OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

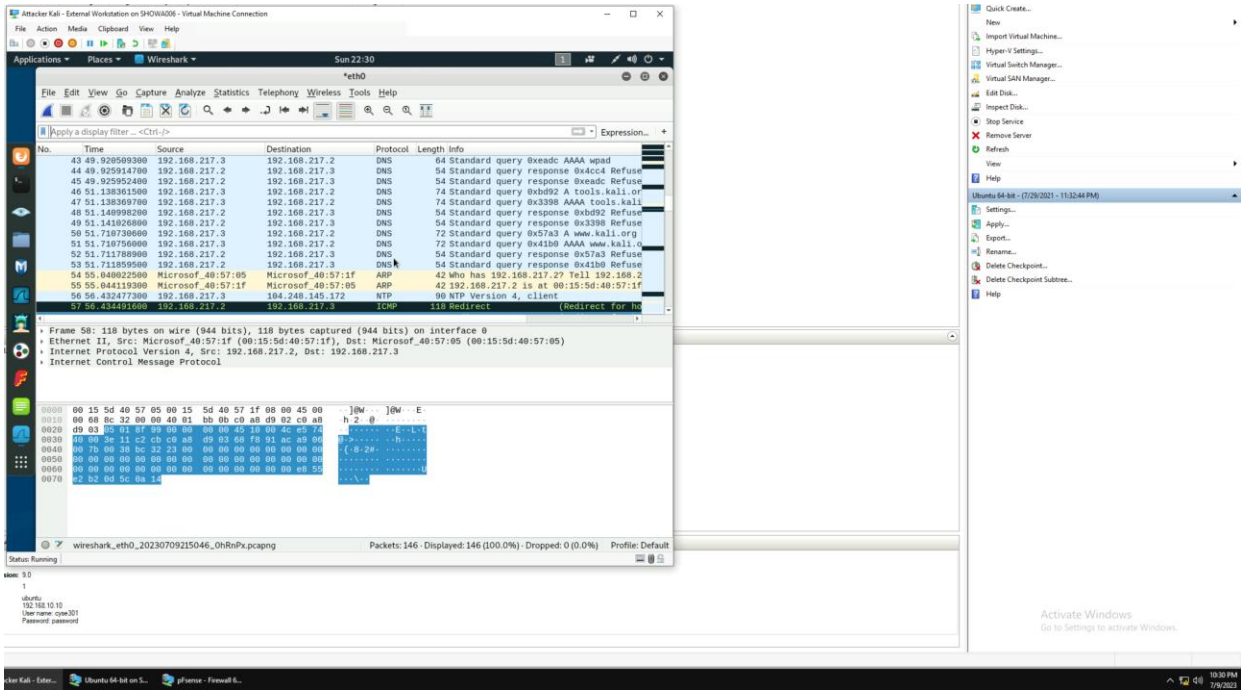
Assignment 2: Traffic Tracing and Sniffing pt A.

Stuart N. Howard

01241576

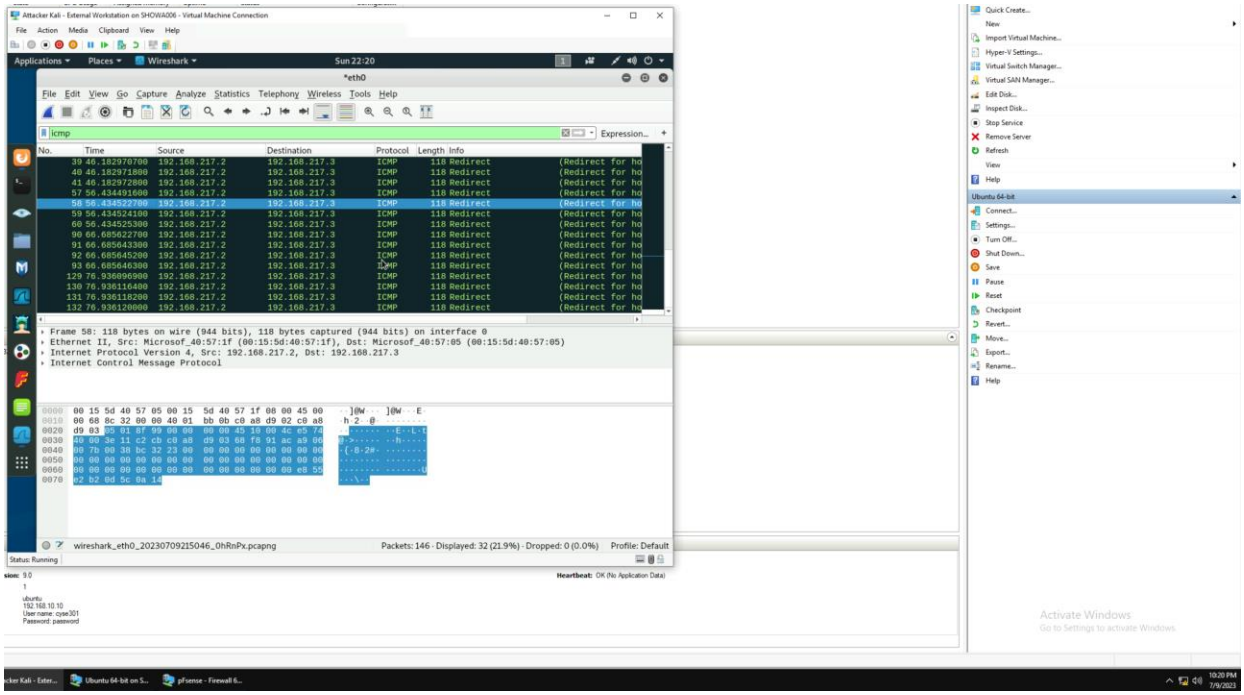
Q1. How many packets are captured in total? How many packets are displayed?

