

UNIT 2: CYBER FORENSICS NOTES

Cyber Forensics : -

Cyber Forensics, also known as digital forensics, is the practice of collecting, preserving, and analyzing digital evidence from electronic devices to uncover information related to criminal activities. It involves examining computers, mobile phones, servers, and storage devices to identify, collect, and preserve evidence in a way that maintains its integrity for use in legal proceedings. Cyber forensics plays a critical role in investigating crimes such as hacking, fraud, cyberbullying, intellectual property theft, and even terrorism.

Forensics specialists use a variety of techniques to extract data from digital devices while ensuring that the original evidence is not altered. For example, in a case of financial fraud, forensic experts can analyze emails, text messages, and transaction records from a suspect's device to uncover how the crime was carried out. This evidence is essential in proving the criminal activity in court. They rely on specific tools and procedures, such as hash functions and chain of custody, to ensure that the evidence remains legally admissible.

A typical cyber forensics investigation follows a series of steps, including the identification of the crime, collection of digital evidence, analysis of the data, and presentation of findings in a legal format. These steps are crucial in ensuring the evidence is not tampered with, and that the results are verifiable. By analyzing the metadata, timestamps, file systems, and hidden data, forensic investigators can uncover the truth behind cybercrimes.

Digital Device : -

A digital device refers to any electronic device capable of storing, processing, or transmitting data. Examples include smartphones, laptops, tablets, digital cameras, and USB drives. Digital devices store vast amounts of personal, financial, and operational data, making them essential sources of evidence in cyber forensics investigations. These

UNIT 2: CYBER FORENSICS NOTES

devices are often involved in criminal activities, from illegal file sharing and fraud to cyberbullying and hacking.

When investigators receive a digital device as part of a criminal investigation, they use specialized tools to extract and analyze the data stored within it. In cases of financial fraud, for example, investigators might examine a suspect's smartphone for transaction records, messages, and calls that could serve as evidence. Forensic experts can retrieve deleted data, uncover hidden files, or trace locations and movements based on GPS data embedded in photos or apps. The data from mobile devices is often encrypted, and investigators may need to use decryption tools to unlock the contents.

Digital forensics experts also look for traces of malware, Trojans, or viruses that could have been installed on the device. In cases where a digital device is used to commit crimes like hacking, investigators examine the device's operating system for signs of unauthorized access or hidden files. One key aspect of forensic analysis is ensuring the chain of custody of the device and the data it contains. This is important to maintain the integrity of the evidence and ensure that the data remains unaltered during the analysis.

The analysis of digital devices in forensics often extends to the examination of internet activity, including web browsing history, social media interactions, and file downloads, to understand the context of a crime. This is especially relevant in cases involving cyberstalking, identity theft, and data breaches.

Hard Disk : -

A hard disk is a primary storage device used in computers to store data, such as operating systems, applications, and user files. It consists of one or more spinning disks (platters) coated with a magnetic material that stores data in the form of bits. The hard disk is essential for both everyday use and forensic investigations, as it stores crucial data that may serve as evidence in criminal cases.

In cyber forensics, the hard disk is often the first place investigators examine, as it holds detailed records of all system activities, including files, user actions, and system events. Forensic experts use specialized tools to clone or image the hard disk to create an exact replica of the data, ensuring that the original device remains unaltered. This process is essential for maintaining the integrity of evidence, as any modification to the original disk could lead to the evidence being disqualified in court.

UNIT 2: CYBER FORENSICS NOTES

The hard disk contains various file systems (e.g., NTFS, FAT32) that dictate how files are organized, stored, and retrieved. Cyber forensics experts analyze these file systems to locate both active and deleted files. In many cases, even deleted files can be recovered by forensic tools that scan the unallocated space on the disk, where the data resides until it's overwritten. These tools allow investigators to retrieve documents, emails, and images that the user thought were deleted, providing critical evidence in investigations.

Metadata, which is information about files (such as creation dates, last access times, and modification logs), is another valuable source of information in forensics. For example, the metadata on a file can help investigators establish timelines of activities, such as when a document was created or edited, and potentially uncover evidence of a crime.

In cases of cybercrimes like hacking, the hard disk's logs may also reveal unauthorized access or installation of malware. These logs contain timestamps of system events, user login records, and changes made to the system, which can point to an attacker's activity.

Disk Characteristics : -

Disk characteristics refer to the unique features of a hard disk, such as its storage capacity, file system structure, physical composition, and read/write speeds. These characteristics are vital in cyber forensics because they help forensic experts understand how the disk is organized and where to look for specific data. Forensic investigators must be familiar with these characteristics to recover, preserve, and analyze data effectively.

