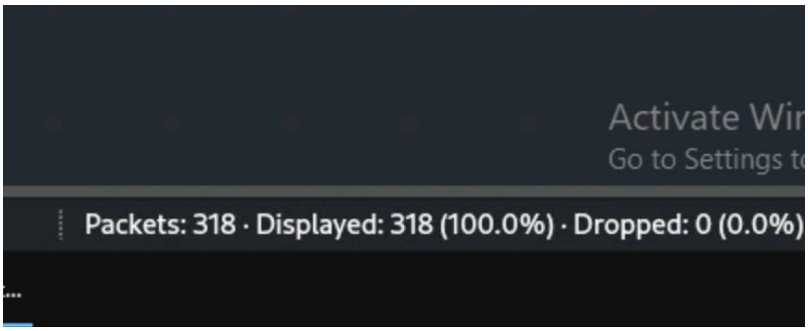
OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS
Assignment #2 Traffic Tracing and Sniffing

Celeste Meraz-Luna
01302562

Task A: Get Started with Wireshark

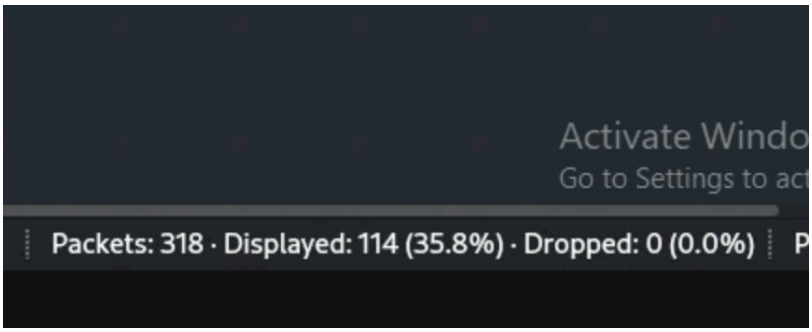
Q1. How many packets are captured in total? How many packets are displayed?

318 packets were captured and displayed in total.



Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).

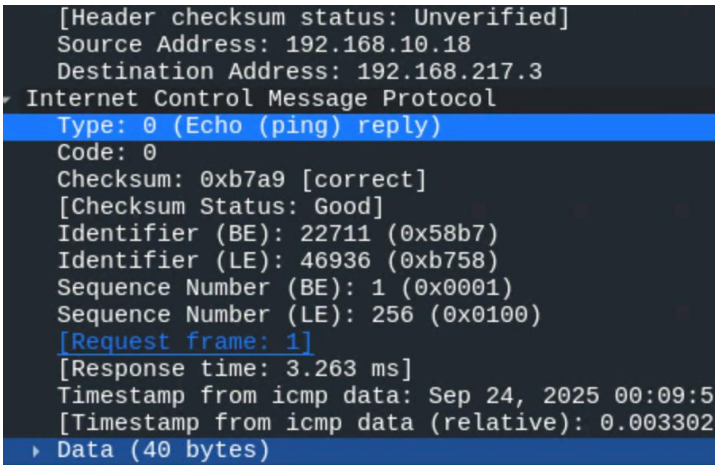
After applying the "ICMP" filter 318 packets were captured and 114 packets were displayed.



Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

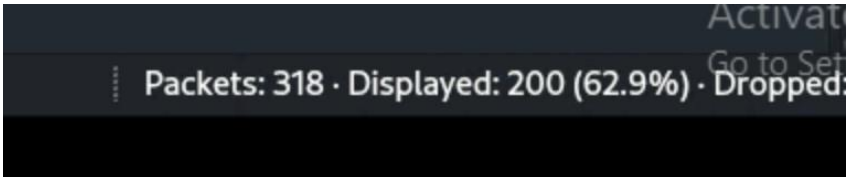
Under the IPV4 header the Source IP: 192.168.10.18, Destination IP 192.168.217.3

Under the ICMP header the Sequence Number: 1 (0x0001), Size of Data: 40 bytes, Response Time: 3.263 ms.



Q4. Apply "DNS" as a display filter in Wireshark. How many packets are displayed?

After applying the "DNS" filter 318 packets were captured, and 200 packets were displayed.

