DIGITAL FORENSICS

Lecture 8

Course Instructor: Dr. Marwa Zamzam
Email: marwa.zamzam@giu-uni.de
Instructor Office: A214
Teaching Assistants
Eng. Salma Abubakr

These slides are based on the updated version of those by Assoc. Prof. Dr. Amr ElMougy.

What is the Network Forensics?

- ❑ It is one of the **sub branches** of digital forensics.

- ❑ **Definition:** It focuses on **monitoring**, **capturing**, **recording**, and **analysis** of **network traffic.**

- ❑ **Purpose:** The main purpose of network forensics is to **trace intrusions and attacks.**

- ❑ **Data Characteristics:** It deals with **volatile** and **dynamic** data.

- ❑ **Attack Vector:** Even the most **sophisticated attacks** result from a **single unauthorized** system entry into the network.

- ❑ **Network Devices Involved:** Data flowing in/out of the network flows over **several devices** such as **routers, firewalls, switches, proxies, etc.**

Network Forensics Challenges

- ❑ **Source Identification:** Accurately identifying the attacker or unauthorized source, especially with techniques like IP spoofing and VPN masking.

- ❑ **Involved Equipment/Services:** Determining which network devices or services were exploited, especially in complex environments with multiple interconnected devices.

- ❑ **Security Weaknesses:** Identifying vulnerabilities in network defenses, such as inadequate firewalls or weak access controls, that allowed the intrusion.

- ❑ **Data Volume and Overload:** Networks generate massive amounts of data, making it difficult to capture, store, and analyze all traffic efficiently. High data volumes can lead to delays in processing and analyzing potential threats.

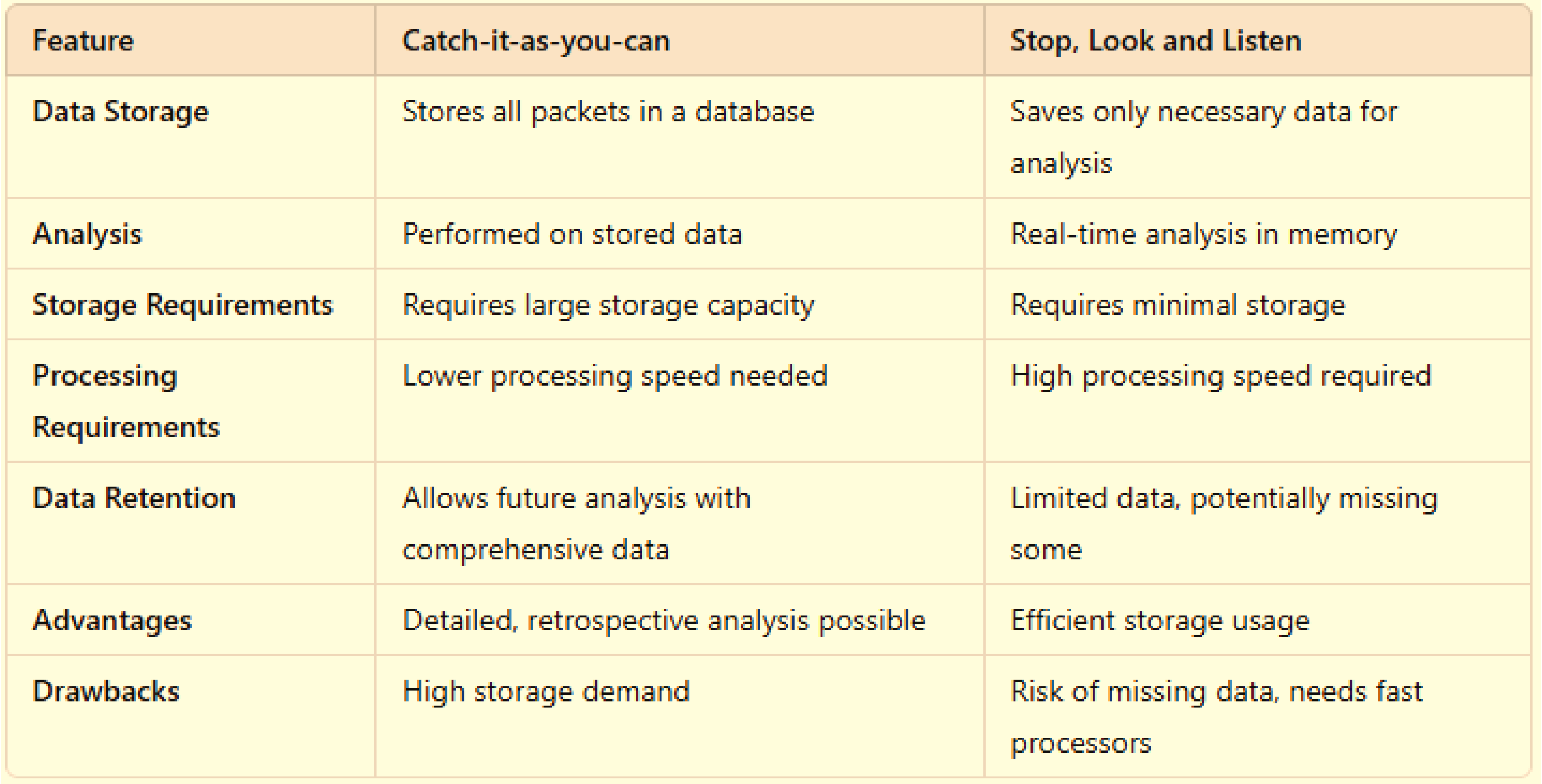
- ❑ **Encryption:** Encrypted traffic, such as HTTPS and VPNs, adds a layer of complexity to network forensics. Investigators often struggle to inspect and analyze encrypted data without decryption keys, limiting visibility into potentially malicious activities.

