

**India Henry
CYSE 301 - 32781
Shideh Yavary Mehr
10 February 2025**

**CYSE: Cybersecurity Technique and Operations
Assignment: Lab 2 - Traffic Sniffing**

Assignment 2.1

1. Open Wireshark on External Kali and listen on interface “eth0”

The screenshot shows the Wireshark interface on an external Kali workstation. The title bar reads "Attacker Kali - External Workstation on CY301-IHENR002". The main window displays a list of captured packets with the following data:

| Time | Source | Destination | Length | Info |
|--------------|--------------------|-----------------|--------|--------------------------------|
| 0.000000000 | 169.254.44.123 | 169.254.5.77 | 128 | KeepAlive Request |
| 0.003587400 | 169.254.5.77 | 169.254.44.123 | 128 | KeepAlive Response |
| 0.003625600 | 169.254.44.123 | 169.254.5.77 | 56 | 47926 → 445 [ACK] Seq=73 Ack=7 |
| 5.119896800 | Microsoft_40:57:28 | | 44 | Who has 169.254.5.77? Tell 169 |
| 5.120593800 | Microsoft_40:57:16 | | 44 | 169.254.5.77 is at 00:15:5d:40 |
| 7.694068400 | 0.0.0.0 | 255.255.255.255 | 344 | DHCP Discover - Transaction ID |
| 10.817953300 | 0.0.0.0 | 255.255.255.255 | 344 | DHCP Discover - Transaction ID |
| 13.945742300 | 0.0.0.0 | 255.255.255.255 | 344 | DHCP Discover - Transaction ID |
| 21.194232800 | 0.0.0.0 | 255.255.255.255 | 344 | DHCP Discover - Transaction ID |

The packet details pane for the first packet (Frame 1) shows:

- Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface any
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 169.254.44.123, Dst: 169.254.5.77
- Transmission Control Protocol, Src Port: 47926, Dst Port: 445, Seq: 73, Len: 128
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)

The status bar at the bottom indicates "any: <live capture in progress>" and "Packets: 9 · Displayed: 9 (100.0%) Profile: Default".

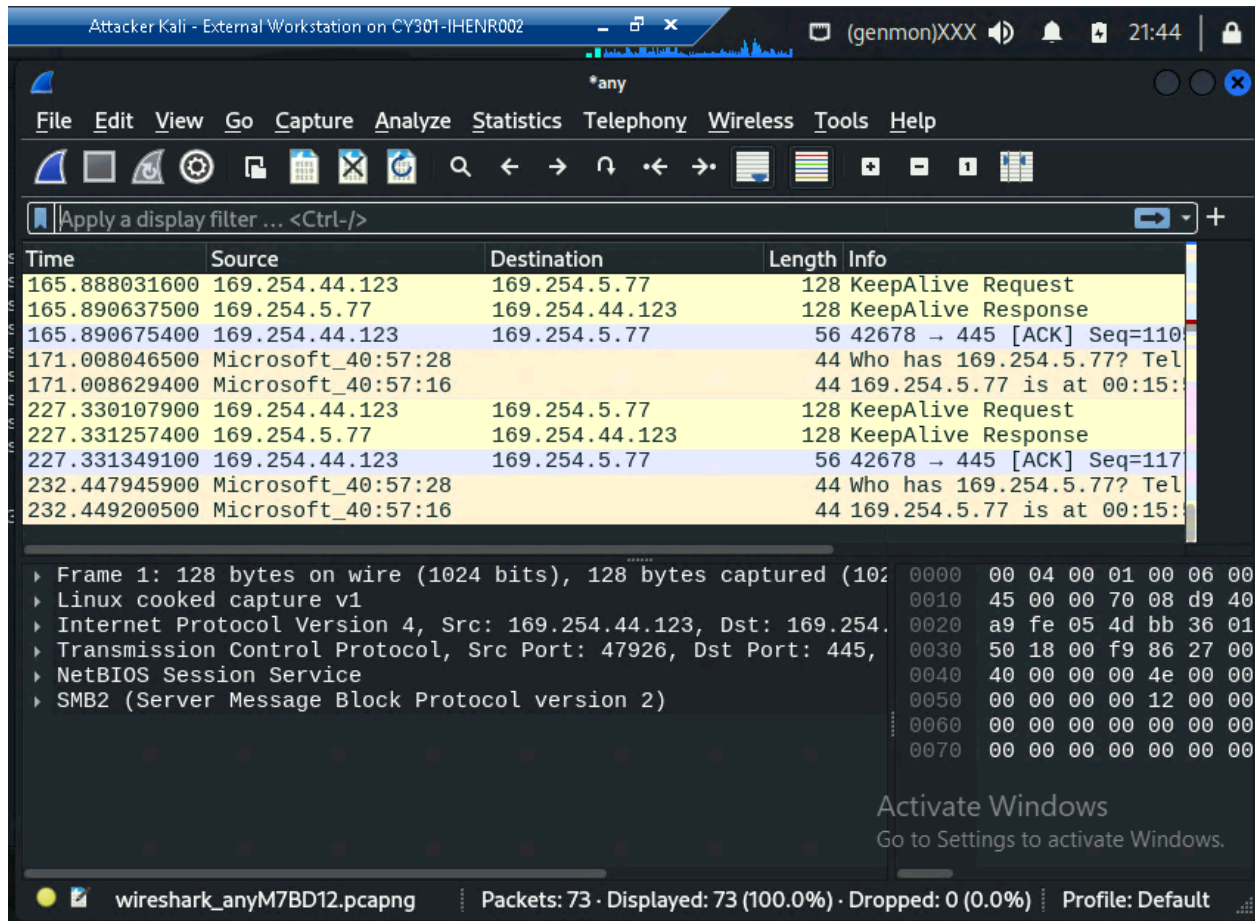
I used any instead of eth0 because eth0 wasn't giving me any packets. I just typed wireshark into external kali.

