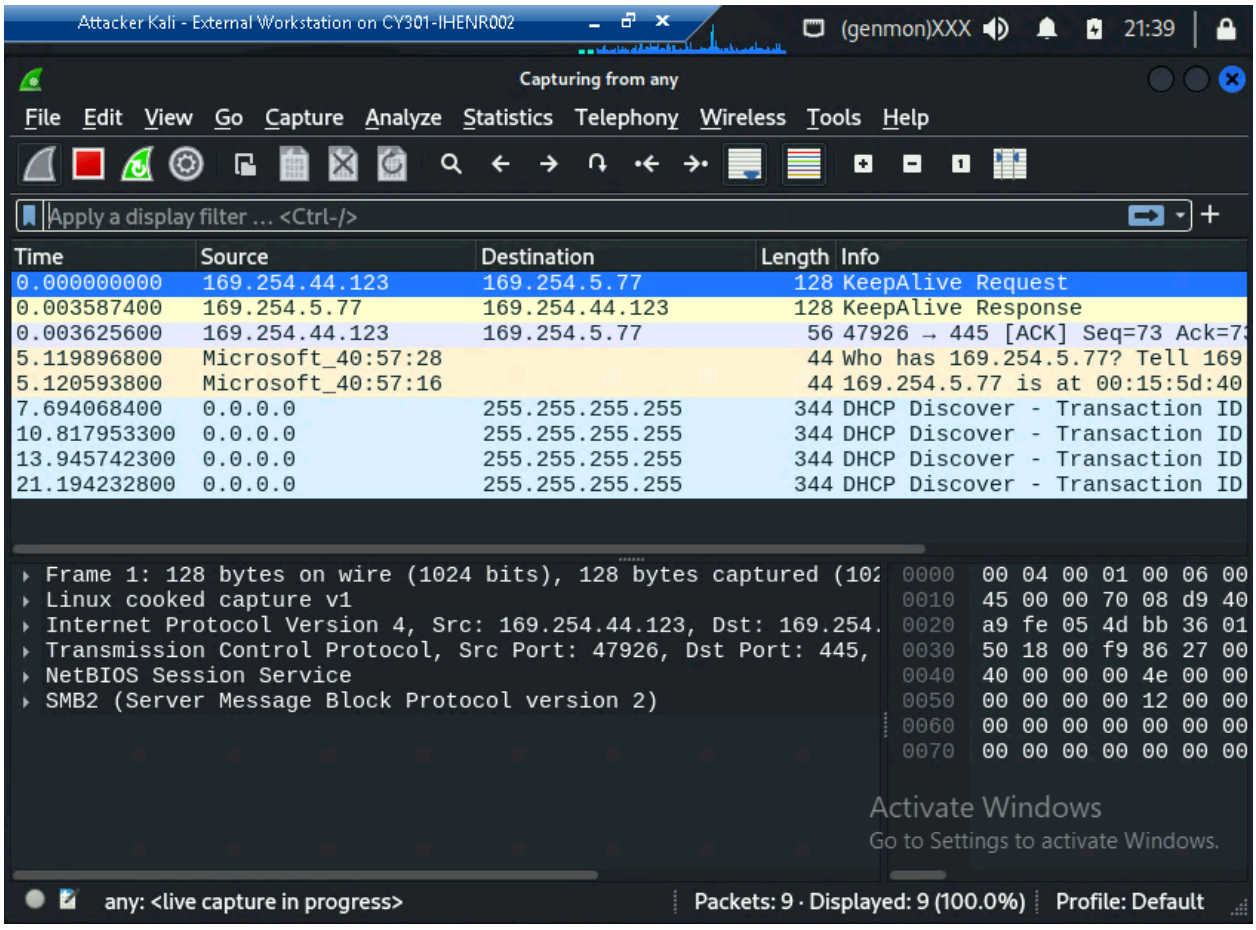
India Henry
CYSE 301 - 32781
Shideh Yavary Mehr
10 February 2025