146 Total packages captured, 146 packages displayed.



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

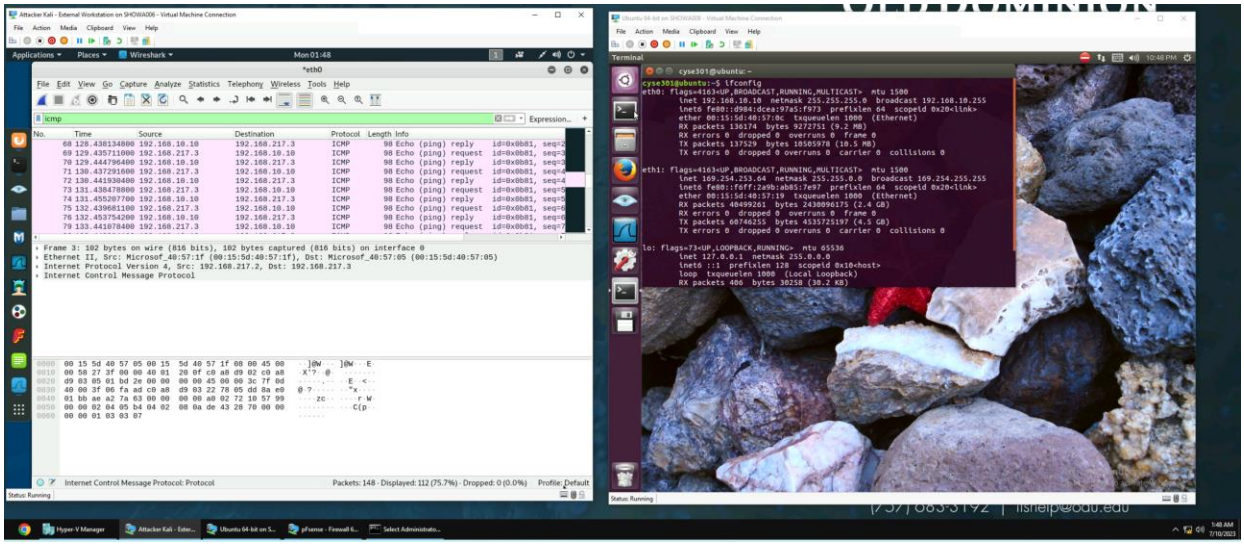
146 Total packages captured, 32 packages displayed.



Q3. Select an Echo (replay) message from the list.

What are the source and destination IPs of this packet?

