OLD DOMINION UNIVERSITY

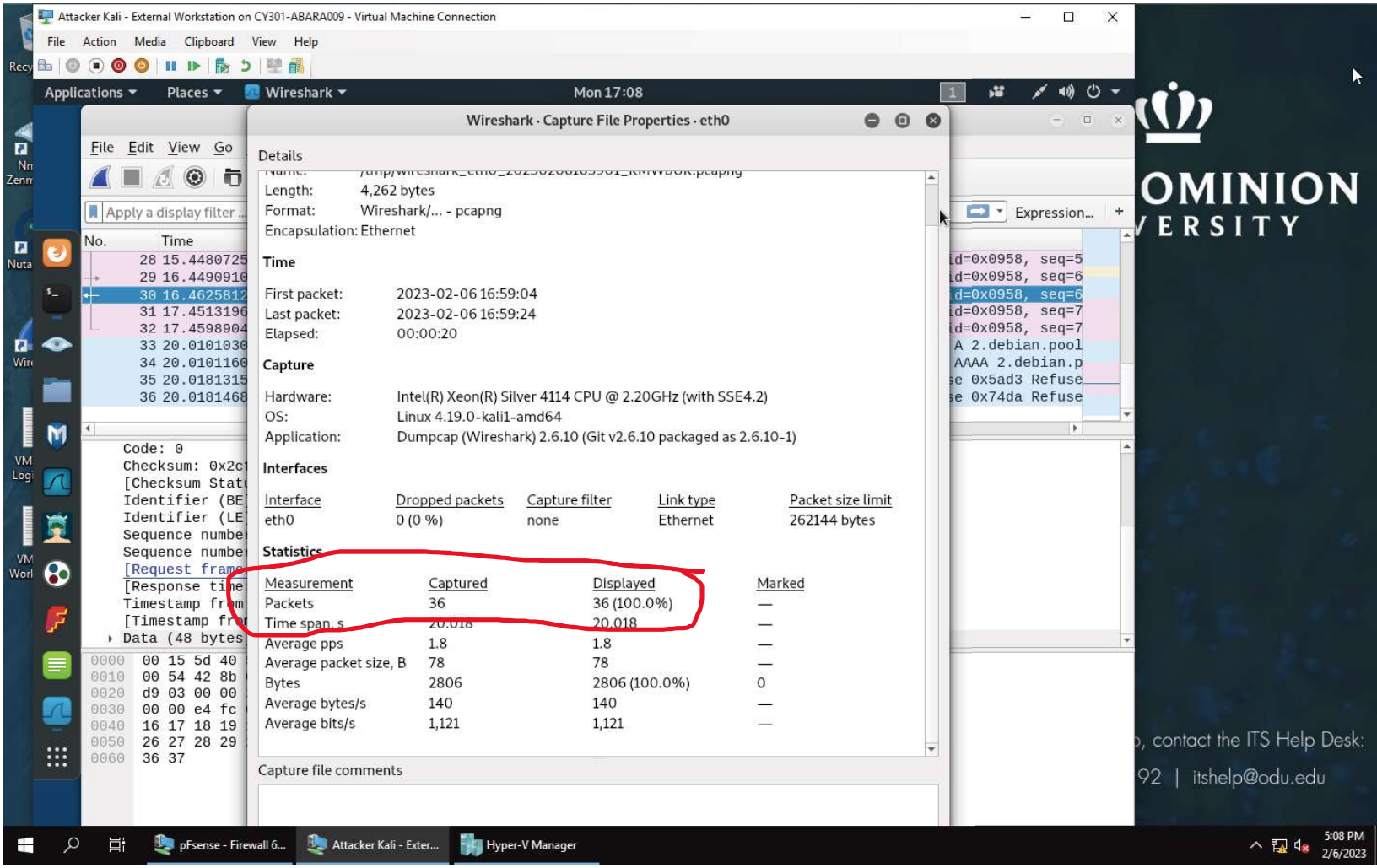
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Ava Baratz
01192426

