Assignment: Lab 2 – Traffic Tracing and Sniffing

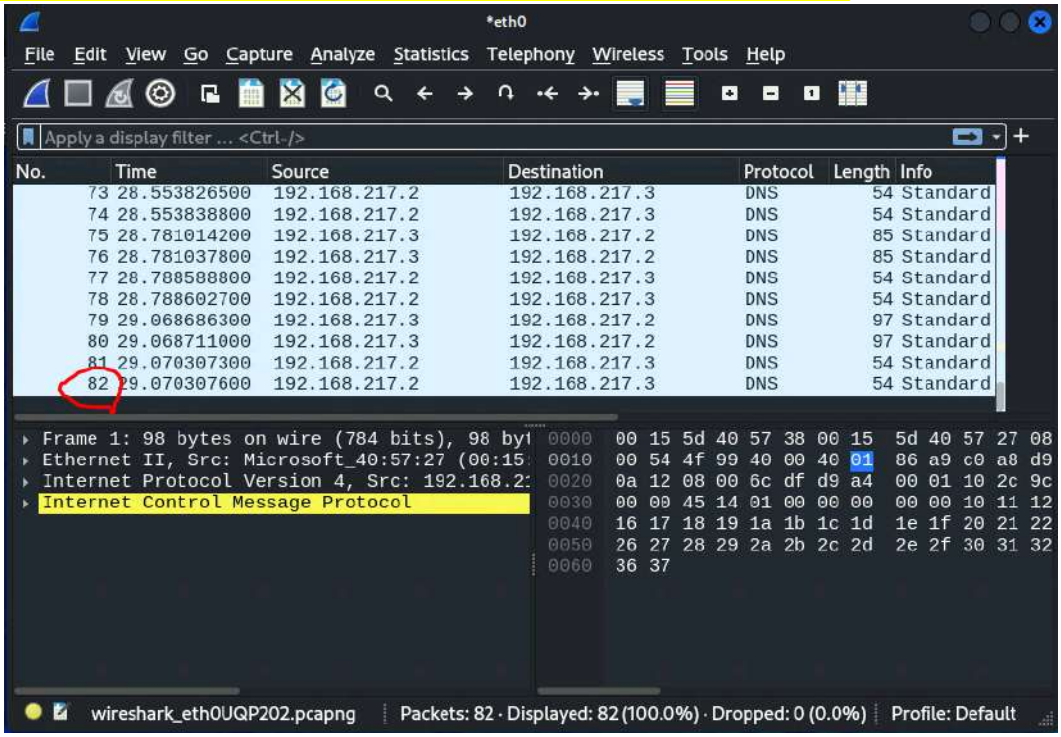
CYSE 301 – Professor Vatsa

Brandon Creech (UIN: 01215415)

