



SIMULATE & ANALYZE DDOS ATTACK

Submitted by:

Ramesh 24109114

Sonia: 24109119

Course: Digital Forensics

Instructor: Muhammad Waqar

UDP FLOOD ATTACK

Objective:

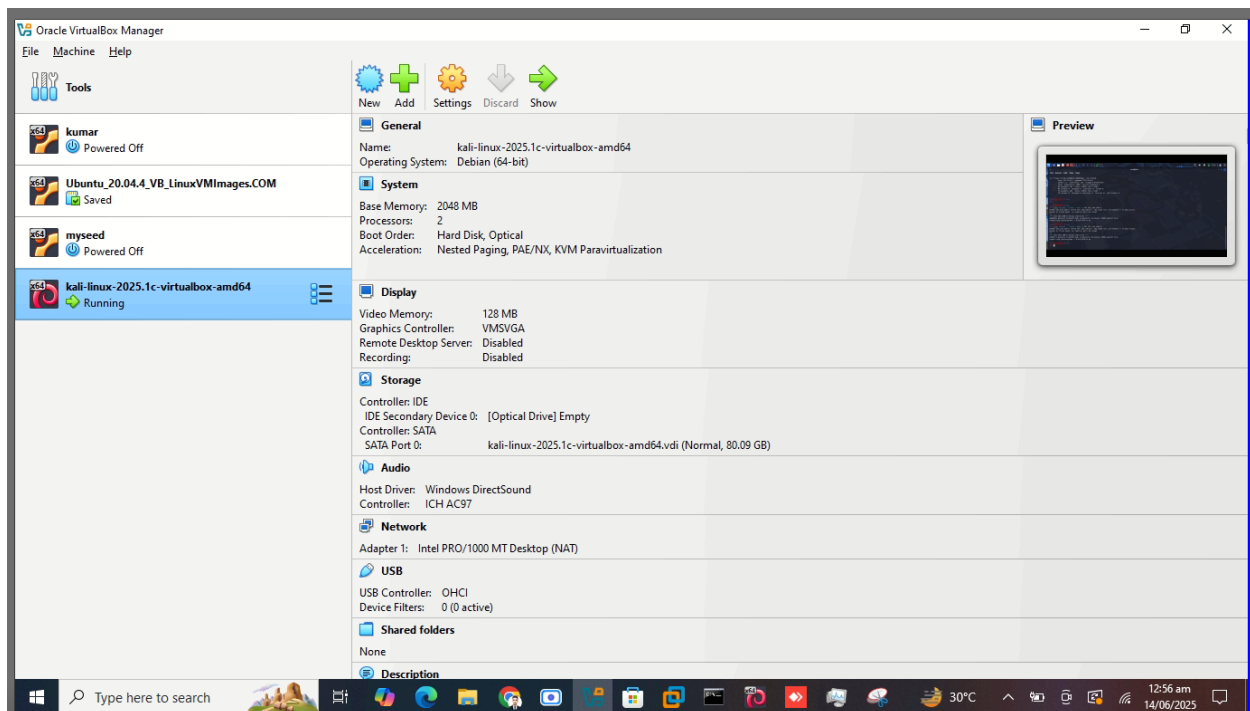
A UDP flood attack is a type of Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack where the attacker **floods** a target system with a large number of UDP (User Datagram Protocol) packets. The goal is to consume the target's resources such as bandwidth or processing power causing the system to slow down, crash, or become unavailable.

I have performed UDP flood attack Target Machine is my Windows: IP: 192.168.100.6

Victim Machine is Kali Linux: IP: 10.0.2.15.