Network Forensics data collection methods:

- **“Catch-it-as-you-can”:** All packets are sent through a traffic point where they are stored in a database. After that, analysis is performed on stored data. Analysis data is also stored in the database. The saved data can be saved for future analysis. It should be noted, though, that this type of system requires a **large storage capacity.**

- **“Stop, look and listen” system:** It is different from the “Catch-it-as-you-can” system, since **only data required for analysis is saved into database**. The incoming traffic is filtered and analyzed in real-time in memory, which means **this system requires less storage but a much faster processor**.

Network Forensics data collection methods:



Feature	Catch-it-as-you-can	Stop, Look and Listen
Data Storage	Stores all packets in a database	Saves only necessary data for analysis
Analysis	Performed on stored data	Real-time analysis in memory
Storage Requirements	Requires large storage capacity	Requires minimal storage
Processing Requirements	Lower processing speed needed	High processing speed required
Data Retention	Allows future analysis with comprehensive data	Limited data, potentially missing some
Advantages	Detailed, retrospective analysis possible	Efficient storage usage
Drawbacks	High storage demand	Risk of missing data, needs fast processors

Sources of Network Evidence

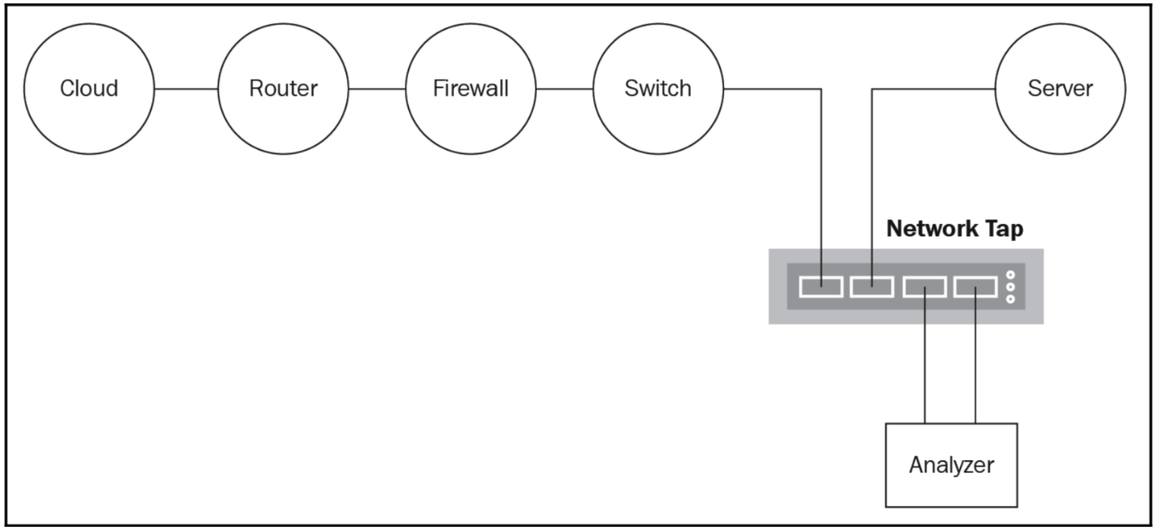
1. Tapping the wire and the air
2. CAM table on a network switch
3. Routing tables on routers
4. Dynamic Host Configuration Protocol logs
5. DNS server logs
6. Domain controller/ authentication servers/ system logs
7. IDS/IPS logs
8. Firewall logs
9. Proxy Server logs

1) Tapping the Wire and Air

- Tapping is done to capture network traffic for analysis without interrupting or alerting the network's operation. It is commonly used to gather evidence in network forensics.

- A **Network TAP (Test Access Point)** is typically positioned between two points in the network (points A and B). The network cable between these points is replaced with a pair of cables connected to the TAP.

- The TAP then forwards this traffic to an analyzer, where it can be examined for any signs of intrusion, data leakage, or other suspicious activities.

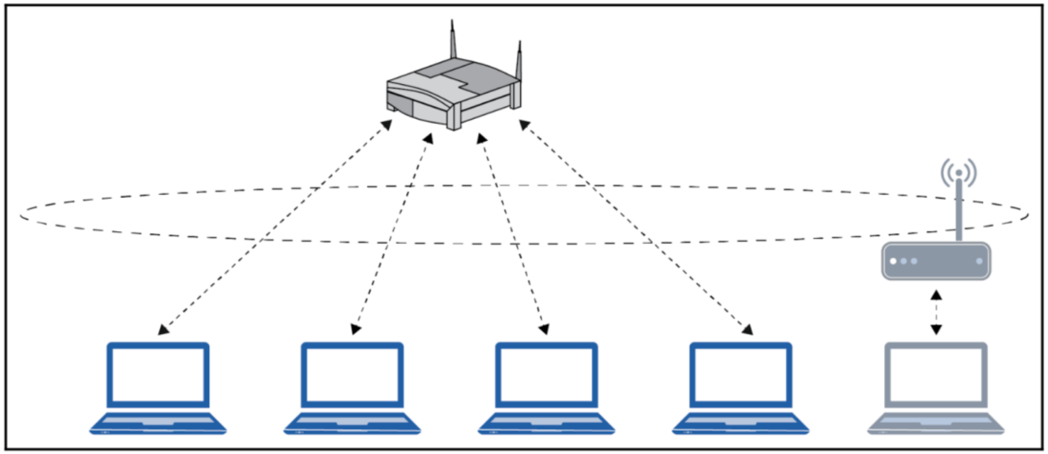


1) Tapping the Wire and Air

- ❑ In a **wireless network**, instead of a physical TAP, an additional wireless receptor (such as a wireless adapter) is connected to an analysis machine. Similar to wired network forensics, this method allows investigators to capture and examine wireless network data.