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

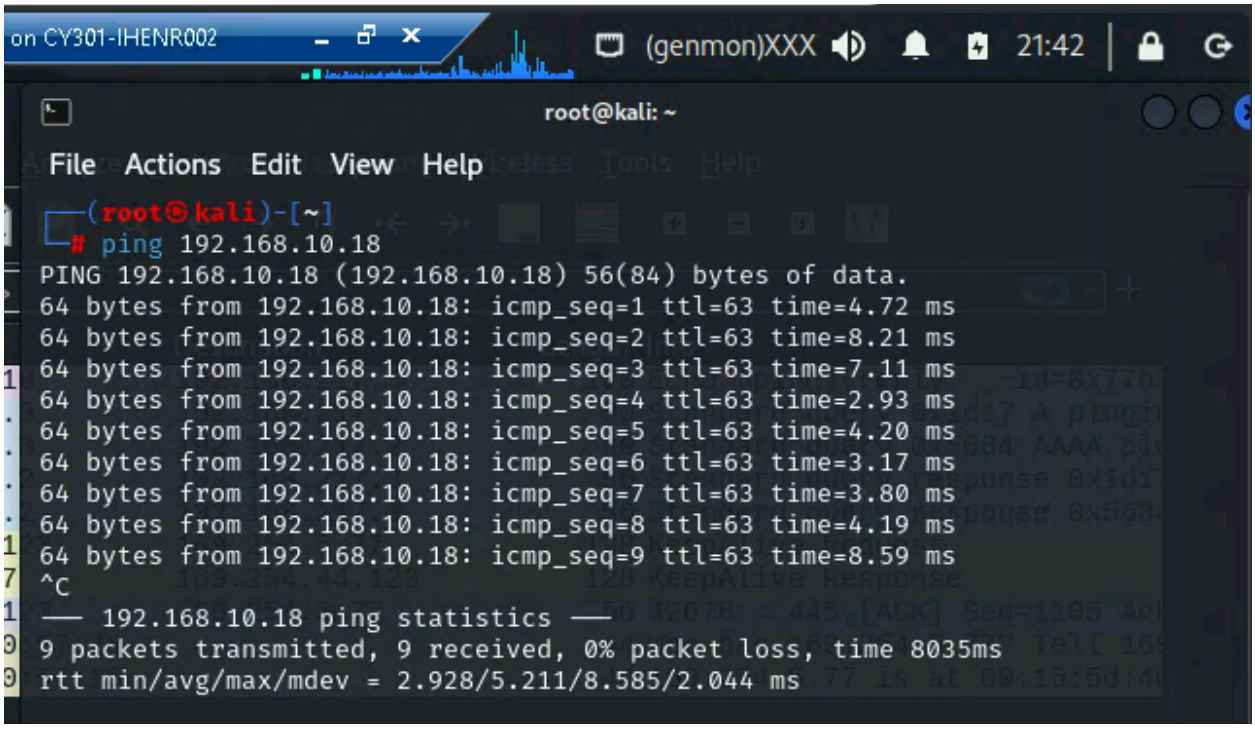
Assignment 2.1

1. **Open Wireshark on External Kali and listen on interface “etho0”**



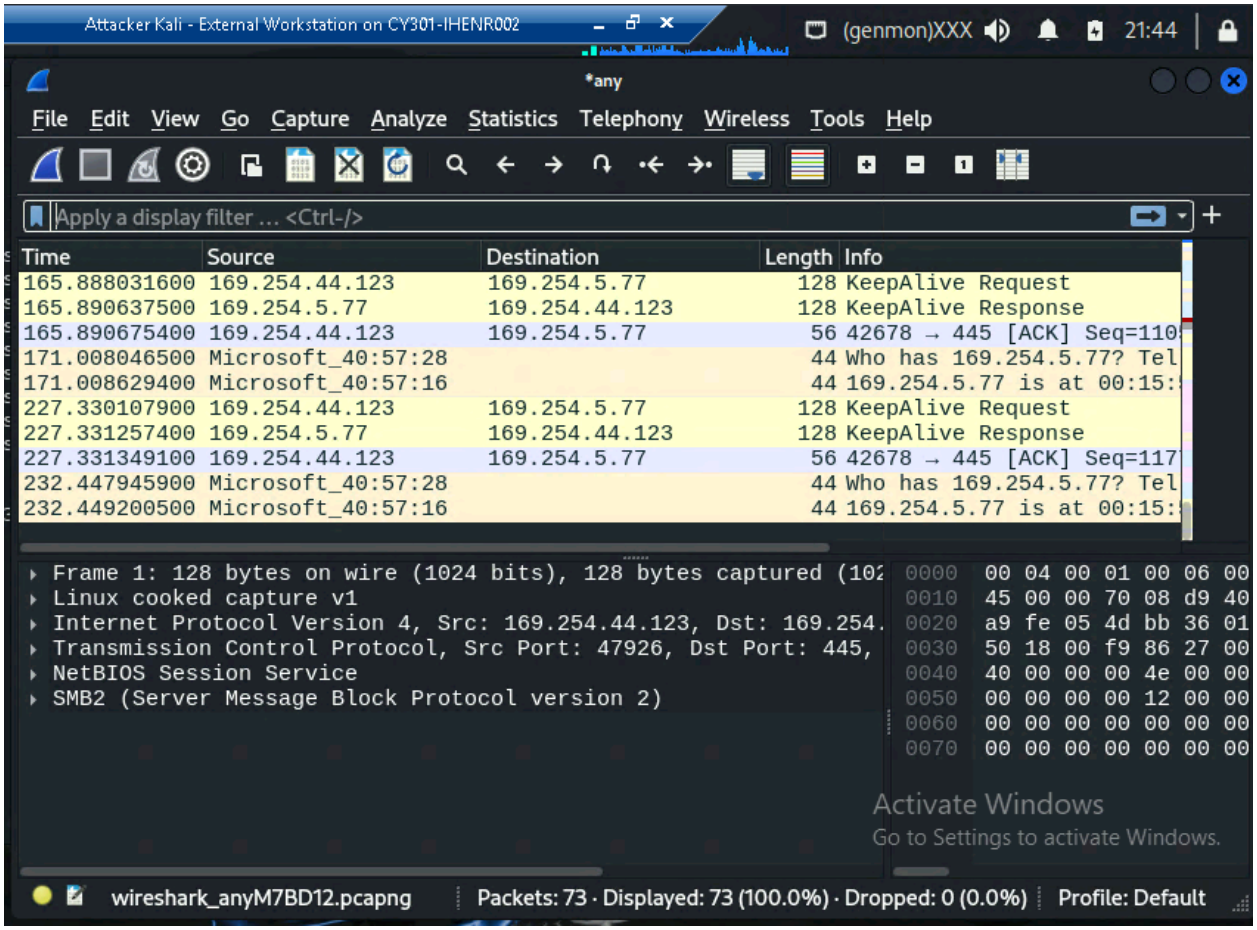
I used any instead of eth0 because eth0 wasn’t giving me any packets. I just typed wireshark into external kali.