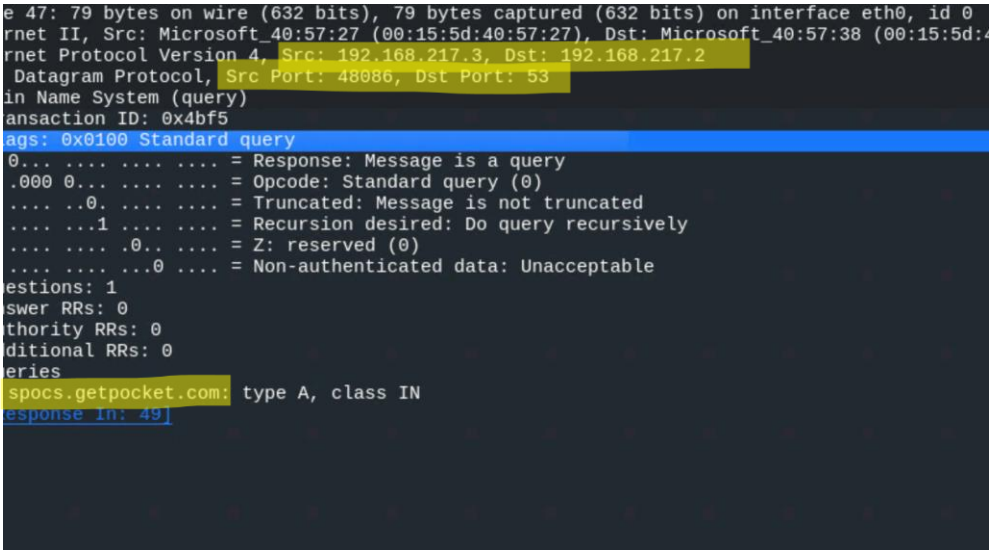


Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

The domain name is under the Queries header: spocs.getpocket.com

The source IP and port 192.168.217.3:48086

The destination IP and port 192.168.217.2:53



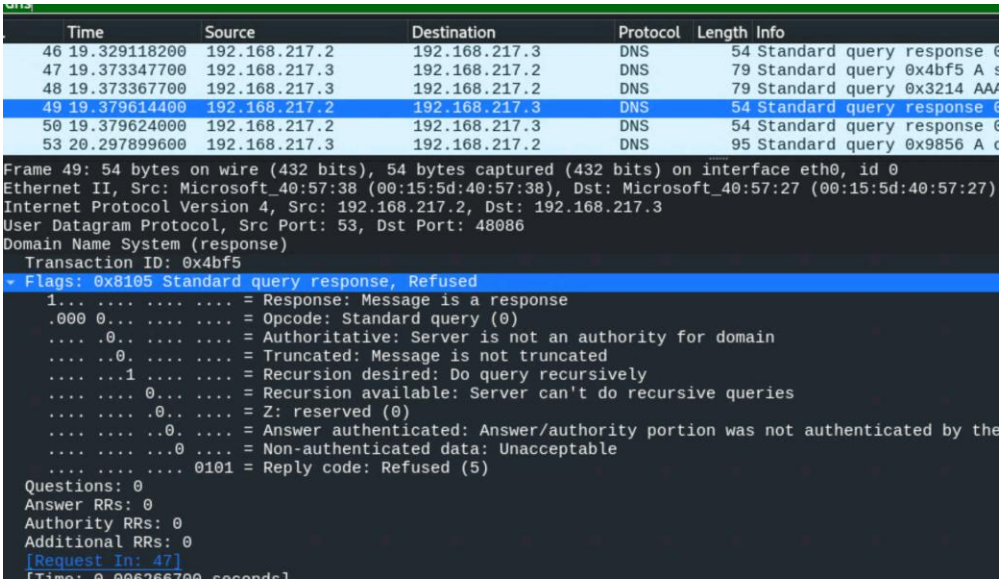
Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

I found the responding packet by looking for the same transaction ID: 0x4bf5.

The source IP and port: 192.168.217.2:53

The destination IP and port: 192.168.217.3:48086

The standard query response is “Refused.”