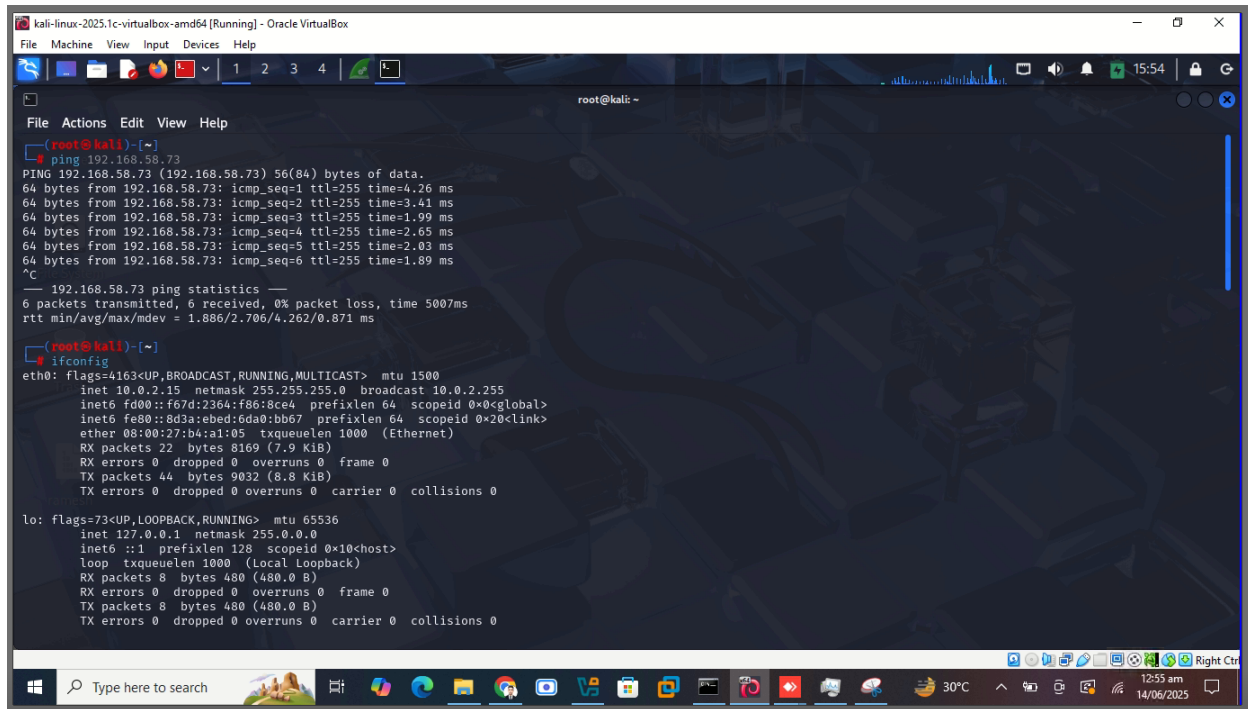
Step 1: Open Kali linux VM in virtual box.

This step initiates the attacker machine using Kali Linux in a virtualized environment. Kali provides essential penetration testing tools like hping3.



Step 2: Open terminal and run the "ifconfig" command to check ip of Kali Linux.

The ifconfig command displays the IP address of the Kali VM (10.0.2.15). This helps in confirming the network configuration of the attacker.