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



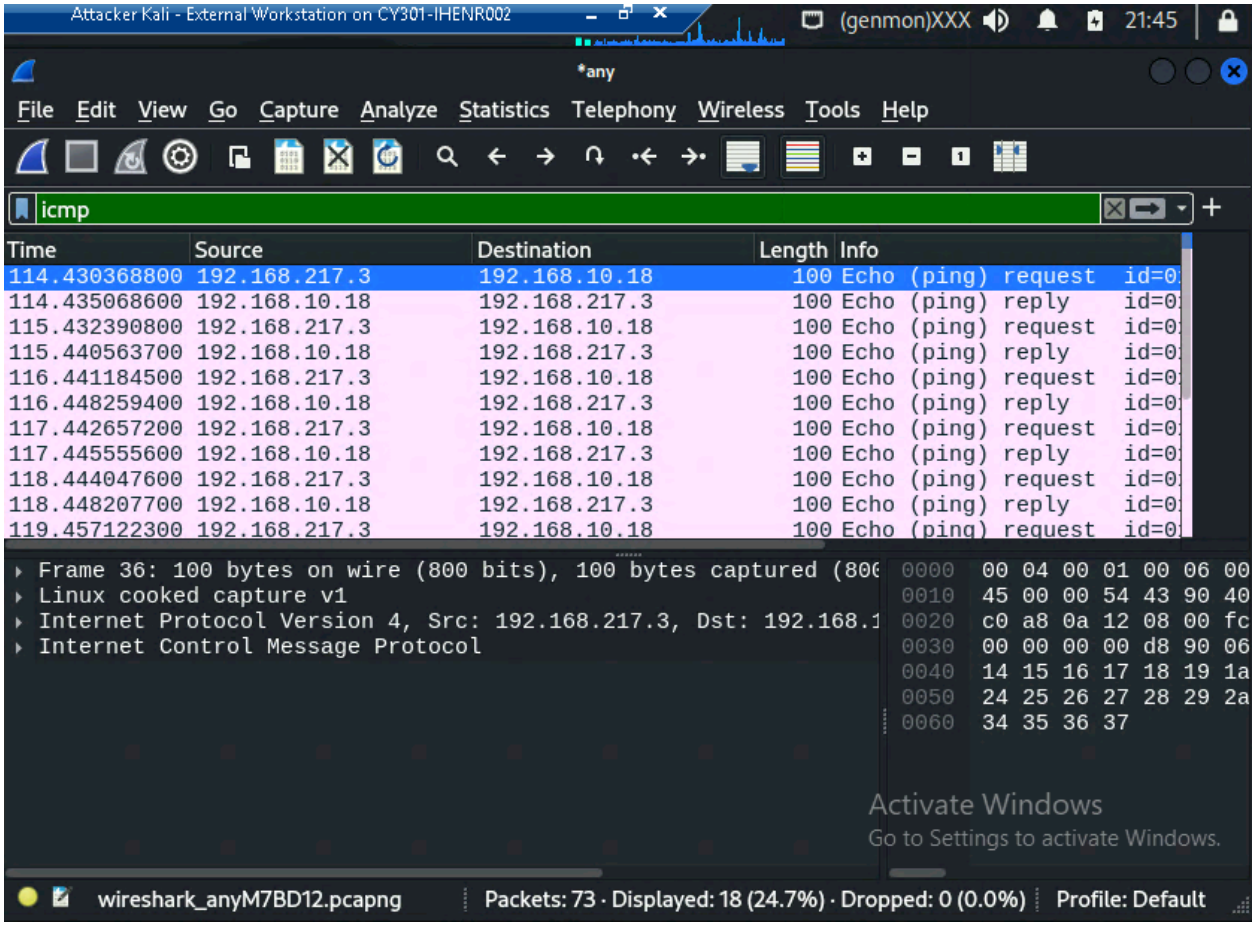
Here I opened another terminal and pinged the Ubuntu VM IP and ran it for about 7 seconds.