2. Open a new terminal then ping Ubuntu VM for 5-10 seconds

```
on CY301-IHENR002 (genmon)XXX 21:42
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# ping 192.168.10.18
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data:
64 bytes from 192.168.10.18: icmp_seq=1 ttl=63 time=4.72 ms
64 bytes from 192.168.10.18: icmp_seq=2 ttl=63 time=8.21 ms
64 bytes from 192.168.10.18: icmp_seq=3 ttl=63 time=7.11 ms
64 bytes from 192.168.10.18: icmp_seq=4 ttl=63 time=2.93 ms
64 bytes from 192.168.10.18: icmp_seq=5 ttl=63 time=4.20 ms
64 bytes from 192.168.10.18: icmp_seq=6 ttl=63 time=3.17 ms
64 bytes from 192.168.10.18: icmp_seq=7 ttl=63 time=3.80 ms
64 bytes from 192.168.10.18: icmp_seq=8 ttl=63 time=4.19 ms
64 bytes from 192.168.10.18: icmp_seq=9 ttl=63 time=8.59 ms
^C
— 192.168.10.18 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8035ms
rtt min/avg/max/mdev = 2.928/5.211/8.585/2.044 ms
```

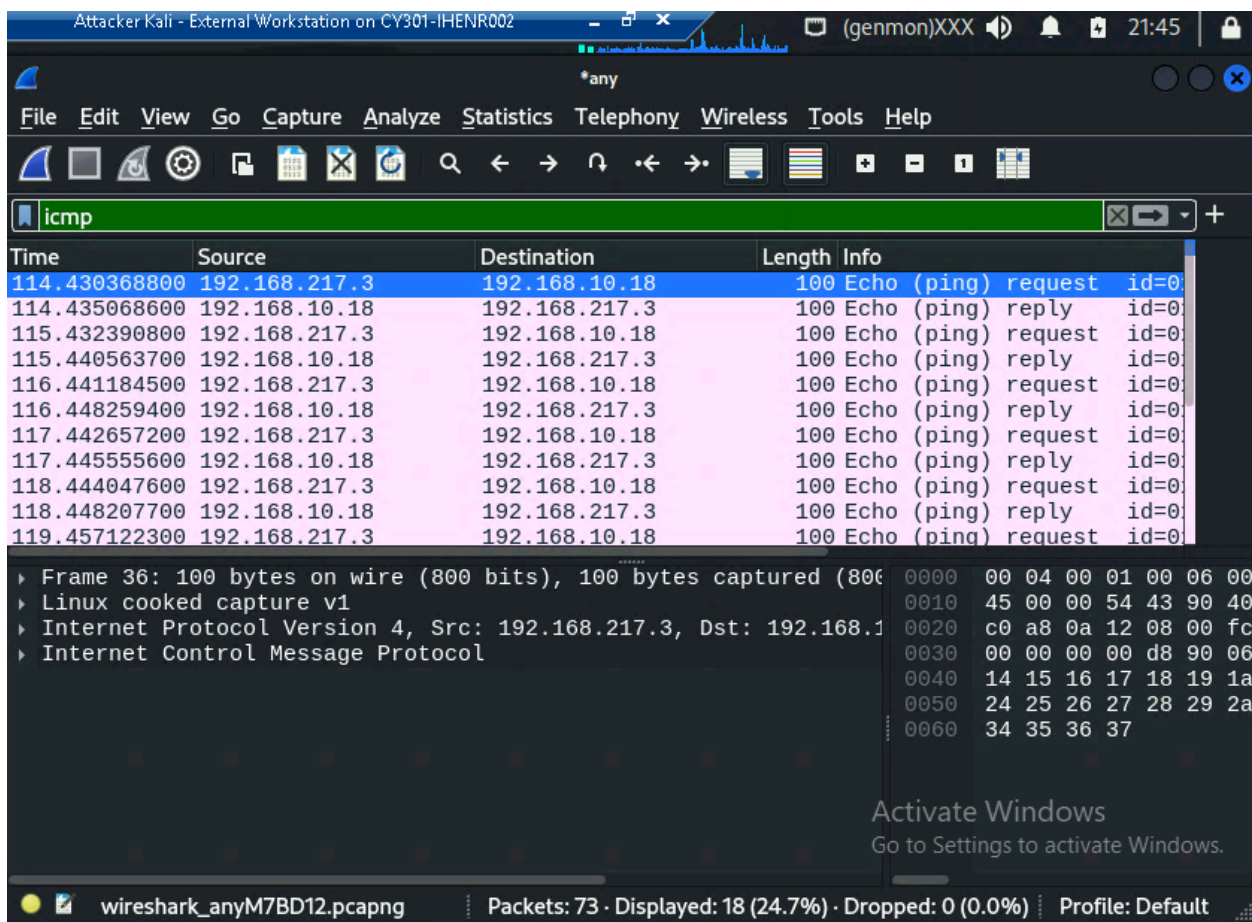
Here I opened another terminal and pinged the Ubuntu VM IP and ran it for about 7 seconds.

3. **Stop capturing (the red button on the tool bar)**



I pressed the square button at the top next to the shark fin icon to stop capturing.

1. **How many packets are captured in total? How many packets are displayed?**
73 packets were captured total; 73 were displayed
2. **Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question**



I typed lowercase "icmp" in the filter

73 packets total; 18 displayed

3. **Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence numbers and the size of the data? What is the response time?**