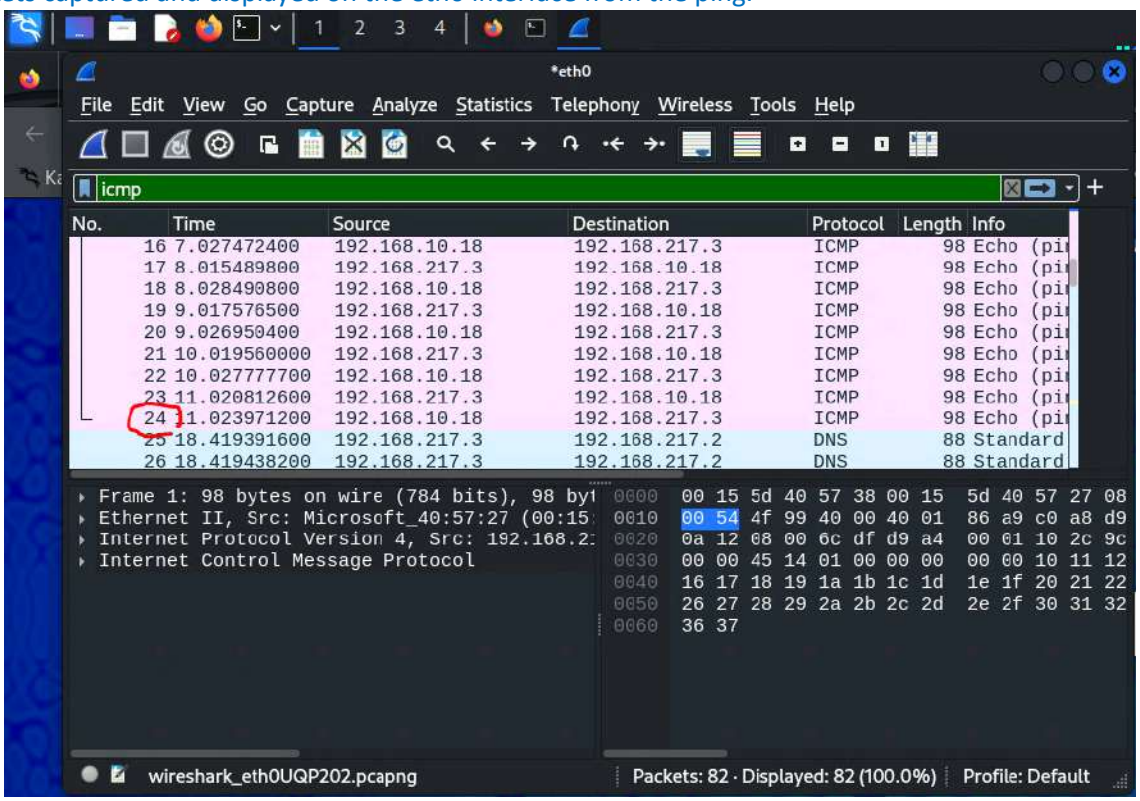
Old Dominion University

TASK A: Get Started with Wireshark

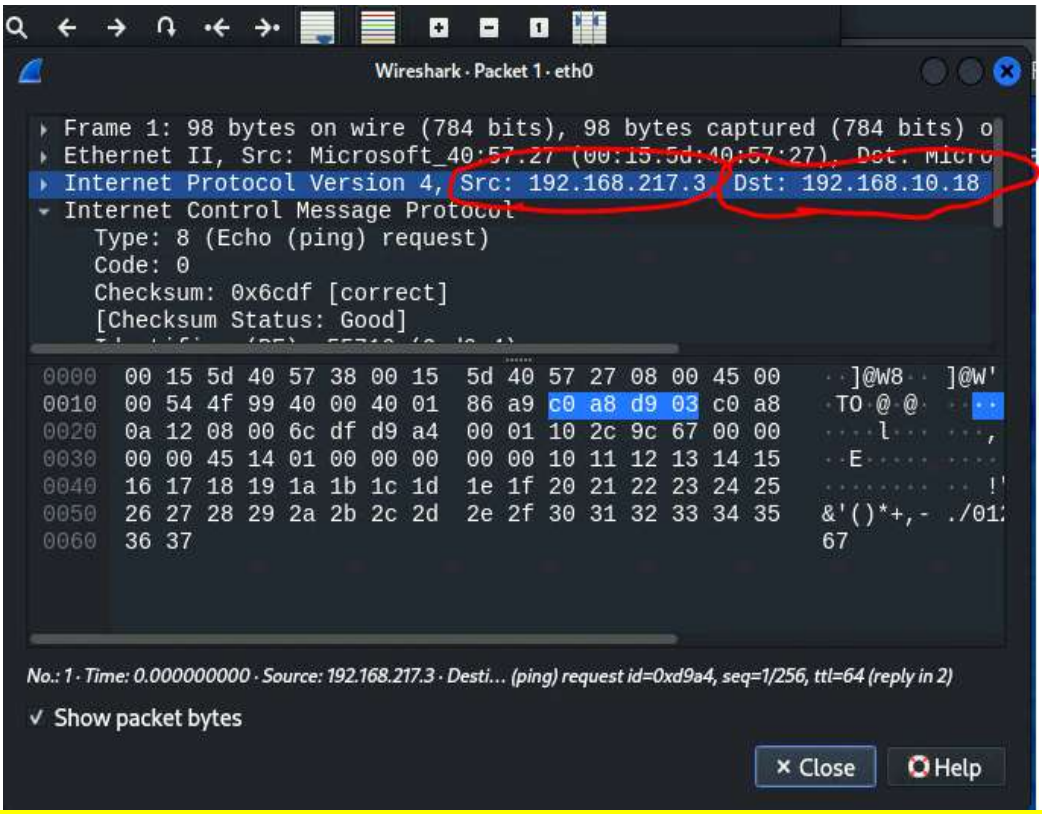
Q1. How many packets are captured in total? How many packets are displayed? There are a total of 82