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



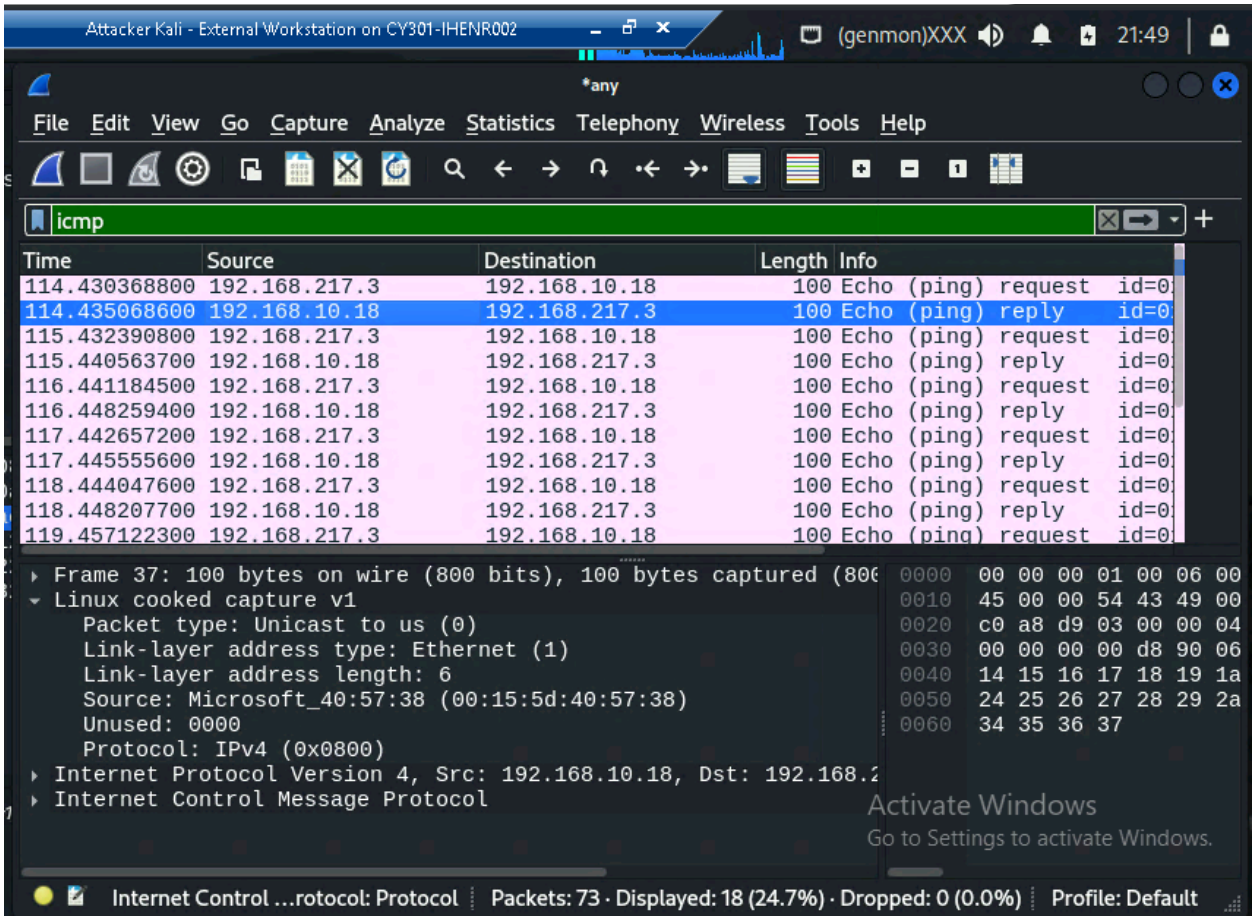
I pressed the square button at the top next to the shark fin icon to stop capturing.