TASK A

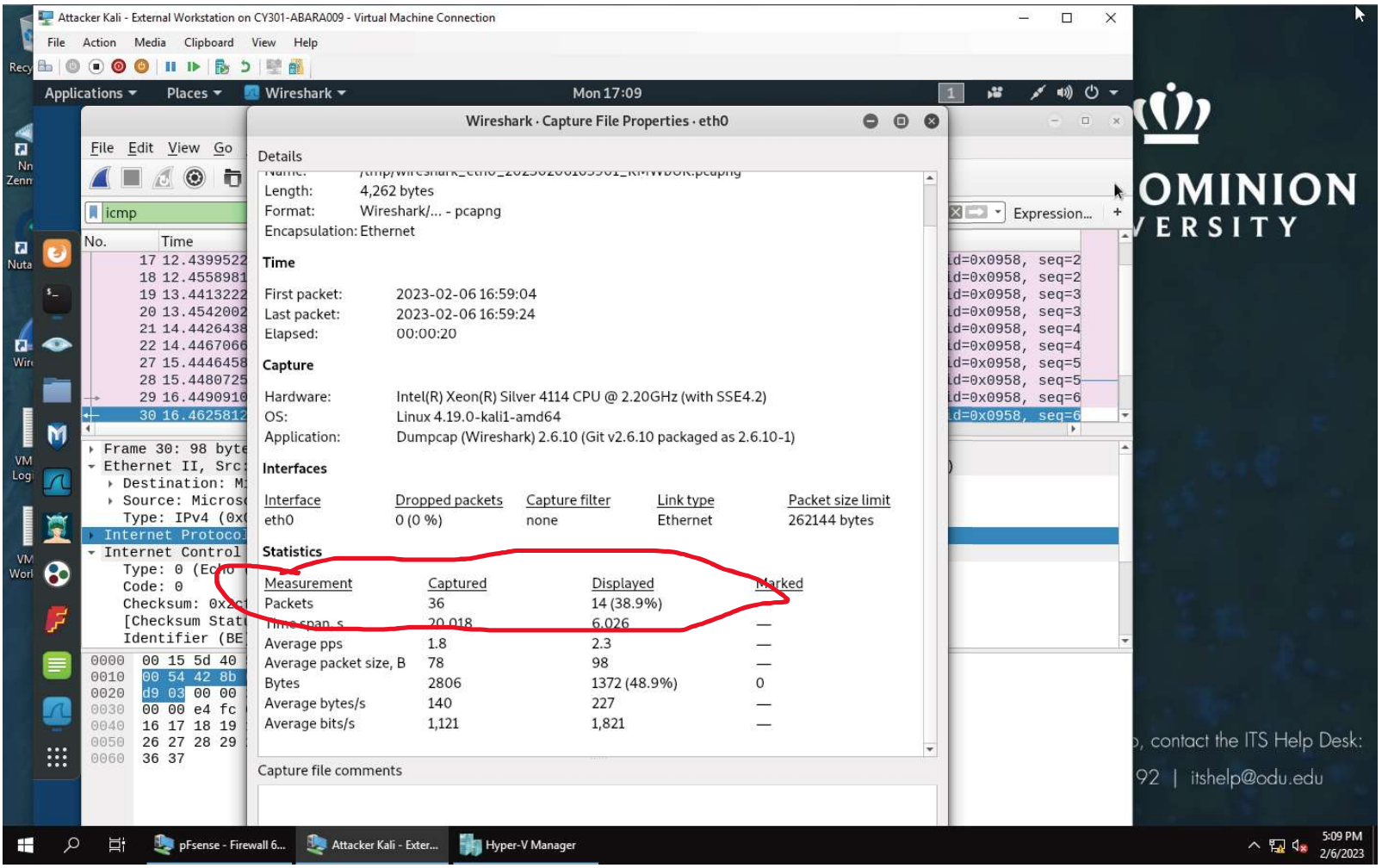
Q1. How many packets are captured in total? How many packets are displayed?



Here, I opened the WireShark Capture File Properties which shows there were 36 packets captured and 36 packets displayed in the eth0 interface.