- ❑ This receptor records all traffic associated with a specific wireless access point on a particular channel.

- ❑ Wireless networks operate on specific channels within certain frequency bands (e.g., 2.4 GHz). Each access point transmits on a designated channel. By tuning the receptor to the same channel as the target access point, it can "listen" to all traffic being broadcast on that channel.



2) CAM table on a network switch

- ❑ Network switches contain dynamic **Content Addressable Memory (CAM)** tables that store the mapping between a system's MAC address and the physical ports.

- ❑ When the packet is sent from A to B the switch will search its CAM table for the port that corresponds to the MAC address of B and will only send the packet to B.

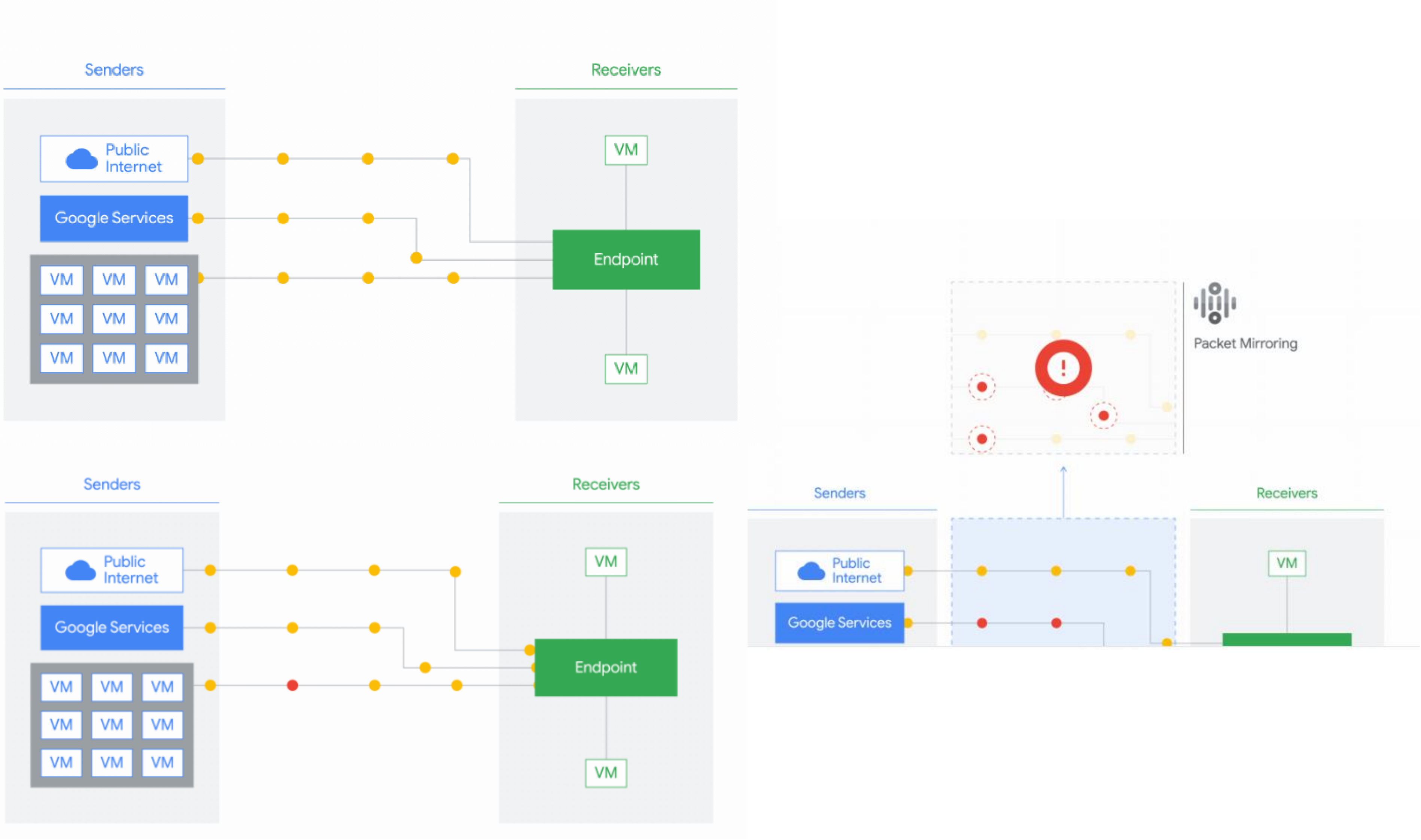
- ❑ Unlike hubs, which flood packets to all connected devices, switches use the CAM table to direct packets specifically to the intended device.

- ❑ **Port mirroring** allows the switch to duplicate traffic from one or multiple ports (or VLANs) and send a copy of this data to a designated analysis port.

- ❑ **Port mirroring** is essential in network forensics as it allows investigators to capture and analyze network traffic without disrupting normal network operations.

- ❑ Through this capability, investigators can **monitor** all communications across different VLANs and systems, making it easier to detect suspicious activities, unauthorized access, or data breaches.

