Network Forensics

1. Introduction to Network Forensics

Network forensics is a branch of digital forensics that focuses on monitoring, capturing, and analyzing network traffic for the purpose of investigations, security monitoring, and legal evidence. Unlike disk forensics, network forensics deals with **volatile and dynamic data**, because network packets exist only briefly while in transit.

Network forensics is mainly used for:

- **Security investigations**: Detecting intrusions, attacks, and policy violations.
- **Law enforcement investigations**: Reconstructing emails, file transfers, chat sessions, and identifying suspects.

Because attackers may delete logs on compromised systems, **network-level evidence** can sometimes be the only reliable source of proof.

2. Network Components and Their Forensic Importance

Understanding network components is essential for effective forensic analysis.

2.1 Host

A **host** is any device connected to a network with an IP address, such as a computer or server. Hosts often contain valuable forensic data, including:

- User activity
- Network logs
- Application data

2.2 Node

A **node** is any device participating in network communication. Nodes can be hosts, routers, switches, or other devices. Nodes help investigators understand the **path of data transmission**.

2.3 Router

A **router** forwards packets between networks. Router logs can provide:

- Source and destination IP addresses
- Routing paths
- Evidence for tracing attackers

2.4 Switch

A **switch** connects devices within a local network. It maintains MAC address tables (CAM tables), useful in identifying:

- Which device was connected to which port
- VLAN-related activity

2.5 Hub

A **hub** broadcasts traffic to all connected devices. Though mostly obsolete, hubs allow easier traffic capture because all packets are visible.

2.6 Network Interface Card (NIC)

The **NIC** connects a device to the network and contains the MAC address. Investigators can place the NIC in **promiscuous mode** to capture all passing traffic.

3. OSI and TCP/IP Models

3.1 OSI Model

The **OSI model** consists of seven layers:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Each layer plays a role in how data is transmitted and where forensic evidence can be collected.

3.2 TCP/IP Model

The TCP/IP model has **four layers**:

1. Link
2. Network

3. Transport
4. Application

Most real-world network forensics investigations are based on the TCP/IP model.

4. Forensics Information from Networks

Major forensic data sources include:

- Hosts
- Routers
- Firewalls
- Switches
- IDS/IDPS
- Wireless Access Points (WAPs)

Intrusion Detection and Prevention Systems (IDS/IDPS)

IDS and IDPS monitor network traffic and generate logs about:

- Suspicious behavior
- Policy violations
- Known attack patterns

These logs are highly valuable for forensic analysis.

5. Log Analysis

Log analysis is a critical step in network forensics.

5.1 Time Stamp Analysis

- Accurate time is essential for timeline reconstruction.
- Network Time Protocol (NTP) ensures clock synchronization.
- Investigators must verify whether NTP was enabled.

5.2 Data Analysis

Network data is transmitted in packets that may take different paths. TCP sequence numbers and acknowledgments help reconstruct:

- Sessions
- File transfers
- Communication timelines

Protocols commonly analyzed include HTTP, FTP, SMTP, DNS, DHCP, ARP, and SSH.

6. Network Forensics Tools

6.1 Technology-Based Tools

- **Network Taps**: Hardware devices that copy traffic for monitoring.
- **Port Mirroring**: Duplicates switch traffic to a monitoring port.
- **Promiscuous Mode**: Allows NICs to capture all packets.

6.2 Software-Based Tools

Wireshark:

- Packet capture and protocol analysis
- GUI-based filtering and visualization
- Reconstructs sessions and files

Tcpdump:

- Command-line packet analyzer
- Useful for fast, low-level packet inspection
- Often used on servers and routers