Digital Evidence.

(12) List out points which be remembered to speed up the evidence preserving process.

(13) Write down the devices which play important role in Digital Forensic investigation.

Q 2. Answer the below long questions:

(1) What is Digital Forensic? Explain in detail with advantages and disadvantages.

(2) Explain Locard's principle of Digital Forensic with suitable example.

(3) Write down Locard's principle of Exchange in Forensic Science. Explain how it can be applied to Digital Forensics.

(4) Explain the Limitations of Locard's Principle of exchange.

(5) List out various branches of Digital Forensics. Explain Computer Forensics and memory Forensics in detail.

(6) Explain Network Forensics and Database Forensics in detail.

(7) Explain Mobile Device Forensics and E mail Forensics in detail.

(8) Explain Digital Forensics Investigation process model in detail.

(9) Why should we preserve Digital forensic evidence? Explain methods for evidence preservation.

(10) Explain essential actions which require to preserve Digital Evidence.

(11) Explain points which be remembered to speed up the evidence preserving process.

(12) Explain devices which play important role in Digital Forensic investigation.

* * *

Multiple Choice Questions (MCQs)

CHAPTER 1

INTRODUCTION OF INFORMATION SECURITY AND CRYPTOGRAPHY

1. What is the primary goal of information security ?

(A) Confidentiality (B) Integrity (C) Availability (D) All of the above

Ans. (D) All of the above

2. Which of the following is an example of a symmetric encryption algorithm ?

(A) RSA (B) AES (C) Diffie-Hellman (D) ECC

Ans. (B) AES

3. Which cryptographic hash function is commonly used for the purpose of password hashing ?

(A) MD5 (B) SHA-1 (C) SHA-256 (D) DES

Ans. (C) SHA-256

4. Which of the following is not a fundamental principle of information security ?

(A) Availability (B) Accessibility (C) Confidentiality (D) Integrity

Ans. (B) Accessibility

5. What does CIA stand for in the context of information security ?

(A) Central Intelligence Agency (B) Computer Incident Assessment

(C) Confidentiality, Integrity, Availability (D) Cybernetic Intrusion Assessment

Ans. (C) Confidentiality, Integrity, Availability

6. Which encryption algorithm is commonly used for secure communication over the internet ?

(A) DES (B) RSA (C) MD5 (D) Caesar cipher

Ans. (B) RSA

7. What is the primary purpose of a message digest in cryptography ?

(A) To encrypt messages (B) To compress messages

(C) To provide message integrity (D) To authenticate messages

Ans. (C) To provide message integrity

8. Which of the following is a characteristic of a cryptographic hash function?

(A) It is reversible (B) It produces a fixed-size output

(C) It requires a secret key for operation (D) It can be decrypted using a public key

Ans. (B) It produces a fixed-size output

9. Which cryptographic property ensures that a small change in the input to a hash function produces a significantly different output ?

(A) Collision resistance (B) Pre-image resistance

(C) Avalanche effect (D) Birthday paradox

Ans. (C) Avalanche effect

10. Which of the following is NOT a potential use case for cryptographic hash functions ?

(A) Password hashing (B) Digital signatures

(C) Data compression (D) Blockchain technology

Ans. (C) Data compression

CHAPTER 2

NETWORK AND SYSTEM SECURITY

1. What is the primary purpose of PGP ?

(A) Secure file transfer (B) Data compression

(C) Email encryption and digital signatures (D) Firewall protection

Ans. (C) Email encryption and digital signatures

2. Which attack involves tricking individuals into revealing sensitive information or performing actions through psychological manipulation ?

(A) Brute force attack (B) Social engineering attack

(C) SQL injection attack (D) Cross-Site Scripting (XSS) attack

Ans. (B) Social engineering attack

3. What is the primary purpose of SSL ?

(A) Encrypting email messages (B) Securing web communication

(C) Managing network traffic (D) Protecting databases

Ans. (B) Securing web communication

4. What is the primary purpose of a digital signature ?

(A) To encrypt the contents of a message

(B) To provide confidentiality to a digital document

(C) To ensure the identity of the sender

(D) To ensure authenticity and integrity of a digital document or message

Ans. (D) To ensure authenticity and integrity of a digital document or message

5. Which cryptographic key is used to create a digital signature ?

(A) Public key (B) Private key (C) Session key (D) Master key

Ans. (B) Private key

6. What does PGP stand for in the context of computer security?

(A) Public Gateway Protocol (B) Pretty Good Privacy

(C) Private Graphical Protocol (D) Protected Group Policy

Ans. (B) Pretty Good Privacy

7. What type of attack floods a network or system with excessive traffic, rendering it unavailable to legitimate users?

(A) Malware attack
(B) Phishing attack
(C) Denial-of-Service (DoS) attack
(D) Man-in-the-Middle (MitM) attack