The screenshot shows a Wireshark capture of ICMP traffic. The packet list pane displays 18 packets, with the second packet (Time: 114.435068600) selected. The packet details pane shows the structure of this selected packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP) fields.

| Time | Source | Destination | Length | Info |
|---------------|---------------|---------------|--------|--------------------------|
| 114.430368800 | 192.168.217.3 | 192.168.10.18 | 100 | Echo (ping) request id=0 |
| 114.435068600 | 192.168.10.18 | 192.168.217.3 | 100 | Echo (ping) reply id=0 |
| 115.432390800 | 192.168.217.3 | 192.168.10.18 | 100 | Echo (ping) request id=0 |
| 115.440563700 | 192.168.10.18 | 192.168.217.3 | 100 | Echo (ping) reply id=0 |
| 116.441184500 | 192.168.217.3 | 192.168.10.18 | 100 | Echo (ping) request id=0 |
| 116.448259400 | 192.168.10.18 | 192.168.217.3 | 100 | Echo (ping) reply id=0 |
| 117.442657200 | 192.168.217.3 | 192.168.10.18 | 100 | Echo (ping) request id=0 |
| 117.445555600 | 192.168.10.18 | 192.168.217.3 | 100 | Echo (ping) reply id=0 |
| 118.444047600 | 192.168.217.3 | 192.168.10.18 | 100 | Echo (ping) request id=0 |
| 118.448207700 | 192.168.10.18 | 192.168.217.3 | 100 | Echo (ping) reply id=0 |
| 119.457122300 | 192.168.217.3 | 192.168.10.18 | 100 | Echo (ping) request id=0 |

Frame 37: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface eth0
 Linux cooked capture v1
 Packet type: Unicast to us (0)
 Link-layer address type: Ethernet (1)
 Link-layer address length: 6
 Source: Microsoft_40:15:5d:40:57:38 (00:15:5d:40:57:38)
 Unused: 0000
 Protocol: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 192.168.10.18, Dst: 192.168.217.3
 Internet Control Message Protocol