2) CAM table on a network switch



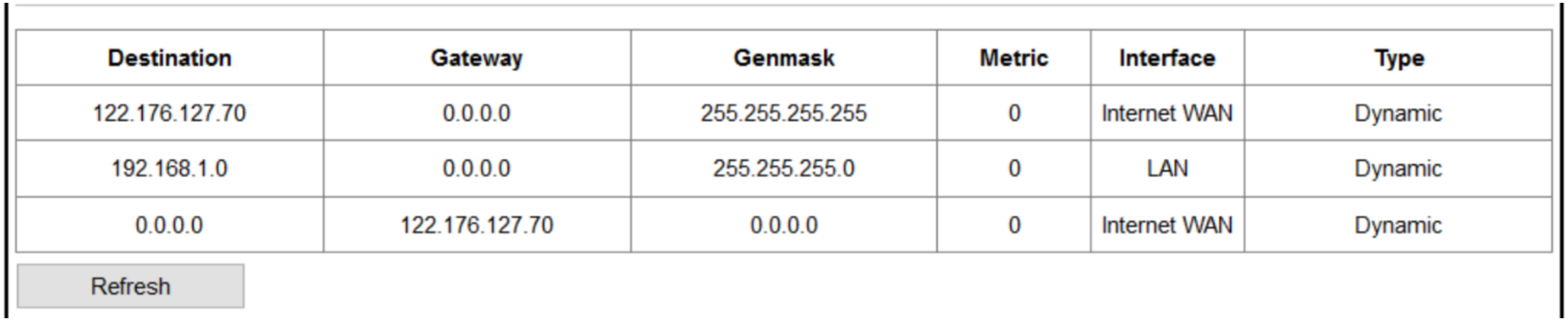
3) Routing tables on routers

- ❑ **Routers** are networking devices that connect multiple networks and forward data packets between them.

- ❑ Routers store routing tables, which contain information about network destinations and the ports or interfaces on the router that lead to those destinations.

- ❑ Routing tables are valuable in network forensics because they help investigators trace the path that network traffic takes as it moves across different routers and networks.

- ❑ By analyzing these tables, investigators can **reconstruct the route** that data packets followed. This helps identify possible intrusion points, track where data may have been leaked, and locate compromised parts of the network.

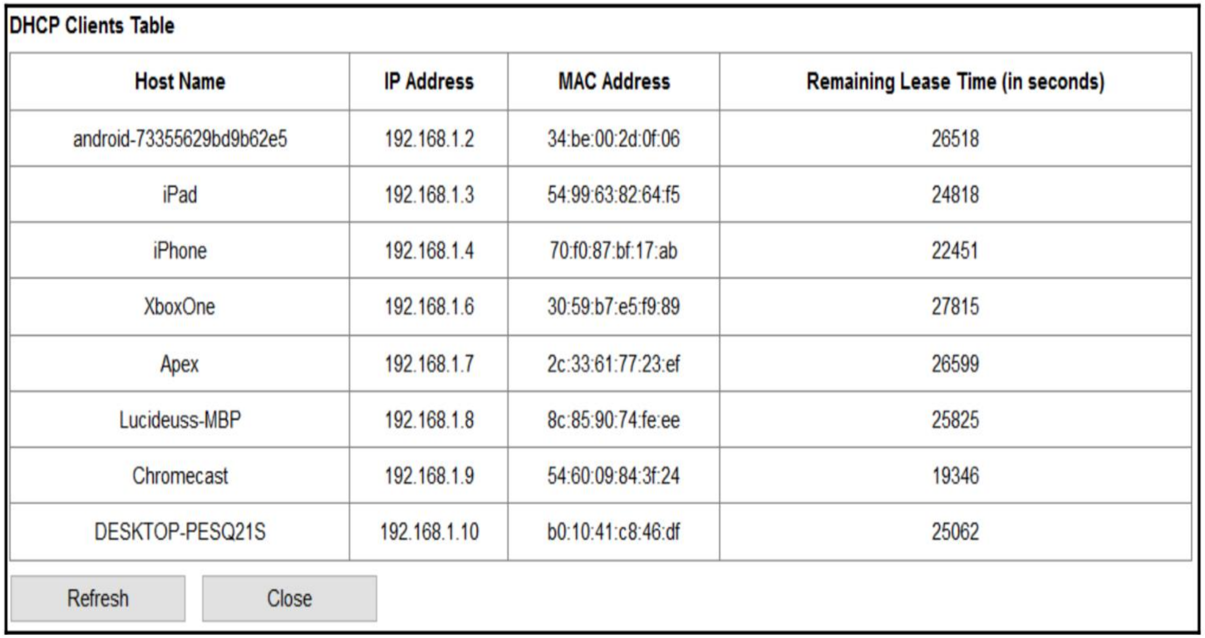


Destination	Gateway	Genmask	Metric	Interface	Type
122.176.127.70	0.0.0.0	255.255.255.255	0	Internet WAN	Dynamic
192.168.1.0	0.0.0.0	255.255.255.0	0	LAN	Dynamic
0.0.0.0	122.176.127.70	0.0.0.0	0	Internet WAN	Dynamic

4) Dynamic Host Configuration Protocol (DHCP)

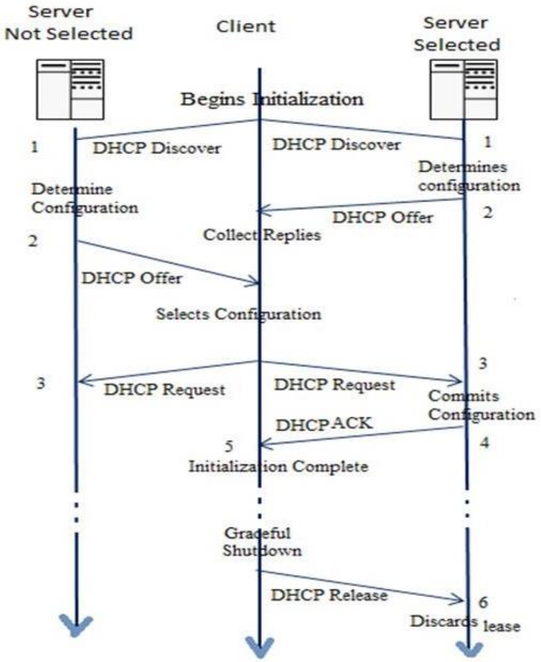
- **DHCP servers log** entries each time a device connects to the network and requests an IP address. These logs typically include information such as the device's MAC address, assigned IP address, and the timestamp of the connection

- By examining DHCP logs, investigators can track the presence and activity of specific devices on the network, helping to identify unauthorized devices, track network access patterns, and detect potential security incidents.