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**

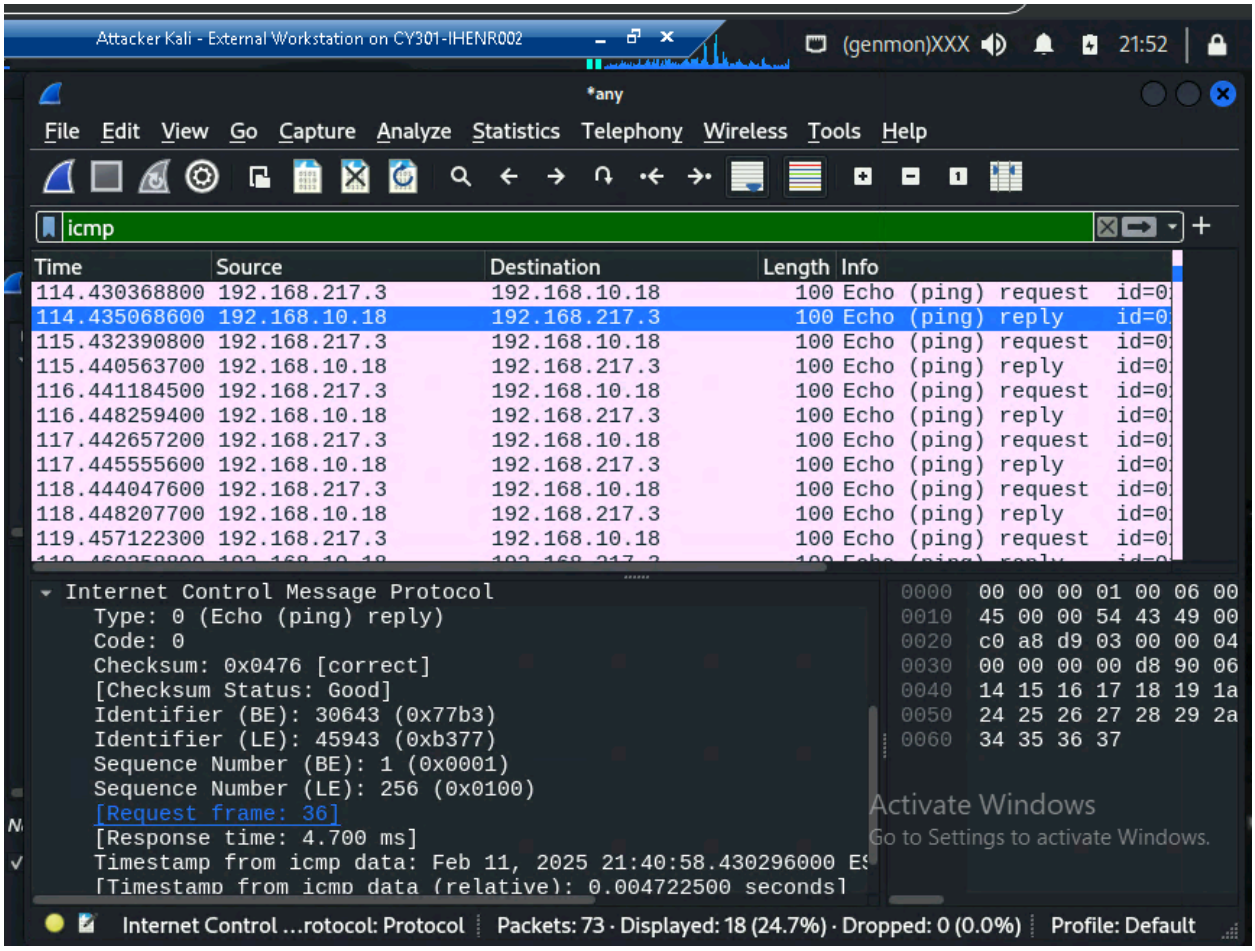


I typed lowercase “icmp” in the filter
73 packets total; 18 displayed

3. **Select an Echo (replay) 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?**



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