TASK A (CONTINUED)

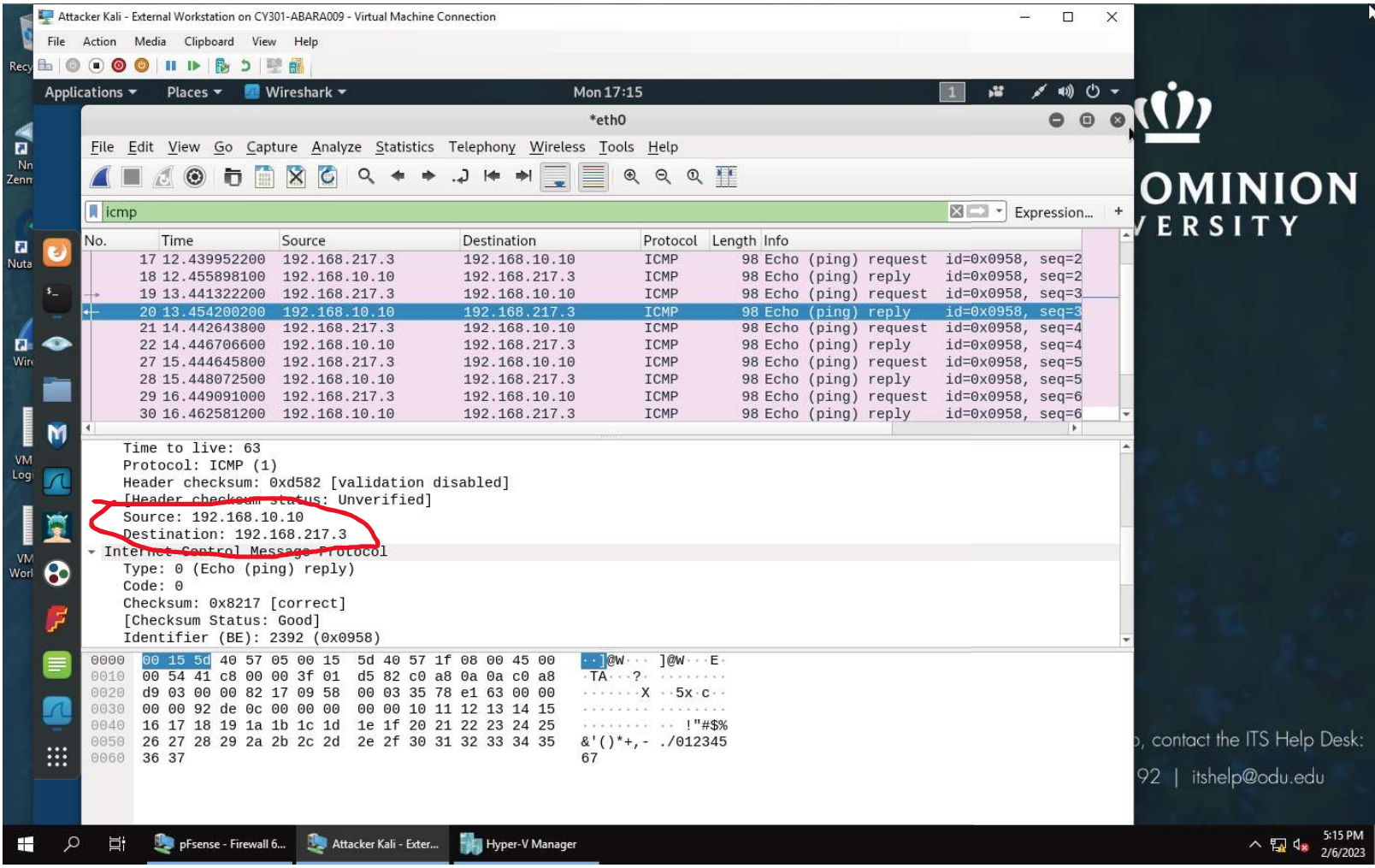
Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous step Q1.



Here, I applied the “icmp” display filter in the search bar. The capture file properties with the ICMP display filter show that there were 36 captured packets and 14 packets displayed in the eth0 interface.