Source IP is 192.168.10.10 and destination IP is 192.168.217.3

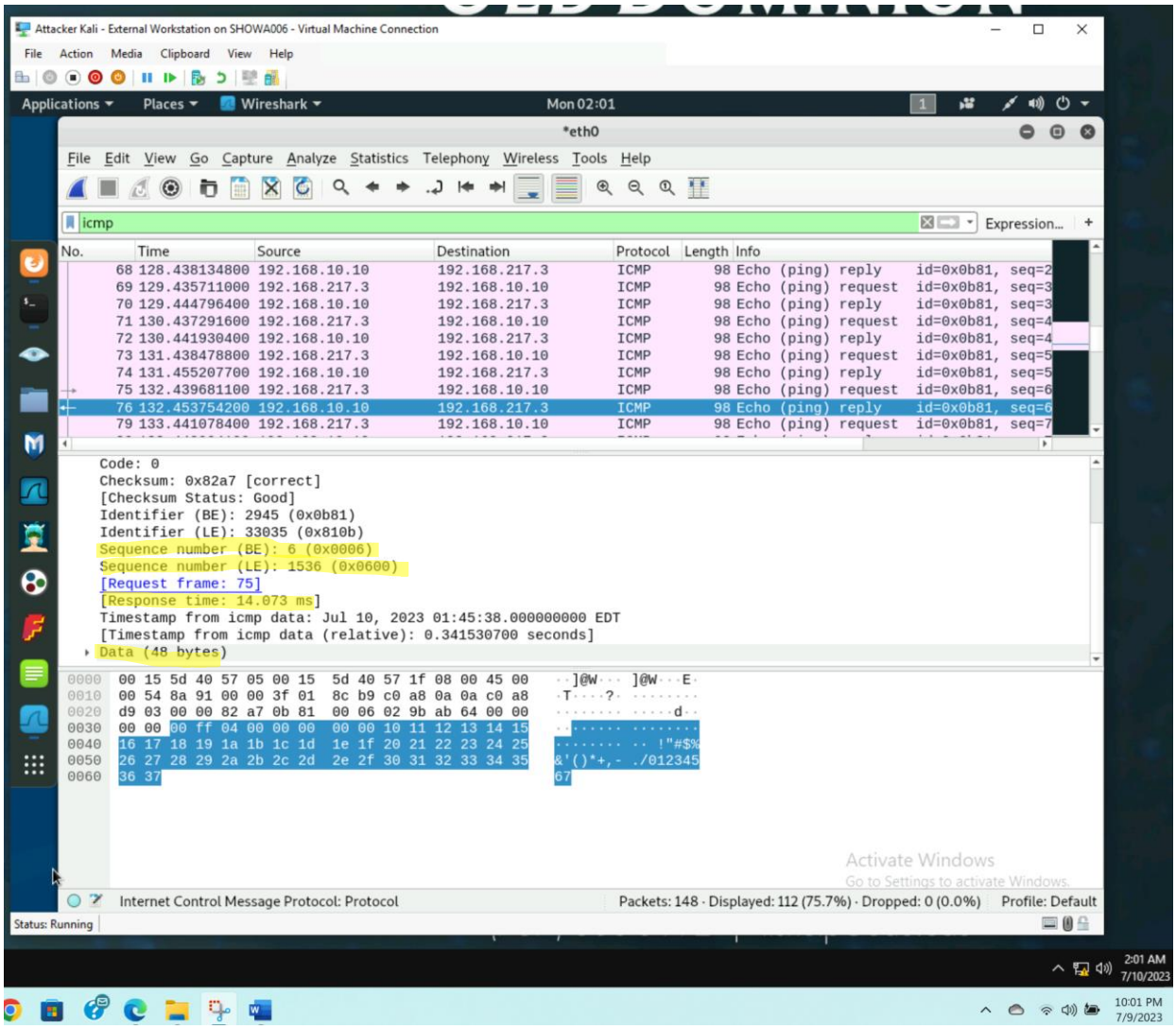


What are the sequence number and the size of the data?