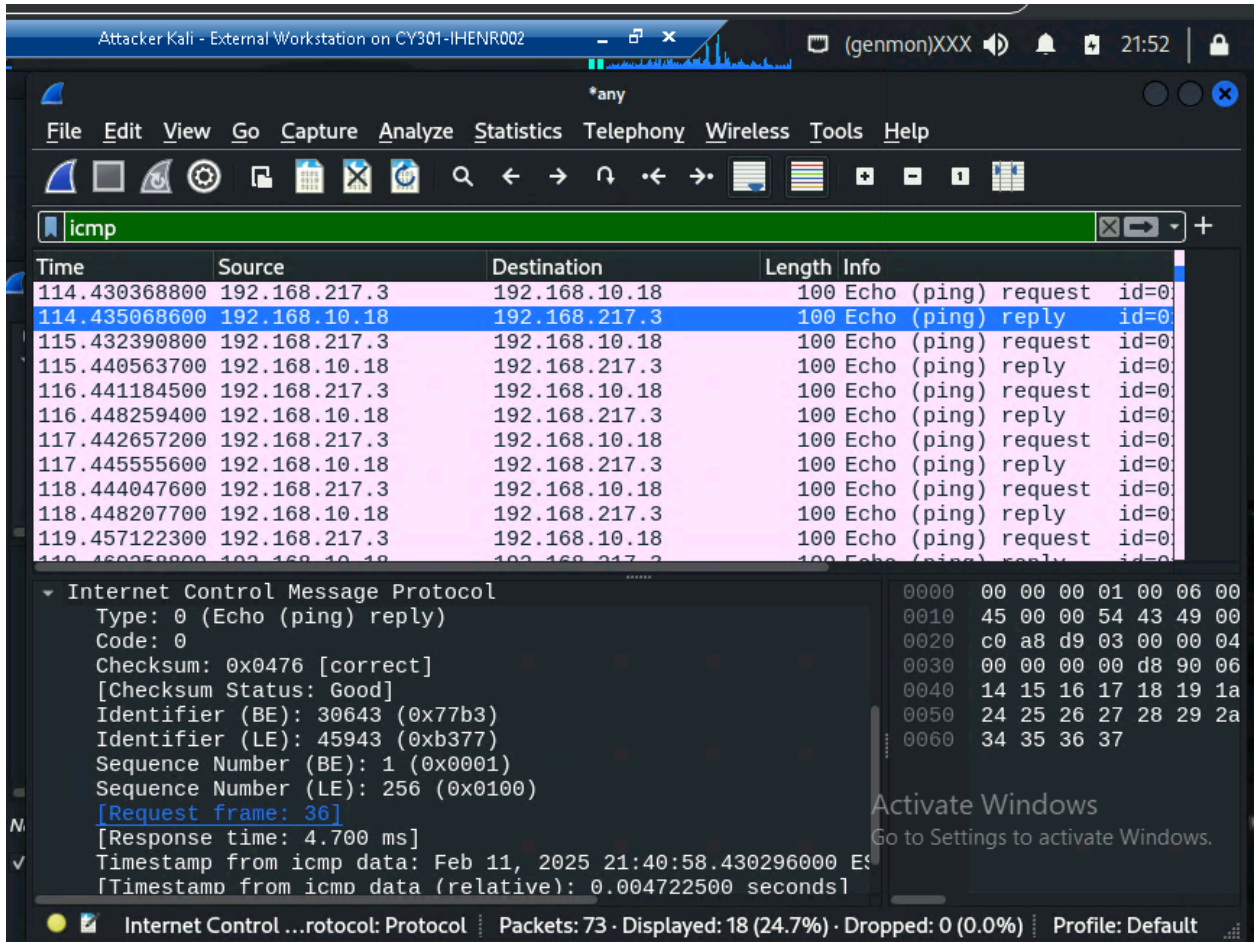
0000 00 00 00 01 00 06 00
 0010 45 00 00 54 43 49 00
 0020 c0 a8 d9 03 00 00 04
 0030 00 00 00 00 d8 90 06
 0040 14 15 16 17 18 19 1a
 0050 24 25 26 27 28 29 2a
 0060 34 35 36 37

Internet Control ...rotocol: Protocol Packets: 73 · Displayed: 18 (24.7%) · Dropped: 0 (0.0%) Profile: Default

I selected the second packet from the list.

Source IP: 192.168.10.18

Destination IP: 192.168.217.3



After doubling clicking the packet and expanding the “Internet Control Message Protocol”

I found the sequence numbers, size of data, and response time

Sequence Number BE: 30643

Size for Sequence Number BE: (0x0001)

Sequence Number LE: 45943

Size for Sequence Number LE: (0x0100)

Response time: 4.700 ms