TASK A (CONTINUED)

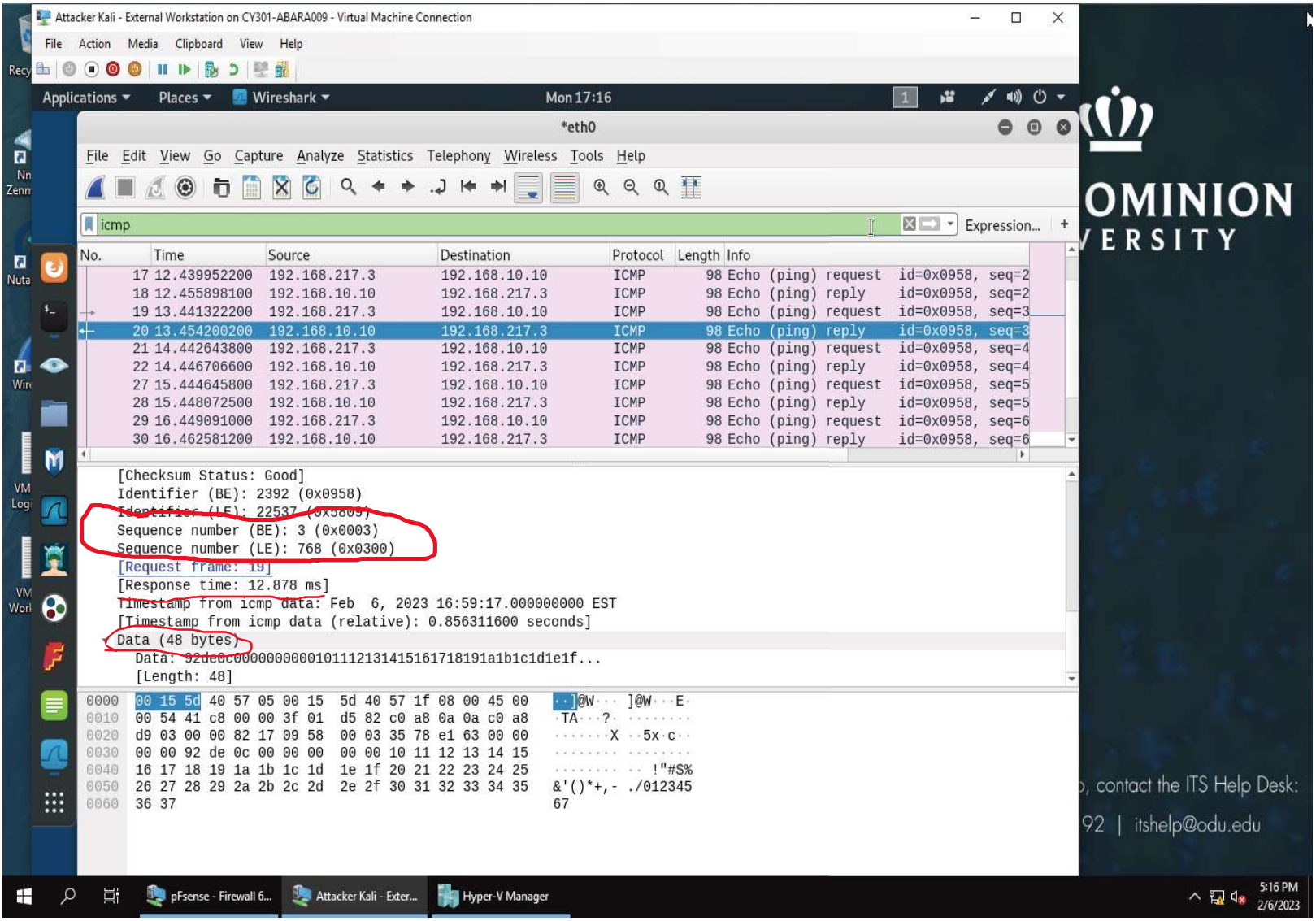
Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this
packet? What are the sequence number and the size of the data? What is the response time?



I selected the 20th packet which is a reply message from the list. This packet has a source IP of 192.168.10.10 and a destination IP of 192.168.217.3.