Ans. (C) Denial-of-Service (DoS) attack

8. What type of attack injects malicious scripts into web pages viewed by other users, potentially stealing sensitive information?

(A) Brute force attack
(B) Social engineering attack
(C) SQL injection attack
(D) Cross-Site Scripting (XSS) attack

Ans. (D) Cross-Site Scripting (XSS) attack

9. Which firewall type inspects each packet passing through the firewall and accepts or rejects it based on predefined rules ?

(A) Stateful inspection firewall
(B) Proxy firewall
(C) Packet-filtering firewall
(D) Next-generation firewall

Ans. (C) Packet-filtering firewall

10. Which firewall type acts as an intermediary between internal and external networks, handling requests on behalf of clients ?

(A) Packet-filtering firewall
(B) Stateful inspection firewall
(C) Proxy firewall
(D) Next-generation firewall

Ans. (C) Proxy firewall

CHAPTER 3

CYBER CRIME

1. What is email bombing in the context of cybersecurity ?

(A) A technique to send a large volume of emails to a target system
(B) A method to encrypt email messages for secure transmission
(C) An approach to authenticate email servers
(D) A strategy to filter spam emails

Ans. (A) A technique to send a large volume of emails to a target system

2. What is the primary objective of a DDoS attack ?

(A) To steal sensitive information
(B) To gain unauthorized access to a system
(C) To overwhelm server resources and disrupt services
(D) To encrypt network traffic

Ans. (C) To overwhelm server resources and disrupt services

3. What is phishing in the context of cybersecurity ?
   (A) A technique to encrypt sensitive data during transmission
   (B) A method to secure network communication
   (C) An attack for tricking individuals into revealing sensitive information
   (D) A process to authenticate email servers

Ans. (C) An attack for tricking individuals into revealing sensitive information

4. Which encryption protocol can help prevent unauthorized access to website content during transmission?
   (A) HTTP (Hypertext Transfer Protocol)
   (B) FTP (File Transfer Protocol)
   (C) SSL/TLS (Secure Sockets Layer/Transport Layer Security)
   (D) SMTP (Simple Mail Transfer Protocol)

Ans. (C) SSL/TLS (Secure Sockets Layer/Transport Layer Security)

5. What is web jacking in the context of cybersecurity ?
   (A) A technique to hijack web servers and host malicious content
   (B) An attack that redirects users to fraudulent websites
   (C) A method to steal sensitive information from web applications
   (D) An attack that takes control of a website's domain or content

Ans. (D) An attack that takes control of a website's domain or content

6. What is the purpose of anti-phishing software ?
   (A) To encrypt email messages for secure transmission
   (B) To prevent unsolicited commercial emails
   (C) To detect and block phishing emails and websites
   (D) To improve network performance

Ans. (C) To detect and block phishing emails and websites

7. What is credit card fraud ?
   (A) A legitimate transaction conducted with a credit card
   (B) Fraudulent use of a credit card or its information for financial gain
   (C) The process of securely storing credit card information
   (D) A type of insurance provided by credit card companies

Ans. (B) Fraudulent use of a credit card or its information for financial gain

8. What is card skimming in the context of credit card fraud ?
   (A) A method of duplicating physical credit cards
   (B) Sending unsolicited emails to obtain credit card information
   (C) Intercepting communication between a user and a payment gateway
   (D) Creating fake websites to trick users into entering credit card details

Ans. (A) A method of duplicating physical credit cards

9. What does Section 65 of the IT Act, 2008, primarily address?

(A) Cyberbullying offenses

(B) Unauthorized access to computer systems

(C) Offenses related to tampering with computer source documents

(D) Data privacy violations

Ans. (C) Offenses related to tampering with computer source documents

10. What is the punishment prescribed under Section 65 of the IT Act, 2008, for offenses related to tampering with computer source documents?