One of the primary disk characteristics is the **storage capacity**, which refers to the total amount of data the disk can hold. Larger disks typically store more data and, therefore, more potential evidence. For example, a suspect's computer with a 1TB hard disk may hold vast amounts of data, including emails, photos, documents, and system logs, all of which could be relevant to an investigation.

The **file system** is another crucial disk characteristic. Common file systems like NTFS (used in Windows) or HFS+ (used in macOS) define how data is organized on the disk. Forensic investigators must understand these systems to properly analyze the stored data. For example, the file system determines how data is stored in clusters, how deleted files are handled, and how metadata is tracked.

UNIT 2: CYBER FORENSICS NOTES

Another important characteristic is **disk partitioning**, which refers to how a disk is divided into sections or partitions. These partitions can separate operating systems, files, and other data, making it easier to isolate evidence during an investigation. For instance, an investigator might discover a hidden partition used for storing illicit data or malware in a criminal case.

The **physical characteristics** of a disk, including the type (HDD vs. SSD) and its physical state (damaged or intact), also play a role in forensics. Solid-state drives (SSDs), for example, store data differently from traditional hard drives, which can impact the recovery process. Forensic experts must use appropriate techniques and tools to extract data from these devices.

Disk Imaging

Disk imaging is the process of creating a bit-by-bit copy (image) of a hard disk, which is essential in cyber forensics. By making an exact replica of the original disk, investigators can analyze the data without altering the original evidence. This method is crucial for maintaining the integrity of the data, as even a small change to the original disk could result in the evidence being compromised.

In a typical investigation, forensic experts first create an image of the suspect's hard disk using specialized tools like FTK Imager or EnCase. This image is stored on a separate device, such as a write-protected external hard drive, to ensure that the original disk remains untouched. Investigators then analyze the image instead of the original disk to uncover evidence. This process ensures that any data extracted from the disk is admissible in court, as it can be demonstrated that the original disk was not altered.

Disk imaging is particularly useful when investigators are dealing with large volumes of data or complex storage structures. By creating an image, they can work with the data offline, allowing them to carefully examine each file, recover deleted files, and search for hidden evidence like passwords, documents, or even encrypted files. For example, in a case involving child exploitation, investigators may use disk imaging to recover deleted images or videos from a suspect's hard disk.

UNIT 2: CYBER FORENSICS NOTES

Step by Step Practical

Pcap file Analysis – Case Study

Step-by-Step PCAP File Analysis Using Kali Linux: Case Study

Packet capture (PCAP) files contain raw data packets transmitted over a network. Analyzing PCAP files helps in identifying malicious activity, troubleshooting network issues, and investigating security breaches. Kali Linux, with its wide range of network analysis tools, is a powerful operating system for conducting such analysis. Below is a detailed step-by-step process for analyzing a PCAP file using Kali Linux, with a case study to help understand the process.

1. Set Up Kali Linux

Ensure you have Kali Linux installed and configured on your system. Kali Linux includes a suite of tools that are crucial for network security and packet analysis. For PCAP analysis, we will be using **Wireshark** and **tcpdump** — two of the most common tools.

- **Wireshark**: A popular graphical network protocol analyzer.
- **tcpdump**: A command-line tool for network packet analysis.

2. Obtain the PCAP File

For the purpose of this case study, let's assume that we have a PCAP file called **malicious_traffic.pcap** captured from a network suspected of being compromised by a hacker. This PCAP file contains all network traffic, including HTTP, DNS requests, and malicious attempts.

UNIT 2: CYBER FORENSICS NOTES

You may acquire PCAP files from intrusion detection systems (IDS), firewall logs, or network monitoring tools.

3. Open the PCAP File Using Wireshark

- Open a terminal in Kali Linux and launch **Wireshark** using the command:

wireshark

- After Wireshark opens, navigate to **File > Open**, then select the `malicious_traffic.pcap` file.
- Wireshark will begin loading the file, displaying the list of network packets in real-time. The packets include detailed information about network traffic, such as the source IP, destination IP, protocol, and payload.

4. Inspect the Packets

Once the file is loaded in Wireshark, you can start analyzing the traffic. Here are the key steps to begin your inspection:

- **Filter Traffic:** Use filters to isolate specific traffic types or protocols. For example, to view only HTTP traffic, use the filter:
http
- **Identify Suspicious Traffic:** Look for abnormal activity such as unusual port numbers, high traffic volumes, or unknown protocols. In our case study, you might notice many HTTP requests to an unknown server or multiple failed login attempts.
- **Examine Packet Details:** Click on individual packets to inspect detailed information. For example, by clicking on an HTTP packet, you can see the full headers, the request method (e.g., GET, POST), and the content being transferred. This can help you identify if sensitive information (like login credentials or personal data) is being transmitted in an insecure manner.