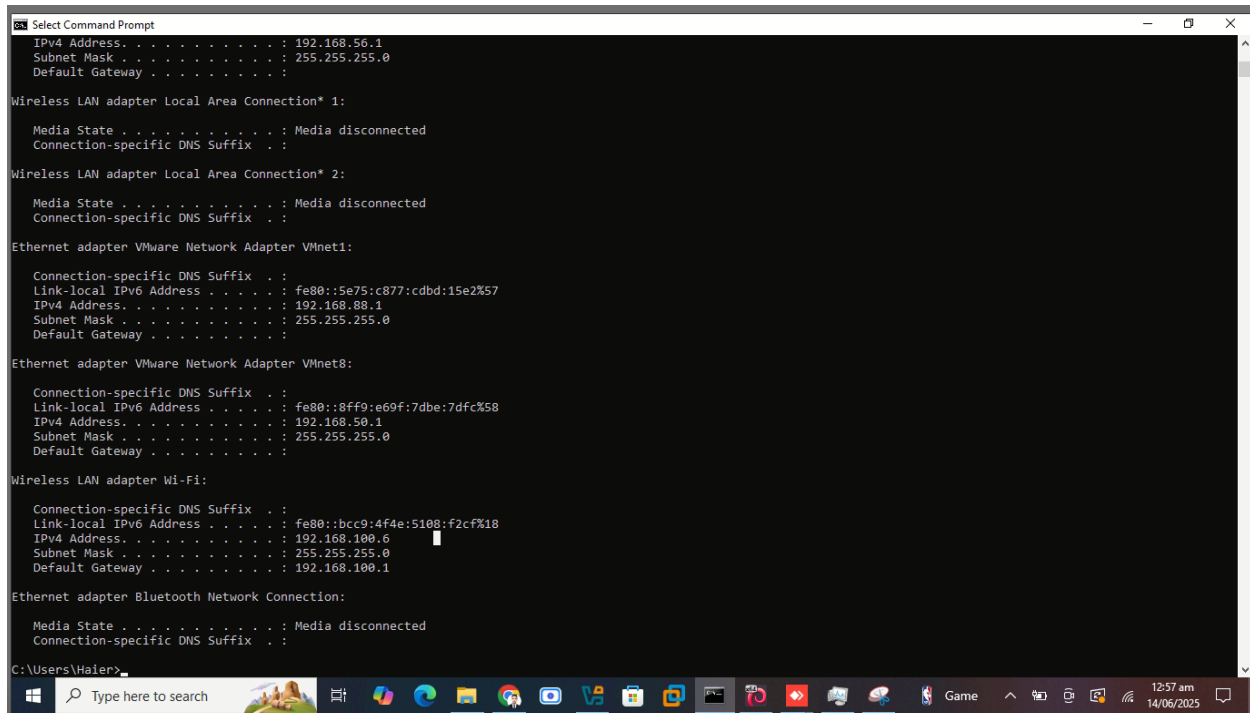


The screenshot shows a Kali Linux terminal window titled "kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running a root shell. The user has executed a ping command to 192.168.58.73, which shows successful results with 0% packet loss. Following this, the user has run the ifconfig command, displaying detailed network configuration for the eth0 and lo interfaces. The eth0 interface is configured with IP 10.0.2.15, netmask 255.255.255.0, and broadcast 10.0.2.255. The lo interface is configured with IP 127.0.0.1 and netmask 255.0.0.0. The terminal window includes a menu bar (File, Machine, View, Input, Devices, Help) and a toolbar with various icons. The bottom of the window shows a Windows taskbar with the search bar and several application icons.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
ping 192.168.58.73  
PING 192.168.58.73 (192.168.58.73) 56(84) bytes of data.  
64 bytes from 192.168.58.73: icmp_seq=1 ttl=255 time=4.26 ms  
64 bytes from 192.168.58.73: icmp_seq=2 ttl=255 time=3.41 ms  
64 bytes from 192.168.58.73: icmp_seq=3 ttl=255 time=1.99 ms  
64 bytes from 192.168.58.73: icmp_seq=4 ttl=255 time=2.65 ms  
64 bytes from 192.168.58.73: icmp_seq=5 ttl=255 time=2.03 ms  
64 bytes from 192.168.58.73: icmp_seq=6 ttl=255 time=1.89 ms  
^C  
--- 192.168.58.73 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5007ms  
rtt min/avg/max/mdev = 1.886/2.706/4.262/0.871 ms  
(root@kali)~  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fd00::f67d:236a:f86:8ce4 prefixlen 64 scopeid 0<global>  
    inet6 fe80::8d3a:ebcd:6da0:bb67 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:b4:a1:05 txqueuelen 1000 (Ethernet)  
    RX packets 22 bytes 8169 (7.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 44 bytes 9032 (8.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step 3: Open CMD and run the "ipconfig" command to check ip of Windows.

Running "ipconfig" on the Windows machine shows its IP address (192.168.100.6), which is needed as the target for the UDP flood attack.



```
Select Command Prompt
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::5e75:c877:cdbd:15e2%57
    IPv4 Address. . . . . : 192.168.88.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::8ff9:e69f:7dbe:7dfc%58
    IPv4 Address. . . . . : 192.168.50.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::bcc9:4f4e:5108:f2cf%18
    IPv4 Address. . . . . : 192.168.100.6
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

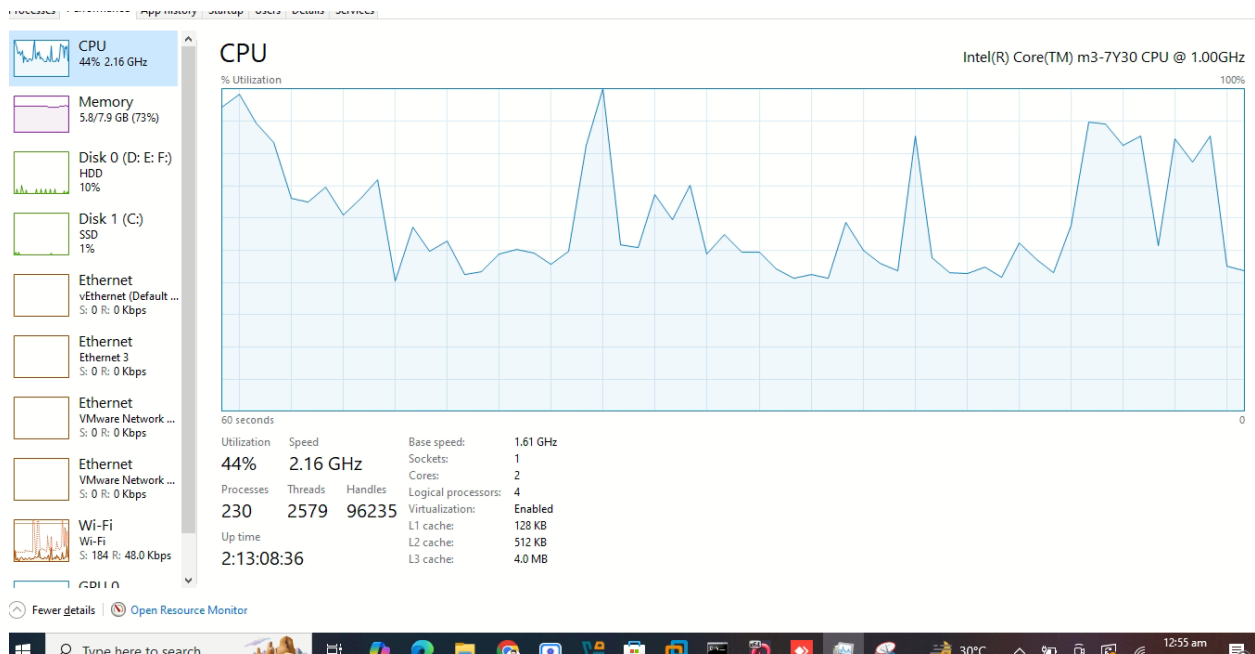
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Haier>
```