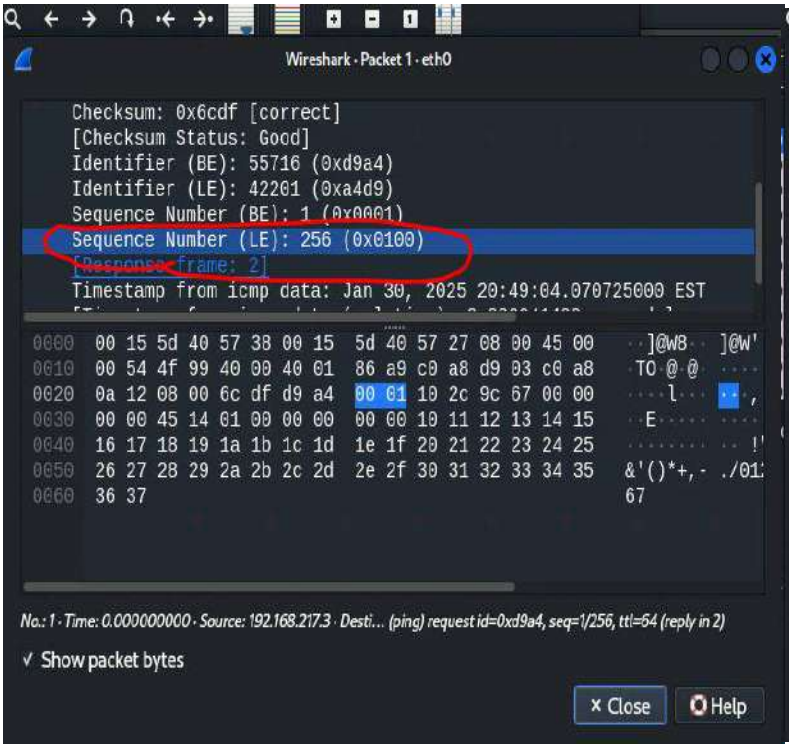
packets captured and displayed on the eth0 interface from the ping.

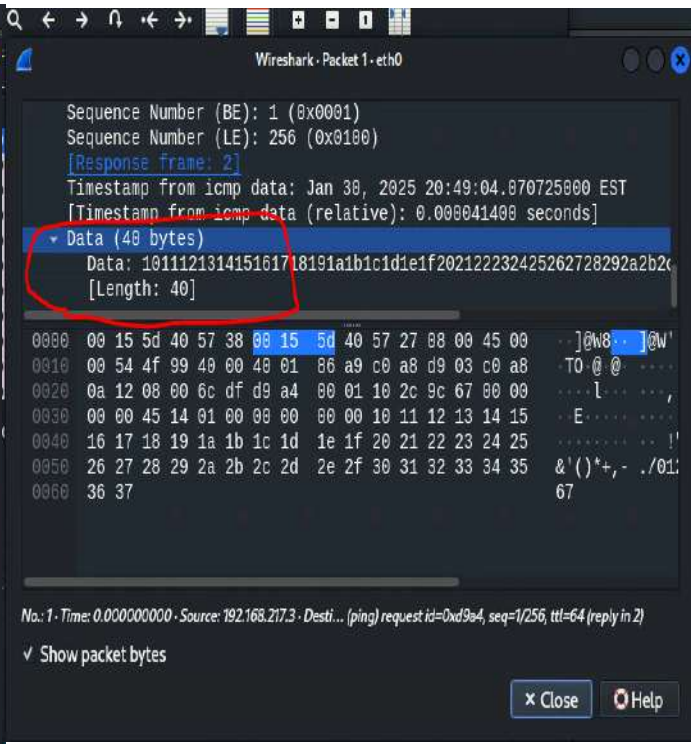


Q2: Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question. After applying the “ICMP” display filter on Wireshark. There are now 24 packets being displayed through the filter.



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

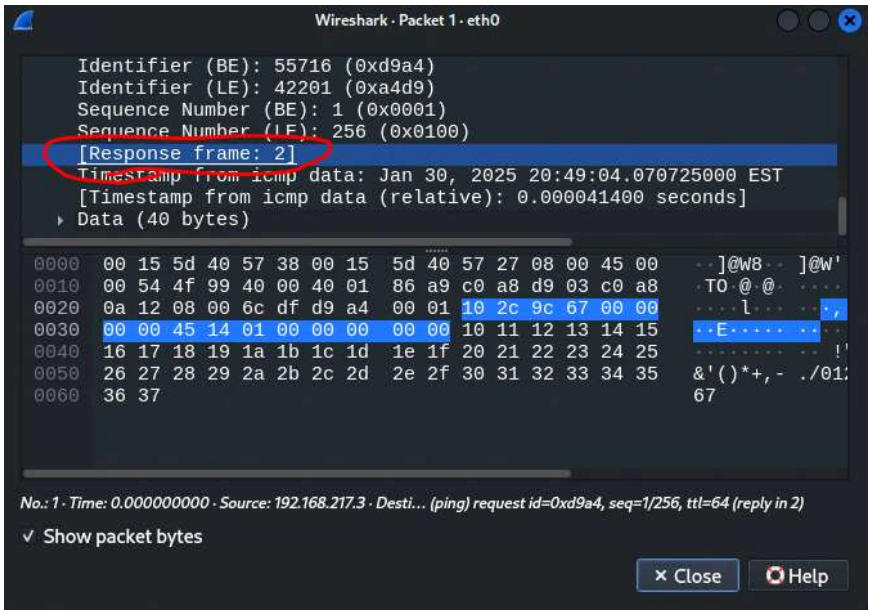




Packet 1 from the Echo message list. The source IP is 192.168.217.3 and the destination IP is 192.168.10.18.