UNIT 2: CYBER FORENSICS NOTES

5. Follow the TCP Stream

Wireshark provides an option to **Follow the TCP Stream**, which allows you to reconstruct the entire conversation between two systems. This is particularly useful when analyzing malware activity or data exfiltration.

- Right-click on a suspicious TCP packet and select **Follow > TCP Stream**.
- Wireshark will show the entire communication between the two endpoints (e.g., a command and control server and an infected client).

If the communication is encrypted (e.g., HTTPS), you might need to decrypt the traffic, which is a more advanced step that involves using SSL keys.

6. Analyze Malicious Indicators

In our case study, suppose the traffic reveals several key indicators of a security breach, such as:

- **Suspicious DNS Requests:** The malware might be using DNS tunneling to send and receive commands from a remote server. You can filter for DNS traffic (**dns**) and look for unusual domains being queried.
- **Command and Control (C&C) Communication:** Look for unusual connections to external IP addresses that are not part of the organization's normal traffic. These could be signs of a botnet or a remote access trojan (RAT).
- **Unusual HTTP Requests:** If there are HTTP requests with payloads that look like executable commands, this could be a sign of malware or a backdoor trying to download further payloads.
- **Port Scanning Attempts:** If there is unusual traffic with many failed connection attempts to multiple IP addresses and ports, this could indicate a port scan or brute-force attack.

UNIT 2: CYBER FORENSICS NOTES

7. Export and Save Analysis Data

Wireshark allows you to export specific information from the captured packets. You may want to save particular packets or streams for further analysis. For example:

- **Export Specific Packets:** Right-click a packet and choose **Export Packet Dissections > As Plain Text** to save the details.
- **Save Filters:** If you apply a filter to identify suspicious traffic, you can save the filtered packets by going to **File > Export Specified Packets**.

You can also save an entire TCP stream (conversation) to investigate the attack vector further.

8. Use tcpdump for Command-Line Analysis

If you prefer command-line tools, **tcpdump** is an efficient tool to capture and analyze network traffic in real-time.

- To analyze a PCAP file with tcpdump, use the following command:

nginx

CopyEdit

```
tcpdump -r malicious_traffic.pcap
```

This will display all the packets in the terminal. You can apply filters like:

```
tcpdump -r malicious_traffic.pcap port 80
```

9. Correlate Data with Other Logs

For a comprehensive investigation, it is useful to correlate the data found in the PCAP file with other logs from IDS systems, firewalls, or endpoint security tools. For example:

UNIT 2: CYBER FORENSICS NOTES

- **Firewall Logs:** Cross-reference any suspicious IP addresses from the PCAP analysis with firewall logs to see if they were blocked.
- **IDS/IPS Logs:** Look for any alerts related to the traffic you identified in Wireshark or tcpdump.
- **Host Logs:** If the compromised system was an endpoint, correlate the traffic patterns with local system logs (such as `/var/log/auth.log` or Windows Event Logs).

10. Document Findings and Create a Report

Once the analysis is complete, you should document your findings. This report should include:

- **Summary of the Incident:** A description of the suspicious traffic and the possible attack method (e.g., data exfiltration, malware infection).
- **Timeline of Events:** A timeline showing key events, such as when suspicious packets were first observed and when they stopped.
- **Malicious Indicators:** IP addresses, domains, protocols, and ports associated with the malicious activity.
- **Recommendations:** Steps to mitigate the attack, such as blocking the identified IP addresses, improving network segmentation, or updating firewall rules.

Conclusion of the Case Study

In this case study, we used **Wireshark** and **tcpdump** on Kali Linux to analyze a PCAP file that revealed suspicious traffic patterns, including unusual DNS requests, abnormal HTTP requests, and command-and-control traffic. This analysis helped us identify a malware infection that was communicating with an external server. By documenting the findings and correlating them with other security logs, we were able to piece together a clear picture of the attack and provide recommendations for preventing future breaches.

UNIT 2: CYBER FORENSICS NOTES

The ability to analyze PCAP files effectively is a crucial skill in cybersecurity and digital forensics, enabling investigators to uncover malicious activity and gather evidence to support legal action.

2. Network Port Scan – Forensics

Network Port Scan – Forensics using Kali Linux : -

Port scanning is a technique used to identify open ports and services running on a remote machine or network. It is commonly used by attackers to find vulnerabilities in a system that they can exploit. In forensic investigations, port scanning is used to detect unauthorized scanning activities and track intrusions. Kali Linux, a penetration testing distribution, provides a variety of tools that can be used for network port scanning and forensic analysis.