DHCP Clients Table

Host Name	IP Address	MAC Address	Remaining Lease Time (in seconds)
android-73355629bd9b62e5	192.168.1.2	34:be:00:2d:0f:06	26518
iPad	192.168.1.3	54:99:63:82:64:f5	24818
iPhone	192.168.1.4	70:f0:87:bf:17:ab	22451
XboxOne	192.168.1.6	30:59:b7:e5:f9:89	27815
Apex	192.168.1.7	2c:33:61:77:23:ef	26599
Lucideuss-MBP	192.168.1.8	8c:85:90:74:fe:ee	25825
Chromecast	192.168.1.9	54:60:09:84:3f:24	19346
DESKTOP-PESQ21S	192.168.1.10	b0:10:41:c8:46:df	25062

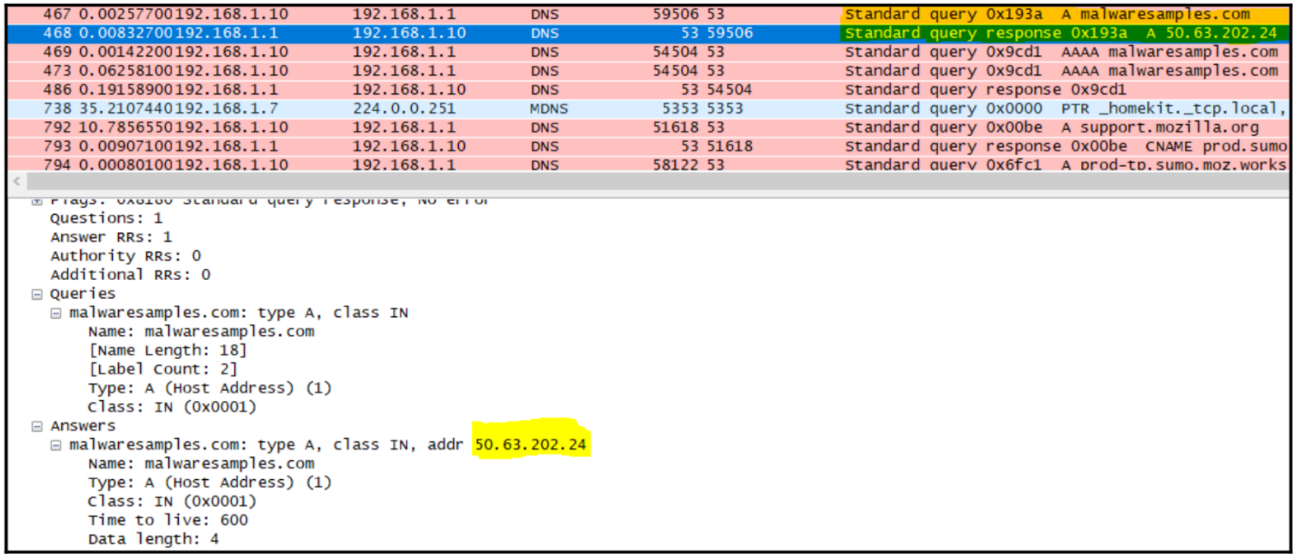


5) DNS Server Logs

- ❑ Every time a device connects to a new website or sends an email, it initiates a DNS request to translate a domain name (e.g., example.com) into an IP address. This process, known as **DNS resolution**, allows the device to identify and communicate with the intended server.

- ❑ By logging the queried domain names, network administrators **can monitor for any requests to known malicious or suspicious domains.**