Sequence number is (BE) 6 (LE) 1536 and date size is 48bytes

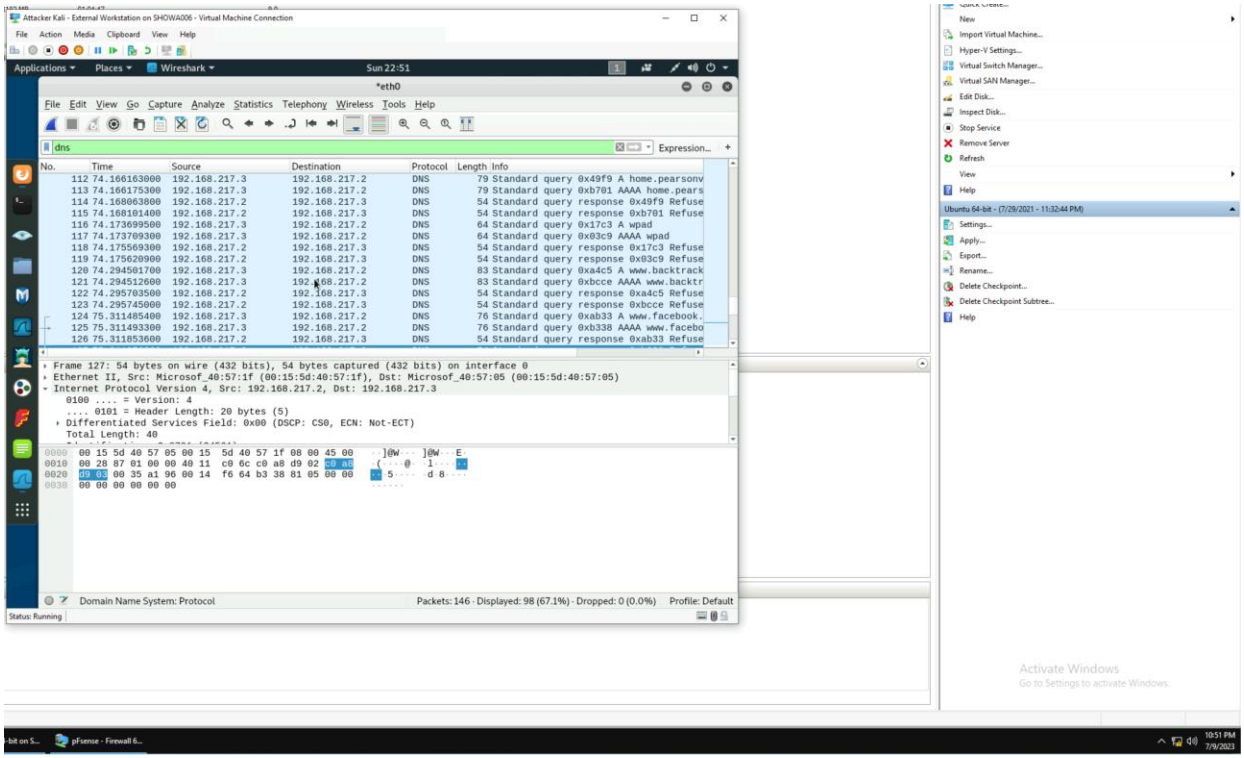
What is the response time?

Response time is 14.037 ms



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

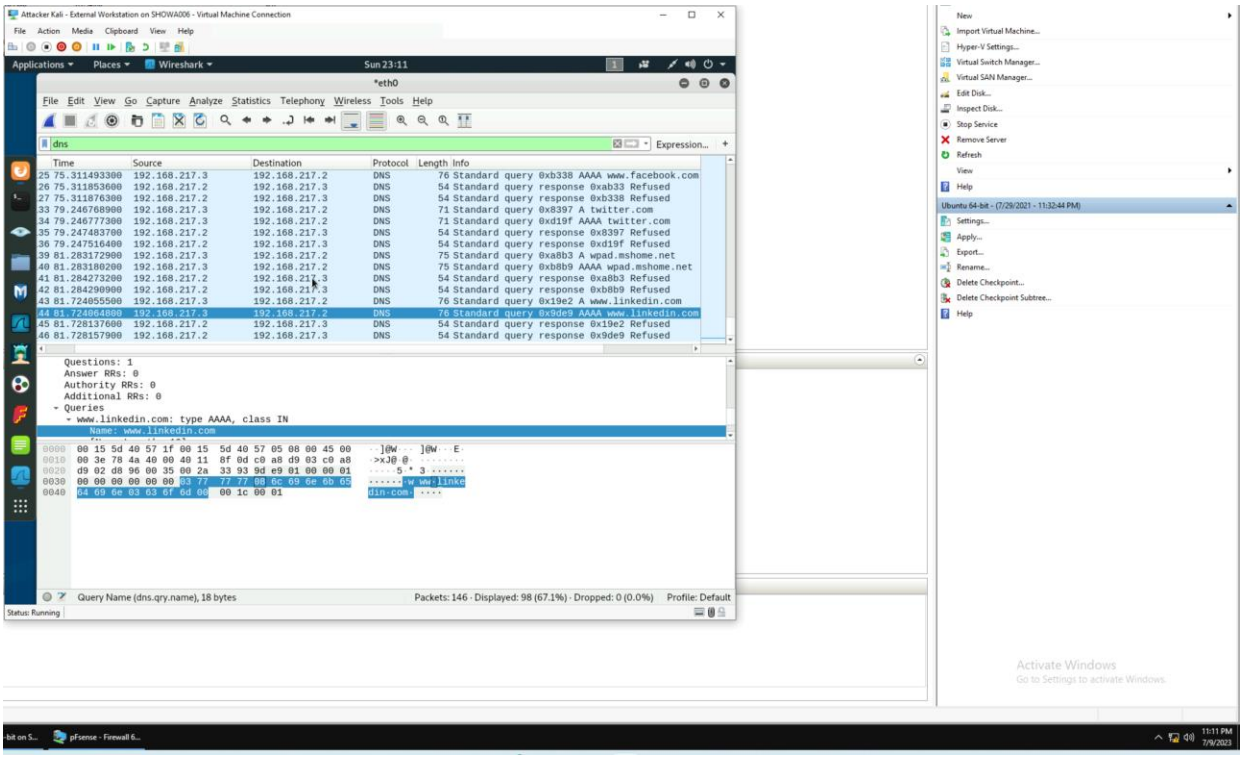
146 Total packages captured, 98 packages displayed**.**