Here's a step-by-step guide on how to perform a network port scan forensics using Kali Linux:

Step 1: Setting Up Kali Linux

1. **Install Kali Linux:** Download and install Kali Linux on a physical machine, virtual machine, or live USB. You can download it from the official Kali Linux website (<https://www.kali.org>).
2. **Update Kali Linux:** Run the following command to ensure your Kali system is up to date

```
sudo apt update && sudo apt upgrade
```

Step 2: Identifying the Target

Before performing a port scan, you need to identify the target system's IP address or network range. You can do this by:

UNIT 2: CYBER FORENSICS NOTES

- Using tools like **nmap** to scan a range of IP addresses.
- Use the **ifconfig** command to determine the IP address of your local machine.
- Alternatively, you can use the **ip** command to get the IP address on Kali Linux.

For example, run:

```
ifconfig
```

Step 3: Performing a Network Port Scan with Nmap

Kali Linux comes with a built-in port scanner called **Nmap** (Network Mapper). You can use Nmap to scan for open ports on the target system.

1. **Basic Port Scan:** To scan a single IP address (e.g., 192.168.1.1) for open ports, run:

```
nmap 192.168.1.1
```

This will show the open ports on the target system. Nmap will perform a SYN scan by default, meaning it will try to send SYN packets to the target and check for responses.

2. **Scan Specific Ports:** To scan specific ports, use the **-p** option. For example, to scan ports 80 (HTTP), 443 (HTTPS), and 22 (SSH), run:

```
nmap -p 22,80,443 192.168.1.1
```

3. **Scan a Range of IPs:** If you want to scan a range of IP addresses (e.g., 192.168.1.1 to 192.168.1.50), you can run:

```
nmap 192.168.1.1-50
```

4. **Scan All Ports:** To scan all 65535 ports on the target system, use the **-p-** option:

```
nmap -p- 192.168.1.1
```

UNIT 2: CYBER FORENSICS NOTES

Step 4: Identifying Port Scanning Activity

In forensic investigations, detecting unauthorized port scans on a network is crucial. After performing a port scan on a target system using Nmap, you need to identify if an attack was carried out or if a legitimate scan has occurred. You can check for signs of network scans in the following ways:

1. **Analyze Firewall Logs:** Many firewalls log incoming and outgoing traffic, including scanning attempts. Look for patterns of repeated requests from the same IP address or a range of ports being accessed in quick succession. In a forensic context, you can access the firewall or router logs to find signs of port scanning.
2. **Intrusion Detection Systems (IDS):** If an IDS like **Snort** is deployed in the network, it may have detected and logged the port scan. IDS systems monitor network traffic for patterns that indicate scanning activities. For example, a series of connection attempts on various ports in a short time interval is often considered a port scan.
3. **Use Netstat to Check for Open Ports:** On the target system, you can use the **netstat** command to check for active connections and open ports. Running the following on the target system can help identify any ongoing connections:

```
netstat -tuln
```

The **-tuln** flag will show active listening ports and associated services.

Step 5: Analyzing Results Using Wireshark

Wireshark is a popular network packet analyzer that helps in forensic investigations by capturing and inspecting network traffic. You can use Wireshark to inspect the packets during a port scan and identify malicious behavior.

1. **Start Wireshark:** Open Wireshark on Kali Linux by typing:

UNIT 2: CYBER FORENSICS NOTES

wireshark

2. Capture Traffic: Choose the network interface you want to capture traffic from (e.g., eth0 or wlan0) and click on it to start capturing.

3. Filter for Port Scanning Activity: You can apply filters in Wireshark to narrow down the captured traffic. For example, to look for SYN packets (used during a SYN scan), apply the filter:

```
tcp.flags.syn == 1
```

This filter will display only SYN packets, which are often sent during port scans. By analyzing the captured packets, you can identify abnormal traffic patterns that might indicate a scan.

Step 6: Analyzing Logs and Tracebacks

In addition to capturing network traffic, you can analyze system logs (e.g., /var/log/auth.log, /var/log/messages) to look for any unauthorized access or signs of scanning. If the target system is compromised, the attacker might leave traces in these logs. For example, unexpected logins, failed login attempts, or SSH login attempts could indicate an ongoing attack.

For example, if you see entries like:

```
sshd[12345]: Failed password for invalid user from 192.168.1.100
```

This may indicate that someone is trying to exploit the system through brute force or port scanning to find vulnerabilities.

Step 7: Report Findings

Once the port scan and forensic analysis are complete, document your findings. The report should include:

UNIT 2: CYBER FORENSICS NOTES

- The tools used for the port scan (e.g., Nmap).
- The IP address or range of the target system.
- A detailed list of open ports and the services running on them.
- Any suspicious or unauthorized scanning activity.
- Evidence from IDS logs, firewall logs, or Wireshark captures.

Make sure the findings are presented clearly and include screenshots, logs, and other relevant data.

UNIT 2: CYBER FORENSICS NOTES