TASK A (CONTINUED)

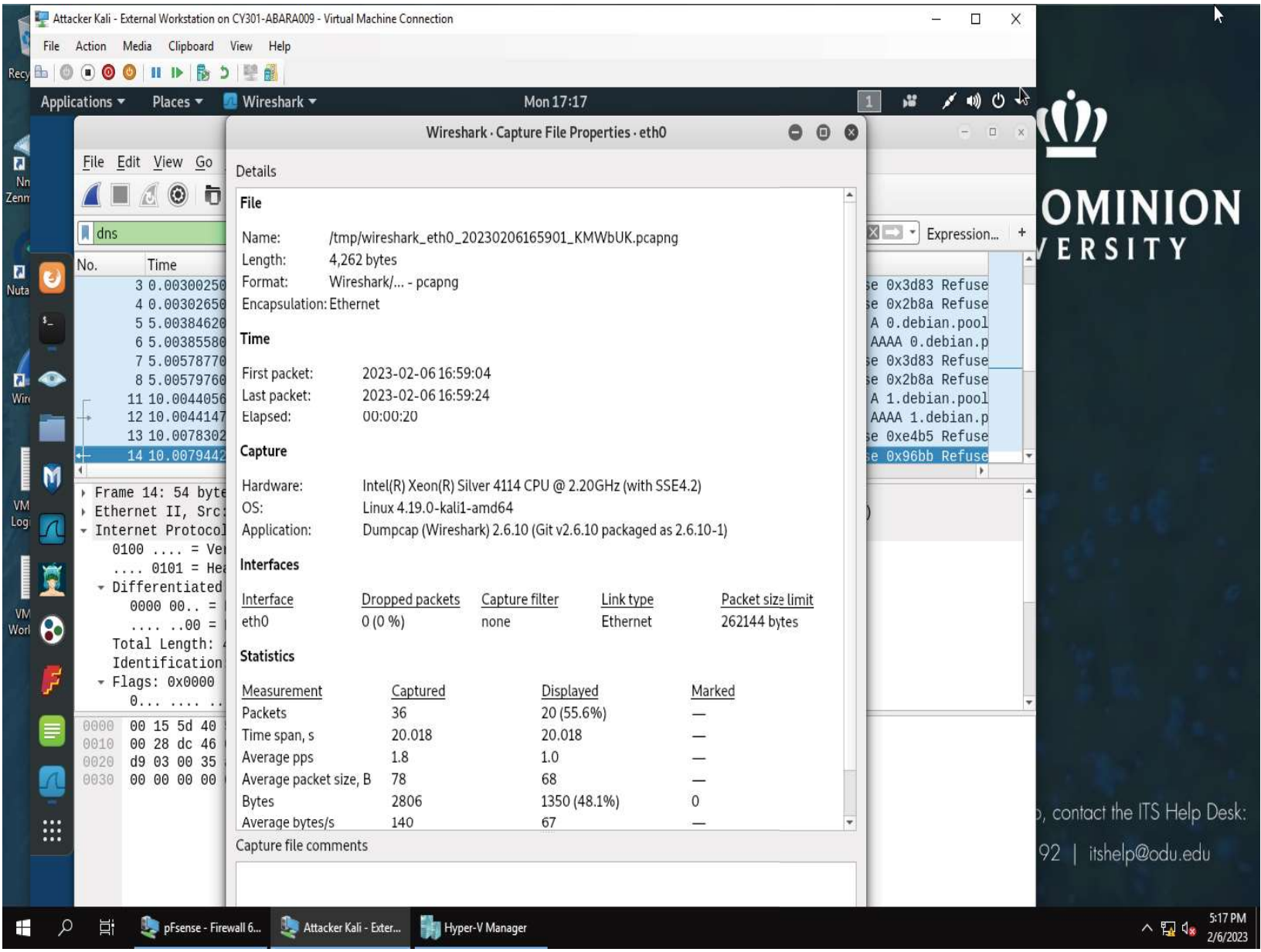
Q3. (Continued) Select an Echo (replay) message from the list. packet? What are the sequence number and the size of the data? What is the response time?



Here, from the 20th packet which is a reply message, the Sequence Number (BE) is 3 (0x0003), and the sequence number (LE) is 768 (0x0300.) The data is 48 bytes. The response time is 12.878 ms.