Q5. Find a DNS query packet.

What is the domain name this host is trying to resolve?

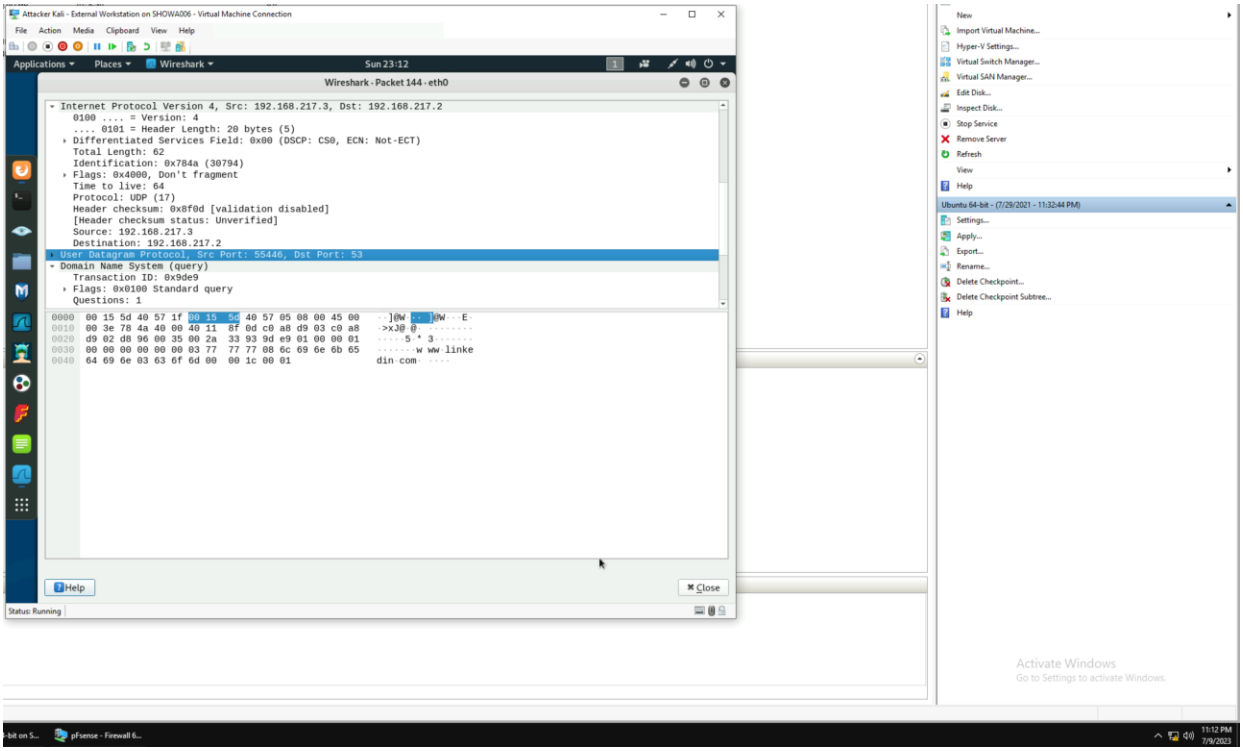
www.linkedin.com



What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

Source IP/port 192.168.217.3:55446

Dst IP/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

Source IP/port 192.168.217.2:53

Dst IP/port 192.168.217.3:55446**?**

What is the message replied from the DNS server?

Flags: 0x8105 Standard query response, Refused