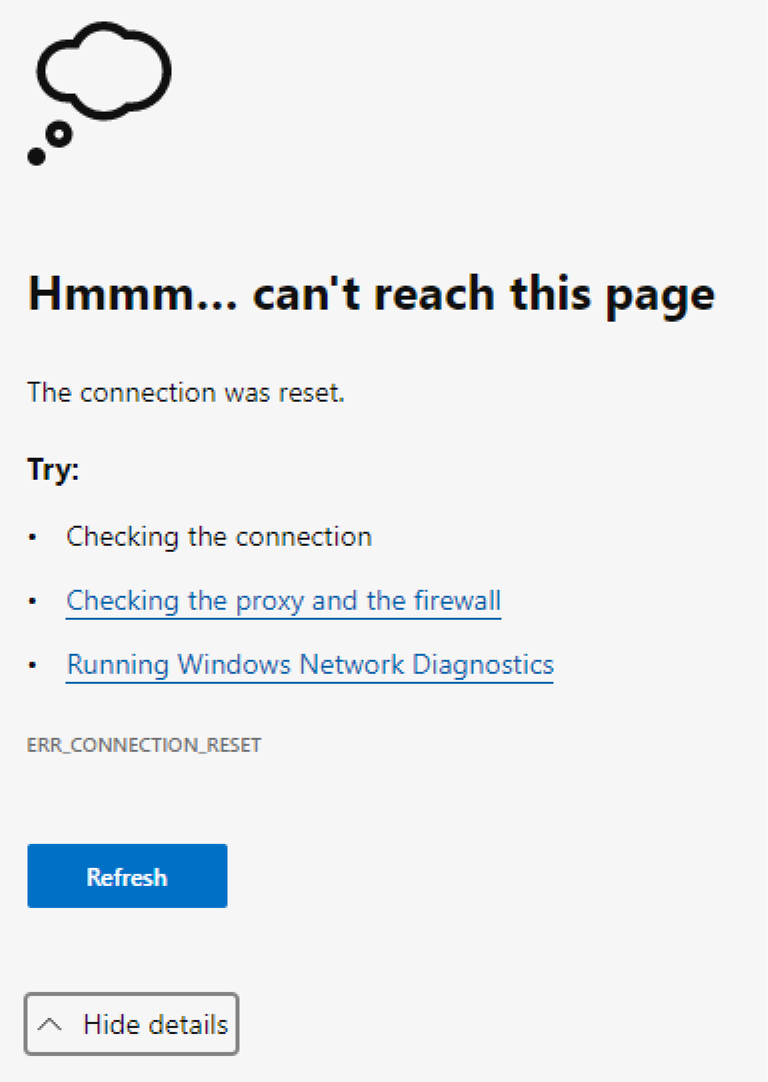
- ❑ Patterns like unusual domain names or repeated lookups of the same domain could indicate malware activity, as malware often tries to connect to attacker-controlled domains for instructions.



```
467 0.00257700192.168.1.10    192.168.1.1     DNS      59506 53       Standard query 0x193a  A malwaresamples.com
468 0.00832700192.168.1.1     192.168.1.10    DNS         53 59506    Standard query response 0x193a  A 50.63.202.24
469 0.00142200192.168.1.10    192.168.1.1     DNS      54504 53       Standard query 0x9cd1  AAAA malwaresamples.com
473 0.06258100192.168.1.10    192.168.1.1     DNS      54504 53       Standard query 0x9cd1  AAAA malwaresamples.com
486 0.19158900192.168.1.1     192.168.1.10    DNS         53 54504    Standard query response 0x9cd1
738 35.2107440192.168.1.7     224.0.0.251     MDNS      5353 5353     Standard query 0x0000  PTR _homekit._tcp.local,
792 10.7856550192.168.1.10    192.168.1.1     DNS      51618 53       Standard query 0x00be  A support.mozilla.org
793 0.00907100192.168.1.1     192.168.1.10    DNS         53 51618    Standard query response 0x00be  CNAME prod.sumo
794 0.00080100192.168.1.10    192.168.1.1     DNS      58122 53       Standard query 0x6fc1  A prod-tp.sumo.moz.works

⊞ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
⊟ Queries
  ⊟ malwaresamples.com: type A, class IN
      Name: malwaresamples.com
      [Name Length: 18]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
⊟ Answers
  ⊟ malwaresamples.com: type A, class IN, addr 50.63.202.24
      Name: malwaresamples.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 600
      Data length: 4
```

5) DNS Server Logs



Hmmm... can't reach this page

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

5) DNS Server Logs

- ❑ **DNS filtering** prevents users from reaching particular websites or domains by blocking the name resolution process (i.e., converting a domain name to an IP address). When a client tries to access a blocked domain, the DNS server intercepts the request and stops communication, preventing the connection.

- ❑ The primary security use of DNS filtering is to block known malicious domains, such as those associated with malware, phishing, or other cyber threats. This helps prevent users from accessing harmful websites.

- ❑ DNS filtering is also commonly used by organizations to enforce business policies or improve productivity. Companies may block categories of websites such as social media, video streaming, or any other distracting or inappropriate domains .

- ❑ DNS filtering can be tailored based on specific needs. Organizations can set filters for: **Individual users, groups of users or all users across the network.**

6) Authentication servers Logs

- An **authentication server** is used to **verify credentials** when a person or another server needs to prove who they are to an application.

- Authentication servers keep logs of all authentication attempts, both successful and unsuccessful. These logs provide valuable insights into potential intrusion attempts by highlighting failed logins, suspicious access patterns, or unauthorized access attempts.

- In a **single-factor authentication** site, the process looks like this:

  1. The user enters a **username and password**. The site **encrypts** that data and sends it to the **server**.
  2. The **server decrypts** the data and compares it to information listed in the **database.**
  3. If the items entered **match** a saved combination, **authentication is complete.**

- More steps are involved in a **multi-factor authentication process**:
  1. The user enters a **username and password**. The site **encrypts** the data and sends it to the **server**.
  2. The **server decrypts** the data and compares it to information saved in the **database.**
  3. If the server finds **a match**, it creates a **one-time password** that it sends back to the user. A text message sent to a cellphone on file or a note to a key in the user's possession would work. The server creates an open window, ready to **accept the one-time password**.
  4. The user receives and enters that one-time password. **Authentication is complete.**

7) IDS/IPS logs

- **Intrusion detection** is the process of monitoring your network traffic and analyzing it for signs of possible intrusions.

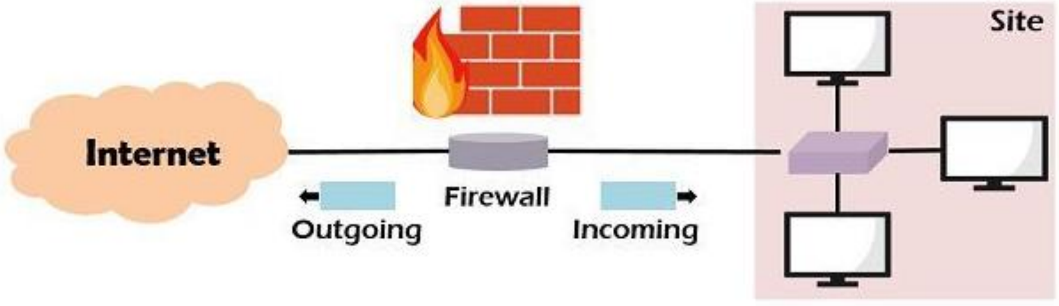
- Building on intrusion detection, **Intrusion Prevention Systems (IPS)** not only detects but also stops the detected threats. IPS perform actions like dropping packets or terminating sessions to block malicious activity in real-time.