Step 4: Windows-based System performance before the attack.

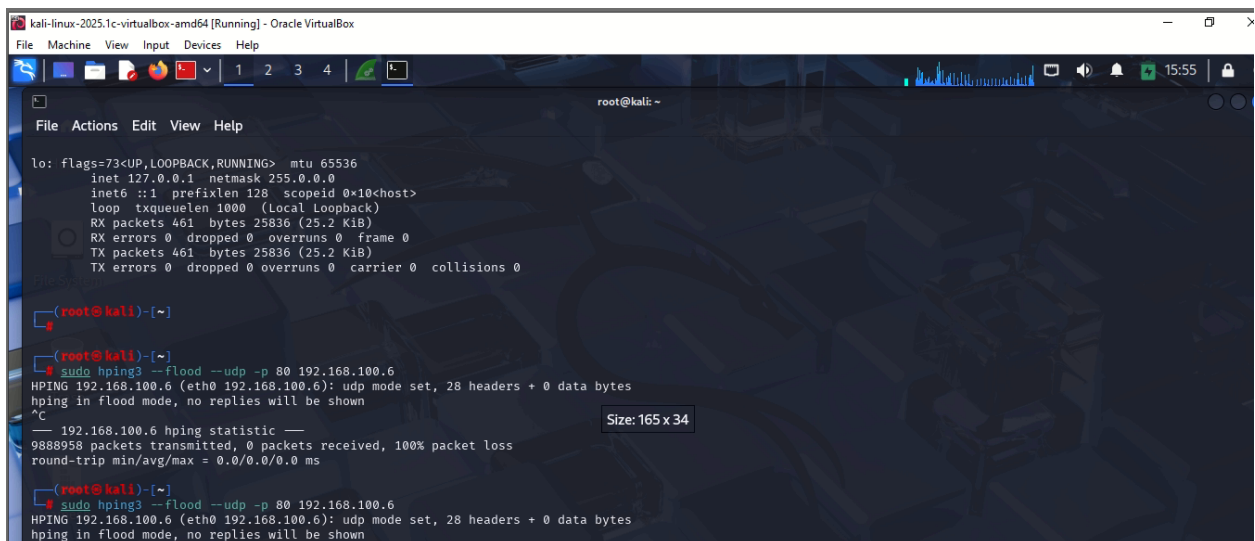
This step records baseline performance (CPU, RAM, network usage) on the Windows machine. It's used for comparing the system's behavior before and after the attack.



Step 5: `sudo hping3 --flood --udp -p 80 192.168.100.6`

This command launches a high-speed UDP flood to port 80 of the Windows machine, aiming to consume its resources and network stack.