TASK A (CONTINUED)

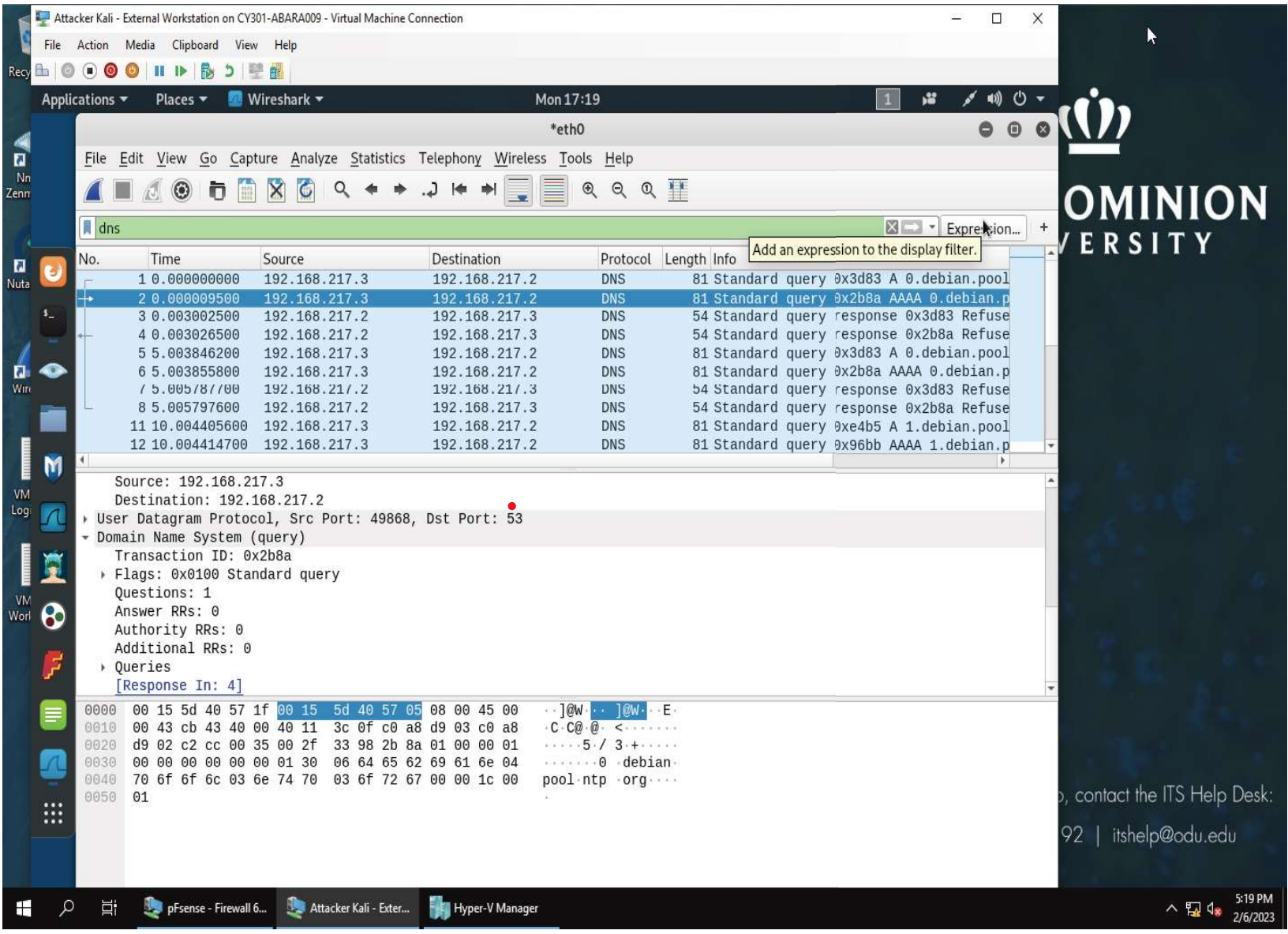
Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



Here, I applied “dns” in the search bar as a display filter in Wireshark. Using Wireshark capture file properties, it shows that 36 packets are captured and 20 packets are displayed with the DNS filter applied.

TASK A (CONTINUED)

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.



Here, I selected the 2nd packet which is a standard query packet. The domain name that the host is trying to resolve is 0x2b8a. The source IP and source port is 192.168.217.3 : 49868. The destination IP and dst port is 168.192.217.2 : 53.