- These logs provide:

  - *IP address* for the source and the destination.
  - *Port number* for the source and the destination.
  - The *matched signatures*.
  - *On going* attacks.
  - *Malware* presence.
  - Command and Control servers: a "boss computer" controlled by a hacker. It tells infected computers (called bots) what to do. For example, if a hacker wants to steal data or spread more viruses, they send commands from the C&C server to the infected computers. Those computers then send back the stolen data or perform the actions the hacker wants.

8) Firewalls Logs

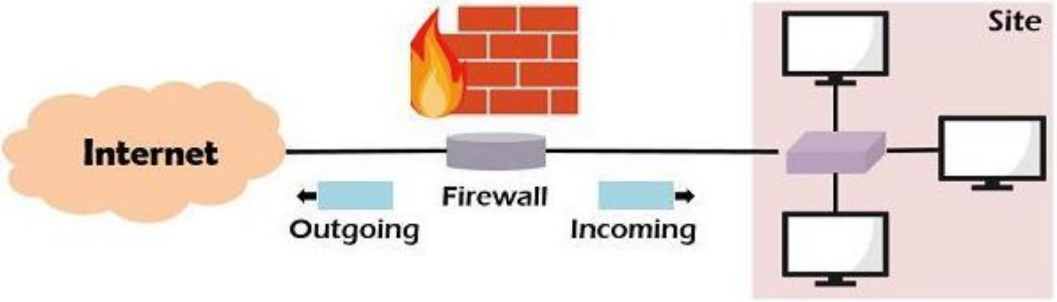
- They capture details about each connection, such as:
  - **Source and Destination IP Addresses:** where the traffic is coming from and going to.
  - **Ports:** which application or service the traffic is trying to reach (e.g., web traffic uses port 80 for HTTP or port 443 for HTTPS).
  - **Date and Time:** the exact time of each connection attempt.
  - **Action Taken:** whether the firewall allowed or blocked the connection.
  - **Protocol:** the communication protocol used (e.g., TCP, UDP).



Firewall

8) Firewalls Logs

- Firewall logs are valuable in network forensics because they help:
  - **Identify Unauthorized Access:** Logs show if any unusual or unauthorized IPs are trying to access the network, helping to detect potential attacks.
  - **Track Intrusion Attempts:** Repeated failed attempts to access certain ports or IP addresses can signal a brute-force attack or scanning activity.
  - **Monitor Suspicious Activity:** By analyzing logs, security analysts can spot patterns of unusual activity, like unexpected data transfers.
  - **Incident Investigation and Response:** After a security incident, firewall logs provide essential data to understand how an attacker gained access, what they targeted, and whether any data was transferred out of the network.

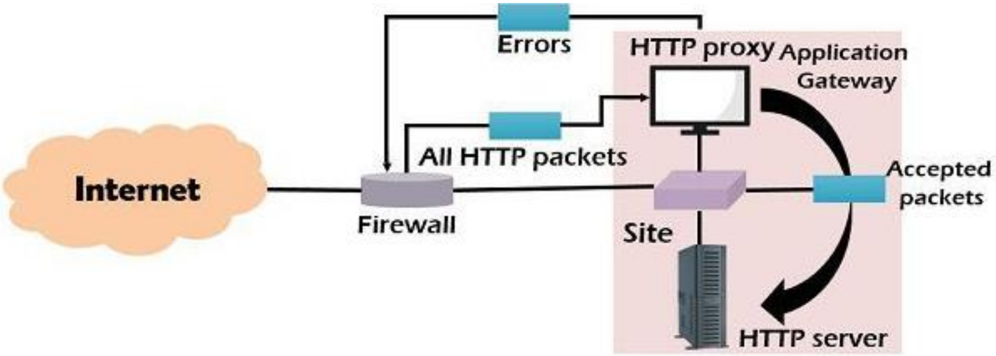


Firewall

9) Proxy server Logs

- A proxy server acts as an intermediary between users and the internet, and it logs information about each request that passes through it. Proxy logs include:

  - **Client IP Address:** the IP address of the user or device making the request.
  - **URL Requested:** the specific website or resource the user tried to access.
  - **Date and Time:** when the request was made.
  - **HTTP Method:** how the request was made, such as GET or POST.
  - **Status Code:** the server's response to the request (e.g., 200 for success, 404 for not found).
  - **Bytes Transferred:** the amount of data sent to or received from the requested site.