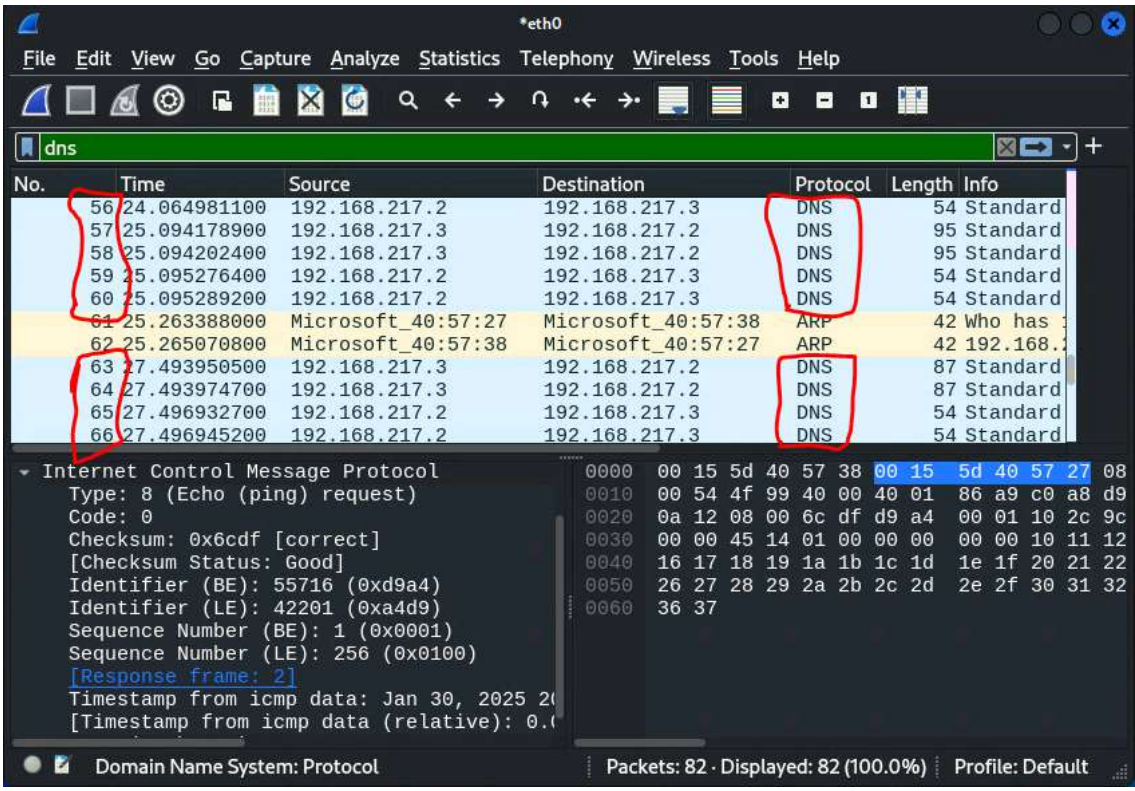
The left screenshot is the sequence number, and the right screenshot is the data size, which both can be found under the packet's information list.

Lastly, the screenshot to the right is the response time of the packet.