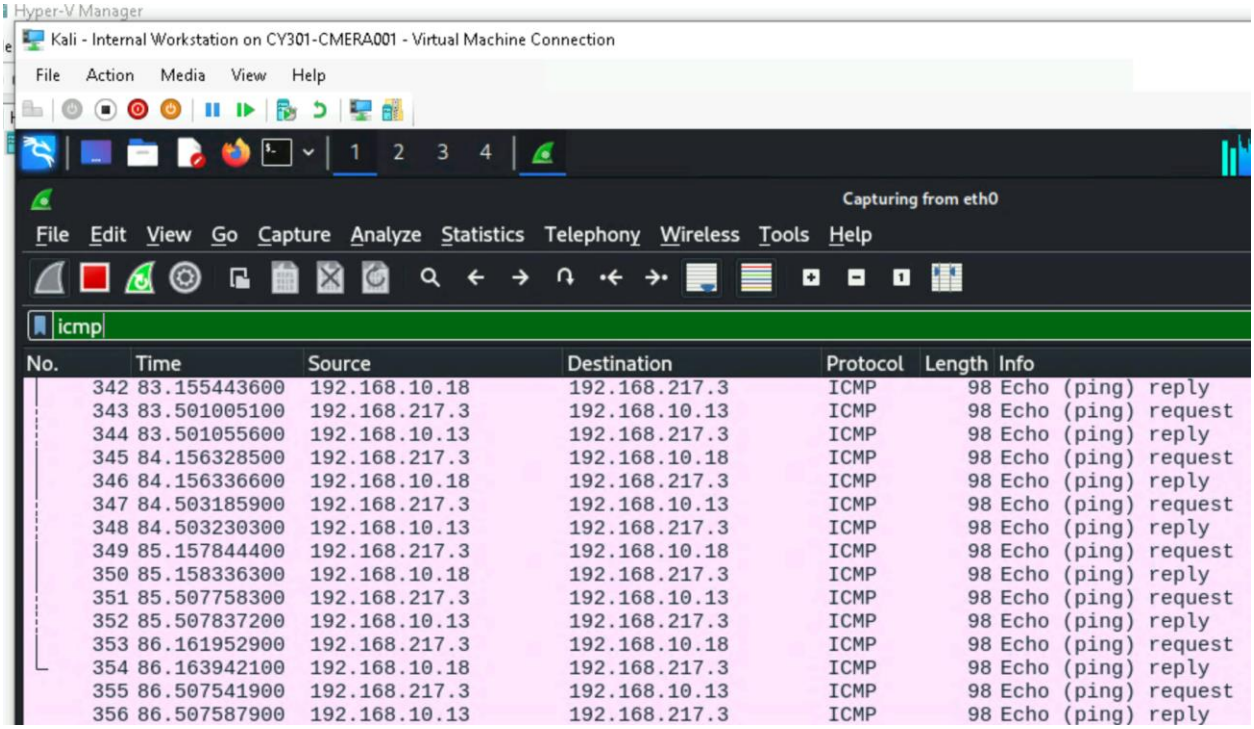


Task B: Sniff LAN Traffic

Q1: Sniff ICMP Traffic

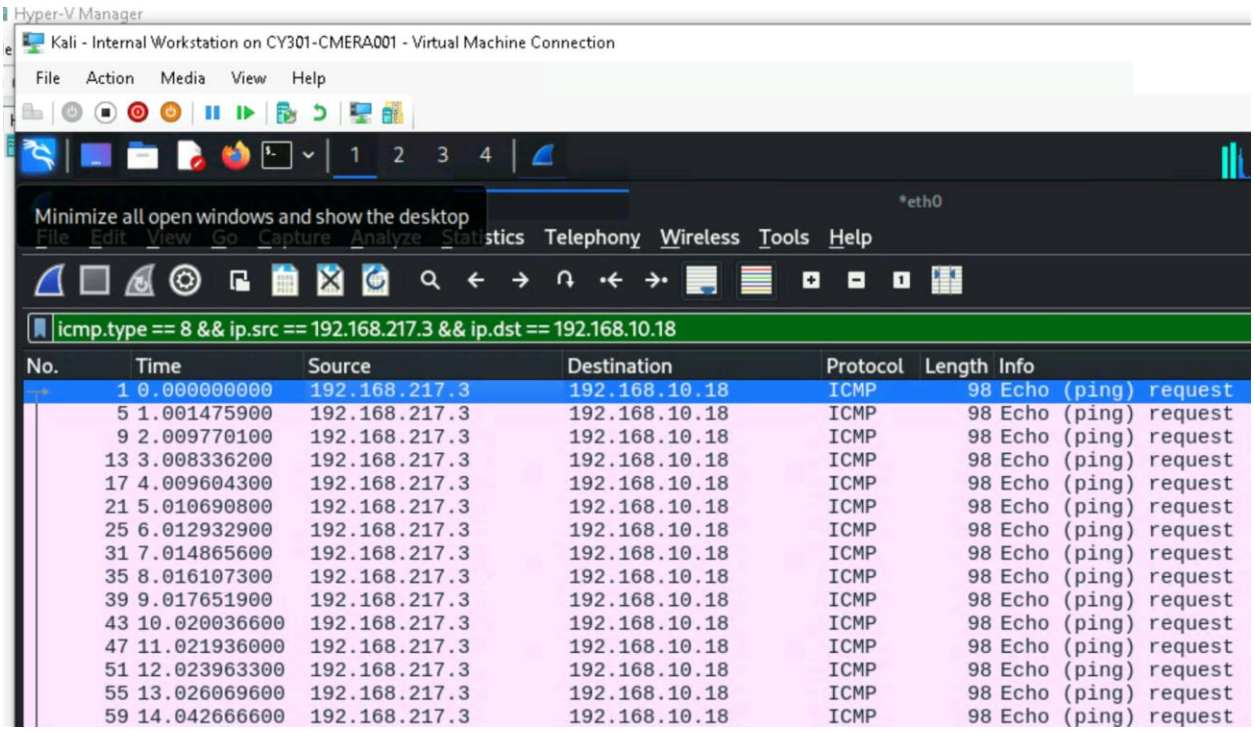
a. Apply proper display or capture filter in Wireshark on Internal Kali VM to show active ICMP traffic.