- **Hping3** is a powerful command-line network tool used primarily for packet crafting and network testing. It is often used in penetration testing to simulate various types of traffic, including DoS/DDoS simulation, firewall testing, network scanning.
- **sudo means:**
 - Run this command as an administrator (superuser).
- **flood** Sends packets as fast as possible (flooding)
 - **UDP** sends UDP packets (instead of TCP)
 - **-p 80** Target port (80 = HTTP, you can change this)



```
kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@kali: ~
File Actions Edit View Help

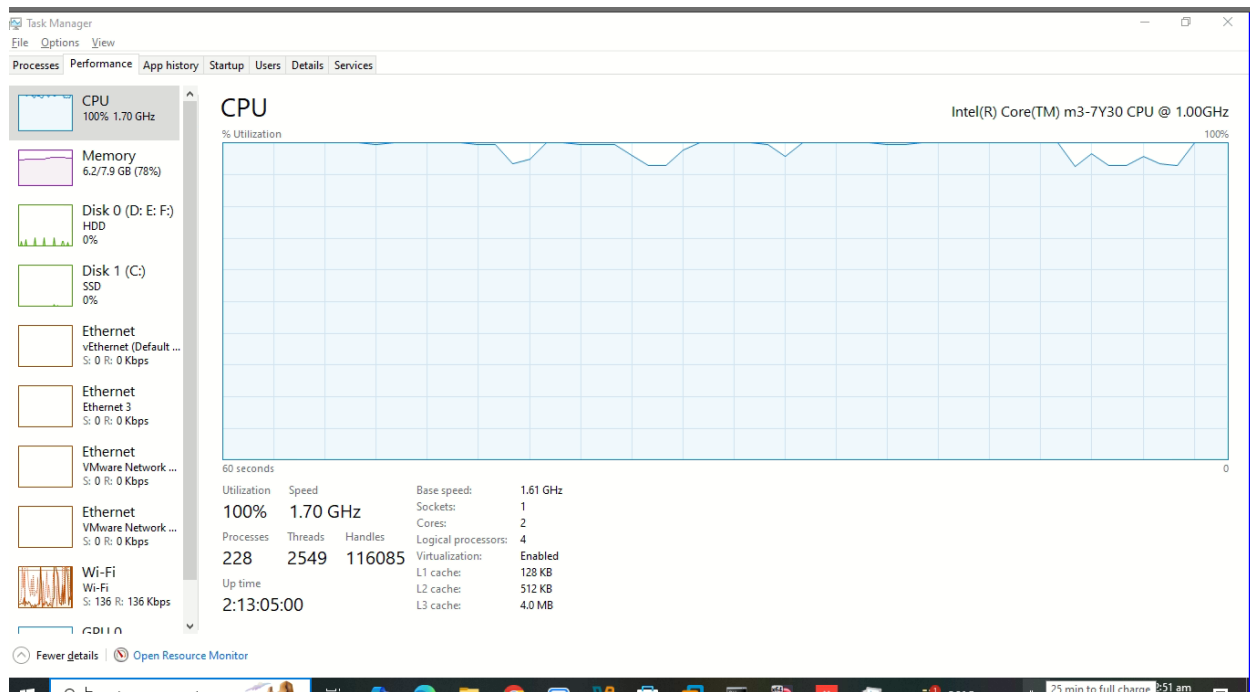
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 461 bytes 25836 (25.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 461 bytes 25836 (25.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
└─$ sudo hping3 --flood --udp -p 80 192.168.100.6
HPING 192.168.100.6 (eth0 192.168.100.6): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.100.6 hping statistic —
9888958 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(root@kali)-[~]
└─$ sudo hping3 --flood --udp -p 80 192.168.100.6
HPING 192.168.100.6 (eth0 192.168.100.6): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Step 6: Windows-based System performance after attack:

Observe the impact of the DDoS attack likely a spike in CPU usage, high network activity, and potential unresponsiveness, indicating successful disruption.



Forensic Elements in this Project

1. Traffic Capture and Analysis (Using Wireshark)

- Capturing network traffic during the attack is core forensic work.
- You analyze packet volume, frequency, and source/destination IPs to identify suspicious patterns.
- Example: Detecting a sudden burst of UDP packets to a single port from one or multiple IPs.

2. Source IP Verification and Spoofing Detection

- Forensics involves examining if source IPs are real or spoofed.
- Tools like Wireshark help you identify anomalies, such as non-existent IPs or private IPs not belonging to your network.

3. System Logs and Performance Metrics

- You compare system resource usage before and after the attack.
- Forensics here includes collecting and preserving CPU, memory, and network usage data as digital evidence of impact.

Forensics in this project is about acting like a network investigator:

Capturing data, identifying what happened, who did it (or where it came from), how it happened, and what it affected.