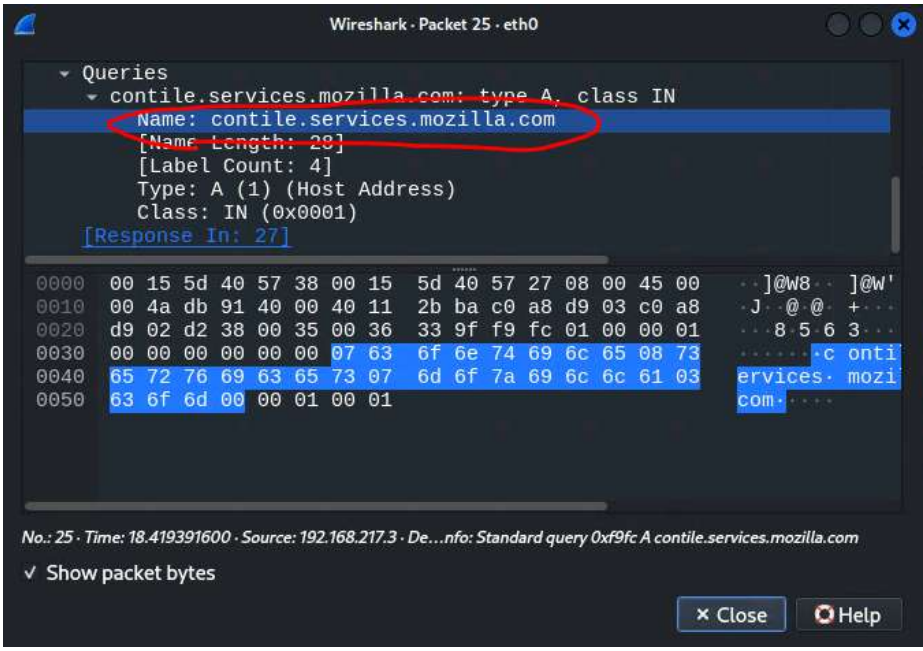
Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

After applying the “DNS” display filter on the packet list, some of the DNS packets are displayed in the screenshot above. The DNS packets on my list are numbers 25-60, and then 63-82. This means there are 56 DNS packets total.