I applied the ICMP filter to display the active ICMP traffic.



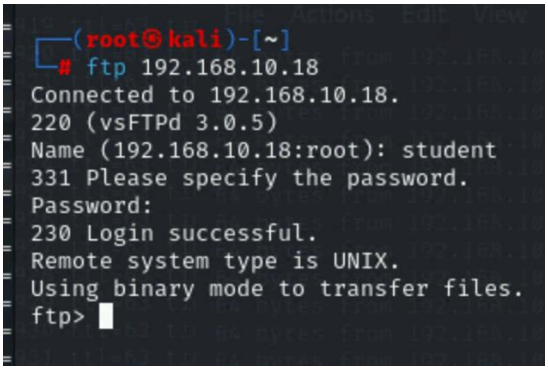
b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM.

I applied the filter icmp.type == 8 && ip.src == 192.168.217.3 && ip.dst == 192.168.10.18. This filter displays the ICMP requests from external Kali VM and goes to the Ubuntu 64-bit VM.

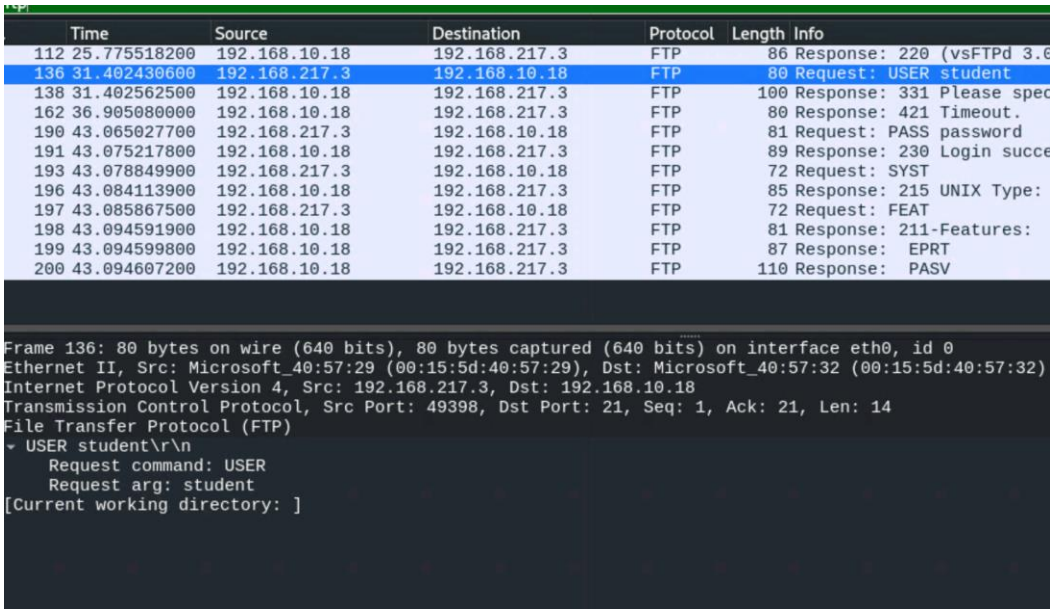


Q2: Sniff FTP Traffic

a. On External Kali I used the FTP 192.168.10.18 command to access the FTP server.



b. Using the FTP filter, I was able to find the USER and PASS of the credentials submitted in the FTP Server. The USER: student and PASS: password



c. This time I used the ftp.request.command to filter out the USER and PASS. MY midas and uin number are shown as the USER and PASS.