(A) Imprisonment for up to 3 years or a fine of up to Rs. 2,00,000, or both

(B) Imprisonment for up to 5 years or a fine of up to Rs. 5,00,000, or both

(C) Imprisonment for up to 7 years or a fine of up to Rs. 10,00,000, or both

(D) Imprisonment for up to 2 years or a fine of up to Rs. 1,00,000, or both

Ans. (A) Imprisonment for up to 3 years or a fine of up to Rs. 2,00,000, or both

11. What is the primary focus of Section 66 of the IT Act, 2008 ?

(A) Unauthorized access to computer systems

(B) Protection of digital signatures

(C) Offenses related to hacking and computer data theft

(D) Regulation of electronic commerce

Ans. (C) Offenses related to hacking and computer data theft

CHAPTER 4

ETHICAL HACKING

1. What is the primary goal of an ethical hacker ?

(A) To cause harm to computer systems

(B) To gain unauthorized access to sensitive information

(C) To identify and remediate security vulnerabilities

(D) To create chaos in the digital environment

Ans. (C) To identify and remediate security vulnerabilities

2. Which type of hacker is also known as a "white hat" hacker ?

(A) Black hat hacker (B) Gray hat hacker

(C) Script kiddie (D) Ethical hacker

Ans. (D) Ethical hacker

3. Which of the following is a penetration testing tool included in Kali Linux ?

(A) Adobe Photoshop (B) Microsoft Word

(C) Wireshark (D) Mozilla Firefox

Ans. (C) Wireshark

4. What is the default username and password for Kali Linux ?

(A) Username: kali, Password: toor (B) Username: root, Password: kali

(C) Username: admin, Password: admin (D) Username: user, Password: password

Ans. (A) Username: kali, Password: toor

5. Which of the following is an example of a password hashing algorithm used for password storage ?

(A) MD5 (Message Digest Algorithm 5) (B) DES (Data Encryption Standard)

(C) ROT13 (Rotate by 13 places) (D) Base64 encoding

Ans. (A) MD5 (Message Digest Algorithm 5)

6. What is password cracking ?

(A) Generating complex passwords for security purposes

(B) Recovering lost passwords from encrypted files

(C) Creating new passwords using machine learning algorithms

(D) Illegally accessing password databases

Ans. (B) Recovering lost passwords from encrypted files

7. What is an injection attack in the context of cybersecurity?

(A) Injecting physical devices into computer systems

(B) Injecting malware into network traffic

(C) Injecting malicious code or commands into input fields or data streams

(D) Injecting cryptographic keys into encryption algorithms

Ans. (C) Injecting malicious code or commands into input fields or data streams

8. Which of the following is a defence mechanism against SQL injection attacks ?

(A) Input validation and sanitization

(B) Enforcing weak password policies

(C) Disabling firewalls

(D) Ignoring security warnings from web browsers

Ans. (A) Input validation and sanitization

9. Which of the following is NOT a feature of RAT tools?

(A) Keylogging (B) Screen capturing

(C) File encryption (D) Webcam hijacking

Ans. (C) File encryption

10. Which of the following is an example of a well-known RAT tool ?

(A) BitTorrent (B) TeamViewer

(C) Adobe Photoshop (D) VLC Media Player

Ans. (B) TeamViewer

11. What is a Remote Access Trojan (RAT) tool primarily used for ?

(A) Automated testing of network vulnerabilities

(B) Monitoring network traffic for security threats

(C) Remotely controlling and accessing compromised systems

(D) Encrypting sensitive data during transmission

Ans. (C) Remotely controlling and accessing compromised systems

CHAPTER 5

DIGITAL FORENSICS

1. What is digital forensics primarily concerned with ?

(A) Recovering lost data from physical storage devices

(B) Investigating crimes involving digital devices and data

(C) Creating backups of important files and documents

(D) Preventing cyber-attacks on network infrastructure

Ans. (B) Investigating crimes involving digital devices and data

2. What is the first step in the digital forensic process ?

(A) Analysis (B) Collection (C) Examination (D) Reporting

Ans. (B) Collection

3. What is steganography in the context of digital forensics ?

(A) The study of cryptographic algorithms

(B) The practice of hiding data within other data

(C) The process of recovering deleted files

(D) The examination of digital artifacts

Ans. (B) The practice of hiding data within other data

4. Which of the following types of information can be obtained through memory forensics ?

(A) Recently deleted files

(B) Internet browsing history

(C) Running processes and open network connections

(D) Encrypted email messages

Ans. (C) Running processes and open network connections

5. Which of the following best describes Locard's Exchange Principle ?

(A) "Every contact leaves a trace."