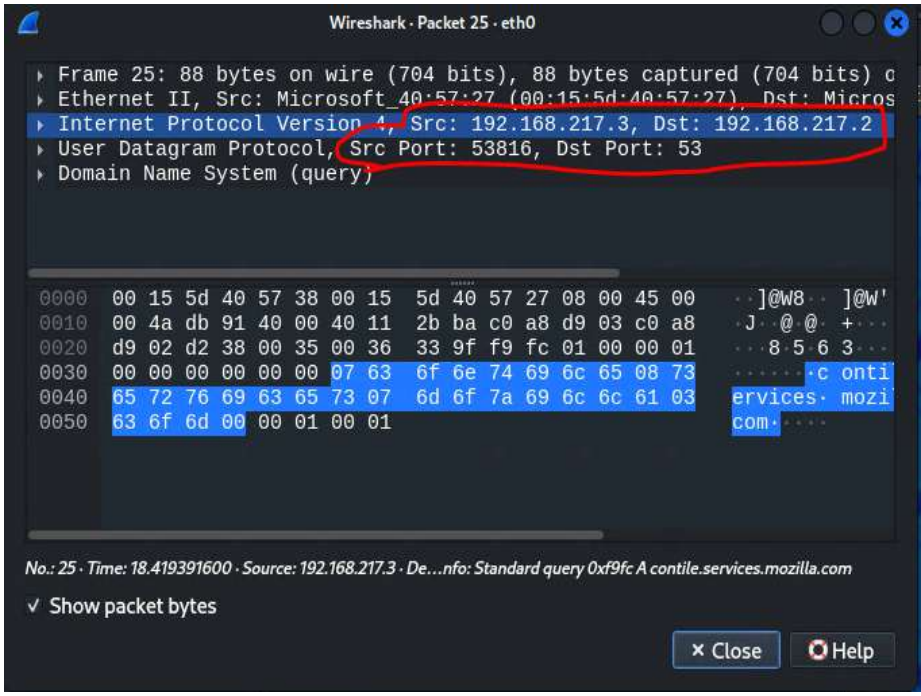


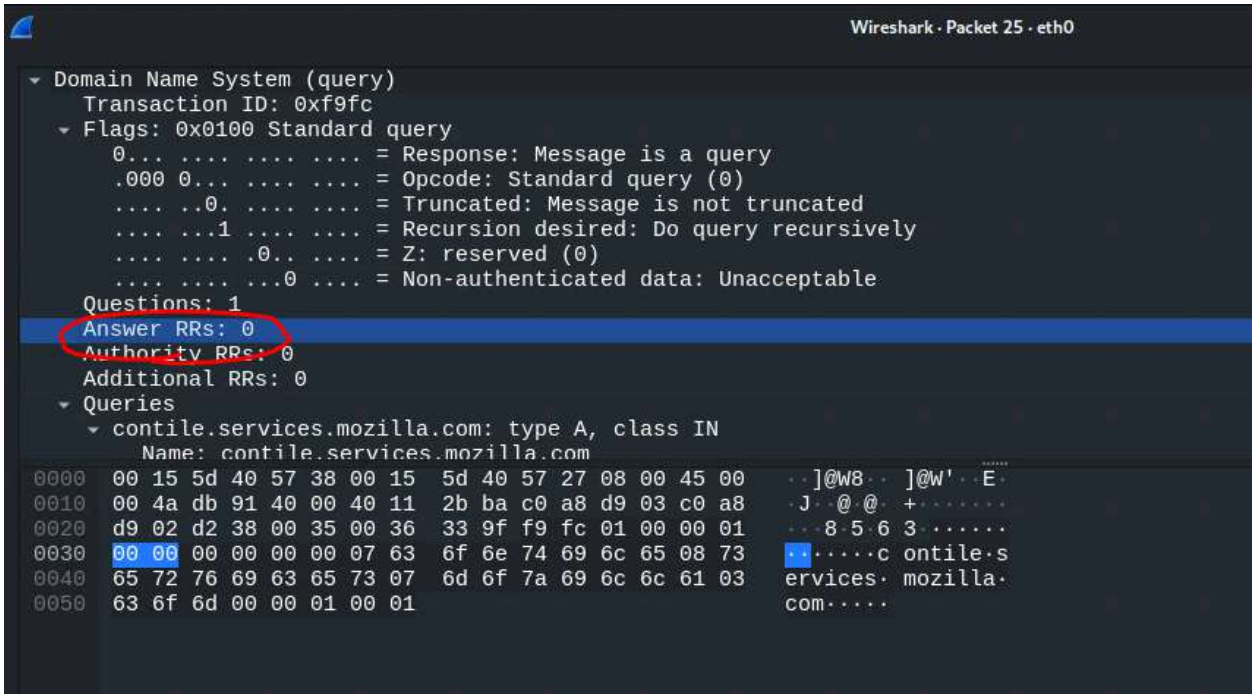
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

After opening a DNS query packet, the screenshot to the right is the domain name that the host is trying to resolve.



This screenshot to the right is the source IP address and the destination IP address. Just below that line are the corresponding port numbers. The IP:port format would be 192.168.217.3:53816 → 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? Source IP Address: 192.168.217.3

Port Number: 53816

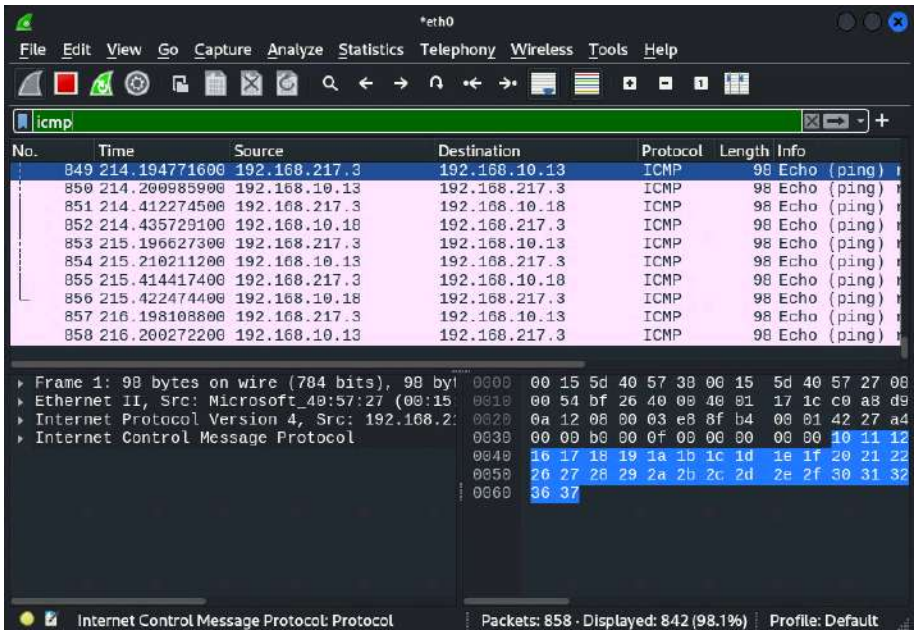
Destination IP Address: 192.168.217.2

Port Number: 53

There was no message replied from the DNS server for me per screenshot above.