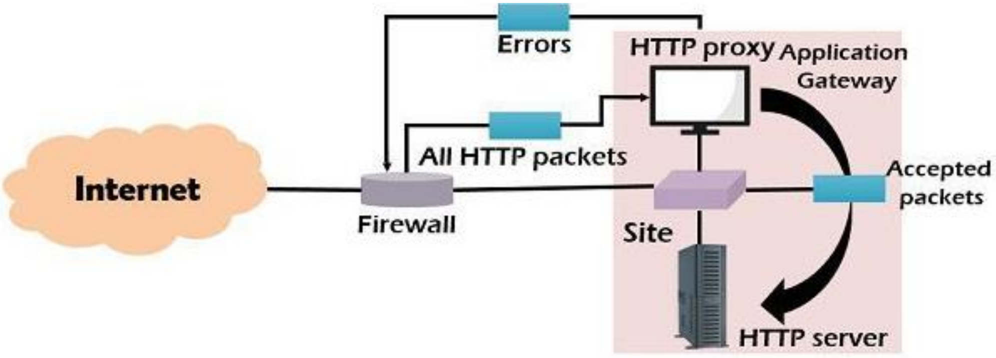


Proxy Server

9) Proxy server Logs

❑ In network forensics, proxy server logs are valuable for:

- **Tracking User Activity:** Proxy logs help track which websites users visit, making it easier to detect suspicious behavior, such as visiting potentially harmful sites.
- **Analyzing Malware Activity:** If a device in the network is compromised, proxy logs may show unusual patterns of web requests to known malicious domains.
- **Monitor Data Theft:** By analyzing outgoing requests, forensics teams can detect if sensitive data is being sent to external, unauthorized servers.



Proxy Server

Network Forensic Process Model

- ❑ Preparation phase
- ❑ Detection phase
- ❑ Incident response phase
- ❑ Collection phase
- ❑ Preservation phase
- ❑ Examination phase
- ❑ Analysis phase
- ❑ Investigation phase
- ❑ Presentation Phase

Preparation and Detection phase

- ❑ Preparation phase
  - Since many tools need to be deployed (IDPSs, firewalls, packet analyzers) on various points on the network, the prime duty is to obtain required **authorization and legal** warrants to ensure privacy.

- ❑ Detection phase
  - Deployed tools generate an **alert or a warning** which indicates a **security breach or policy violation.**

  - A quick **validation** is done to assess and **confirm the suspected attack**.

Incident response and collection phase

- Incident response
  - The response initiated in this phase depends on the **type of attack** identified and also by organizational and legal policy.
  - This phase is **applicable only when investigation is initiated during the attack**.

- Collection phase
  - The **most difficult part** because **data that flows over a network changes rapidly** and it is not possible to generate the same trace at later stages.
  - It is crucial to have **reliable hardware and software**, along with well-defined procedures to **collect maximum evidence** with minimum impact on the network.

Preservation and Examination phase

- ❑ Preservation Phase

  - Original data is kept safe along with computed hashes. **Another copy of data will be used for analysis**. This is done to ensure that there is no unauthorized use or tampering.

- ❑ Examination Phase

  - This phase examines previous phase. This is done in a methodical way so no key information is lost. All hidden or altered data done by attacker needs to be uncovered.

  - **Reduction of high volume data is necessary** in order to identify the least information holding the highest probable evidence.

Analysis and Investigation phase

❑ Analysis Phase

- The collected evidence is analyzed in order to **find a specific indicator of an intrusion**. Also, **statistical analysis and data mining** is performed to search for data and to match it to attacking model.

- The **attacking patterns** are put together and reconstructed to understand the purpose and methodology of the attack.

❑ Investigation Phase

- This phase **uses information gathered through analysis phase**, and concentrates on **identifying attacker**, which is the most difficult part of analysis phase.

- Attacker may use many different techniques to **hide their intentions or their identity**, such as IP spoofing or stepping stone attack. Actual approach in investigation phase depends on **attack type**.

Presentation phase

- It is the final stage in processing model. Systematic **documentation**, along with **observation with explanations** are presented in **readable and understandable format**.

- Everything that has been **performed** needs to **be presented** in accordance to applicable legislation and security policy, along with **recommendations on how to prevent future attacks.**

This framework for network forensics shows how methodical and precise approach an investigator needs to take in order to have v**aluable, legally acceptable and forensically sound evidence to present.**

Network-based evidence Challenges

- Network-based evidence poses special challenges in several areas:

  - **Acquisition:** It can be difficult to **locate specific evidence in a network** environment. But, even when you know where a specific piece of evidence is located, you may have **difficulty gaining access** to it for various reasons.

  - **Content:** Unlike **file systems**, which are designed to contain **all the files and their metadata**, **network devices may not store evidence with that level of diversity.**

  - **Storage:** Network devices normally do not employ **secondary or persistent storage**, and often have **very limited storage capacity.**

Network-based evidence Challenges

- Network-based evidence poses special challenges in several areas:

  - **Privacy:** Depending on jurisdiction, **there may be legal issues** involving personal privacy that are unique to network-based acquisition techniques.

  - **Seizure: Seizing a hard drive** can inconvenience an **individual or organization**. Seizing a network device can be much more disruptive. In the most extreme cases, **an entire network segment may be brought down indefinitely.**

  - **Admissibility:** File system-based evidence is now regularly admitted in both **criminal and civil proceedings**. In contrast, network forensics is a **newer approach to digital investigations**. There **are sometimes conflicting or non-existing legal procedures for admission on various types of network based digital evidence.**

Network Forensic Analysis Tools (NFATs)

- ❑ Some of the **commercial NFATs** available in the market are: NetIntercept, NetDetector, NetFlow, SilentRunner, EnCase, and VisualRoute.

- ❑ The **open source NFATs** are: TCPDump, Libpcap, WinDump, Wireshark, Snort, Nmap, P0f, Tcpstat, Tcptrace, and Tcpflow.

- ❑ Some of the NFATs functions are:
  - Network traffic recording and analysis
  - Network performance
  - Intellectual property protection
  - Detection of employee misuse/abuse of
  - Risk assessment
  - Network forensics and security investigation
  - Exploit attempt detection
  - Data aggregation from multiple sources
  - Incident recovery
  - Prediction of future attacks
  - Anomaly detection

Thank You ☺