(B) "Evidence is the key to solving crimes."

(C) "Criminals always return to the scene of the crime."

(D) "The guilty party will always confess under interrogation."

Ans. (A) "Every contact leaves a trace."

6. What is the difference between static and live digital forensics analysis ?

(A) Static analysis involves examining data in real-time, while live analysis involves analysing archived data.

(B) Static analysis involves analysing data stored on physical devices, while live analysis involves examining data in volatile memory.

(C) Static analysis is conducted by law enforcement agencies, while live analysis is performed by private investigators.

(D) Static analysis is more time-consuming than live analysis.

Ans. (B) Static analysis involves analysing data stored on physical devices, while live analysis involves examining data in volatile memory.

7. What is the purpose of creating a forensic image of digital evidence ?

(A) To delete unnecessary files

(B) To encrypt the evidence for security

(C) To preserve the original state of the evidence

(D) To share evidence across multiple platforms

Ans. (C) To preserve the original state of the evidence

8. Which of the following devices is commonly used in digital forensics for data acquisition?

(A) USB mouse (B) External hard drive

(C) Laser printer (D) Webcam

Ans. (B) External hard drive

9. Which of the following devices is often used for creating forensic images of storage media ?

(A) USB flash drive (B) CD-ROM drive

(C) Write-blocking device (D) Forensic imaging tool

Ans. (D) Forensic imaging tool

10. Which of the following is an example of volatile digital evidence ?

(A) Hard disk drive (B) Random access memory (RAM)

(C) Solid-state drive (SSD) (D) Optical disc

Ans. (B) Random access memory (RAM)

★ ★ ★

Seat No. : _____ Enrolment No. _____

Subject Code : 4361601 **Date :**

Subject Name : CYBER SECURITY AND DIGITAL FORENSICS

Time : **Total Marks : 30**

Instructions :

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

MODEL QUESTION PAPERS-1

		Marks	CO (Course Outcome)
Q. 1	**(a)** Explain fundamental goals of Information Security.	03	COa
	(b) Explain Hashing with its working diagram and list out applications of Hashing.	07	COa
Q. 2	**(a)** Differentiate: Active Attack V/s Passive Attack	03	COb
	(b) Write a short note on Digital Signature.	07	COb
	OR		
	(b) What is firewall? Explain Packet filtering firewall with its working in detail.	07	COb
Q. 3	**(a)** Differentiate: Symmetric Cryptography V/s Asymmetric Cryptography.	03	COa
	(b) Explain e mail bombing in detail	07	COc
	OR		
Q. 3	**(a)** What is Virus? Explain with its lifecycle and types.	03	COb
	(b) Explain DOS Attack and DDOS attack with differentiation.	07	COc

* * *

Seat No. : _____ Enrolment No. _____

Date :

Subject Code : 4361601

Subject Name : CYBER SECURITY AND DIGITAL FORENSICS

Total Marks : 30

Time :

Instructions :

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

MODEL QUESTION PAPERS-2

		Marks	CO (Course Outcome)
Q.1	(a) Explain Section 65 in brief.	03	COc
	(b) Explain challenges and preventions of Cybercrime.	07	COc
Q.2	(a) What is hacking? Explain various types of hacking.	03	COd
	(b) What is SQL Injection Attack? Explain with one simple example.	07	COd
	OR		
	(b) What is phishing? Explain different types of phishing attacks.	07	COd
Q.3	(a) What is Digital Forensics? List out its advantages and Disadvantages.	03	COe
	(b) Explain Digital Forensic Investigation method in detail.	07	COe
	OR		
Q.3	(a) Differentiate: Malware Forensics V/s Malware Analysis.	03	COe
	(b) Explain Digital Evidence preservation methods in detail.	07	COe

* * *