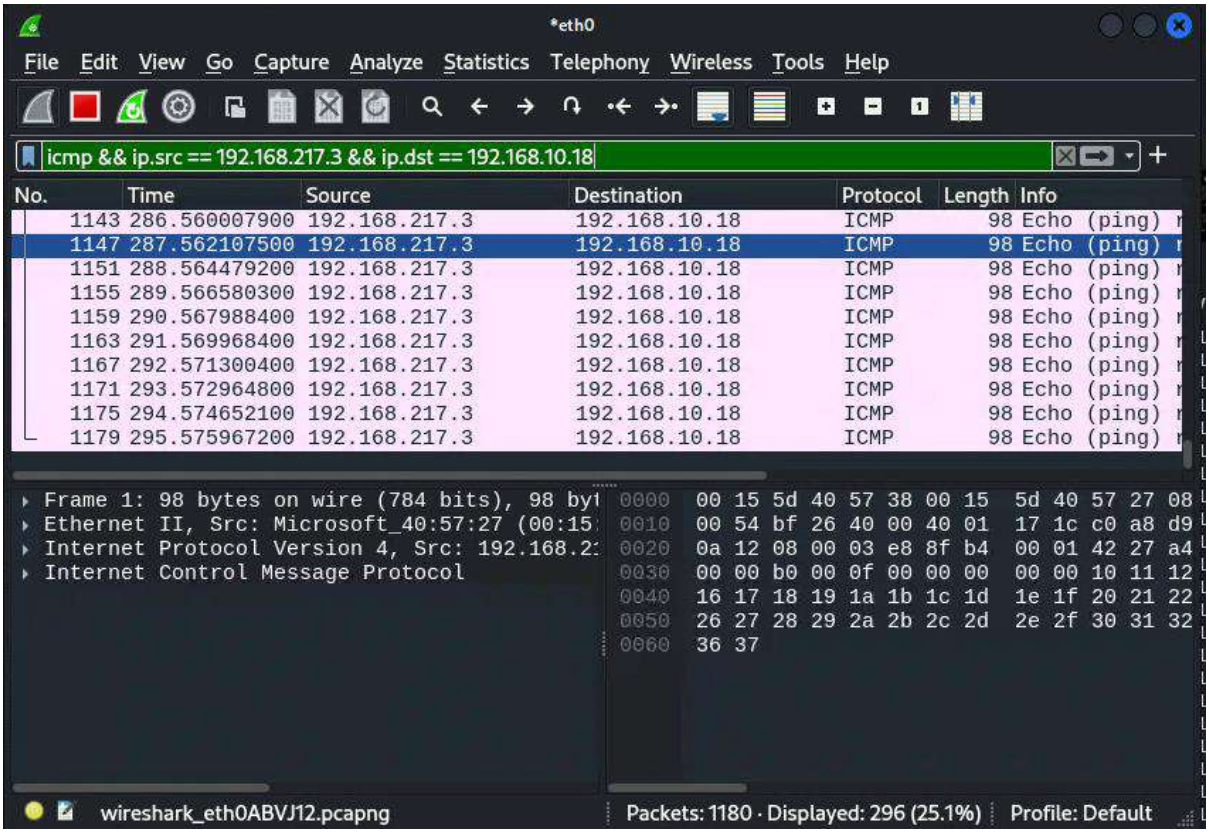
TASK B:

1. A.

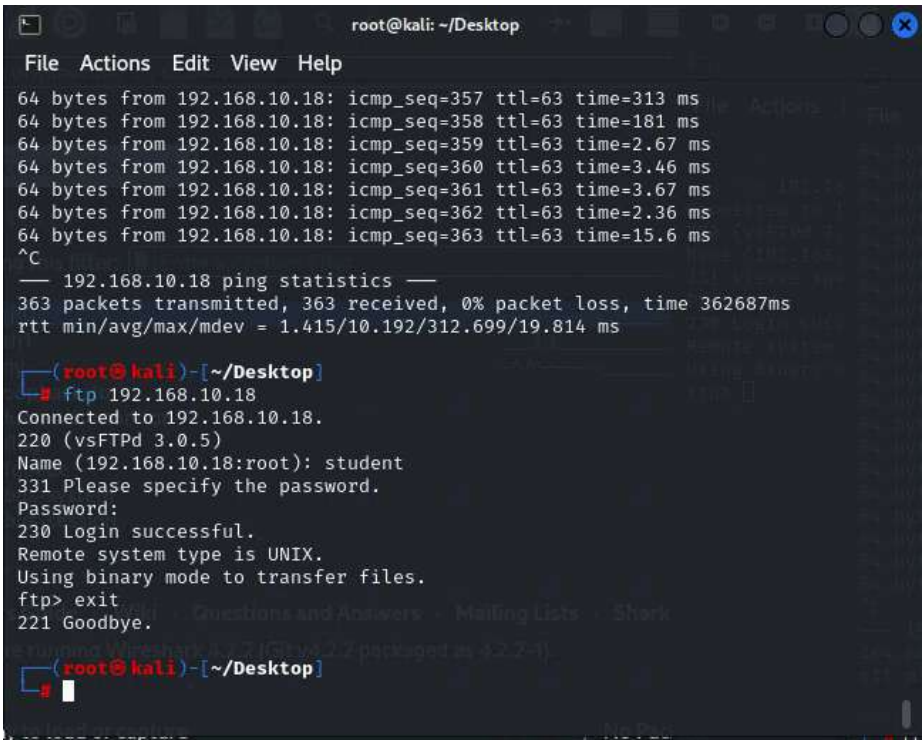


SNIFFING ICMP TRAFFIC

1. B.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp && ip.src == 192.168.217.3 && ip.dst == 192.168.10.18
No. Time Source Destination Protocol Length Info
1143 286.560007900 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1147 287.562107500 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1151 288.564479200 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1155 289.566580300 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1159 290.567988400 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1163 291.569968400 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1167 292.571300400 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1171 293.572964800 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1175 294.574652100 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
1179 295.575967200 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping)
Frame 1: 98 bytes on wire (784 bits), 98 byt
Ethernet II, Src: Microsoft_40:57:27 (00:15:
Internet Protocol Version 4, Src: 192.168.2:
Internet Control Message Protocol
0000 00 15 5d 40 57 38 00 15 5d 40 57 27 08
0010 00 54 bf 26 40 00 40 01 17 1c c0 a8 d9
0020 0a 12 08 00 03 e8 8f b4 00 01 42 27 a4
0030 00 00 b0 00 0f 00 00 00 00 00 10 11 12
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32
0060 36 37
wireshark_eth0ABVJ12.pcapng
Packets: 1180 · Displayed: 296 (25.1%)
Profile: Default

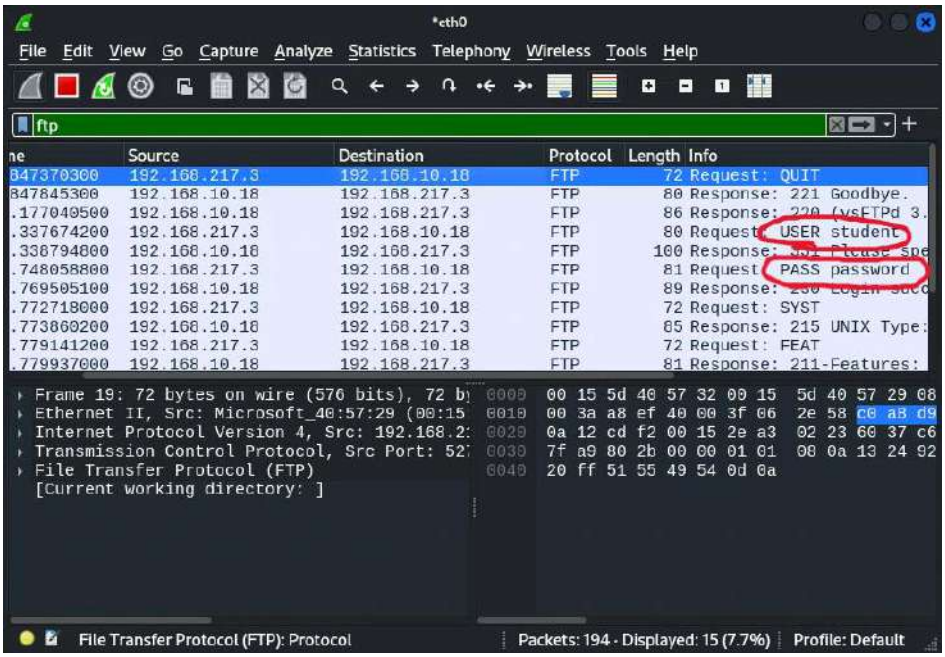
1. A.


root@kali: ~/Desktop
File Actions Edit View Help
64 bytes from 192.168.10.18: icmp_seq=357 ttl=63 time=313 ms
64 bytes from 192.168.10.18: icmp_seq=358 ttl=63 time=181 ms
64 bytes from 192.168.10.18: icmp_seq=359 ttl=63 time=2.67 ms
64 bytes from 192.168.10.18: icmp_seq=360 ttl=63 time=3.46 ms
64 bytes from 192.168.10.18: icmp_seq=361 ttl=63 time=3.67 ms
64 bytes from 192.168.10.18: icmp_seq=362 ttl=63 time=2.36 ms
64 bytes from 192.168.10.18: icmp_seq=363 ttl=63 time=15.6 ms
^C
— 192.168.10.18 ping statistics —
363 packets transmitted, 363 received, 0% packet loss, time 362687ms
rtt min/avg/max/mdev = 1.415/10.192/312.699/19.814 ms
(root@kali)-[~/Desktop]
ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
(root@kali)-[~/Desktop]
#

SNIFFING FTP TRAFFIC

2. B.

I found the password by utilizing the ftp Ubuntu IP command and finding the FTP packets after logging into the FTP server. The FTP packets with the USER student and PASS password was the info needed.



STEALING FILES WITH WIRESHARK

2. C.