

Assignment: Lab 2 – Traffic Tracing and Sniffing

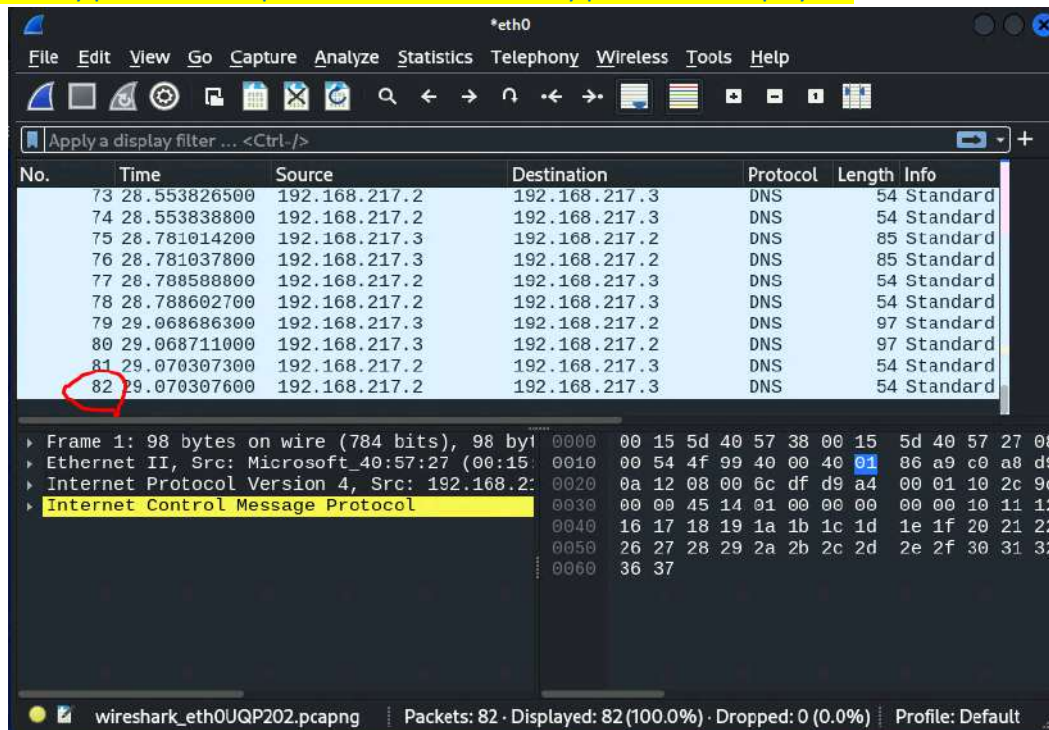
CYSE 301 – Professor Vatsa

Brandon Creech (UIN: 01215415)

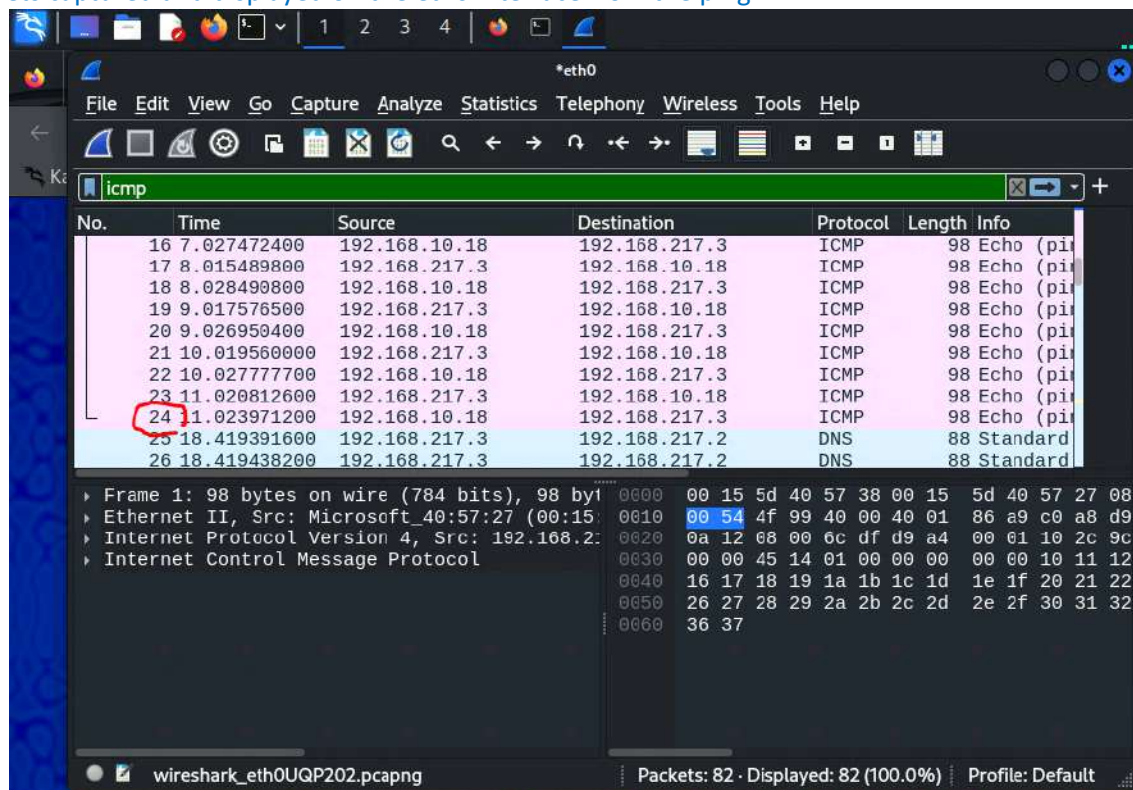
Old Dominion University

TASK A: Get Started with Wireshark

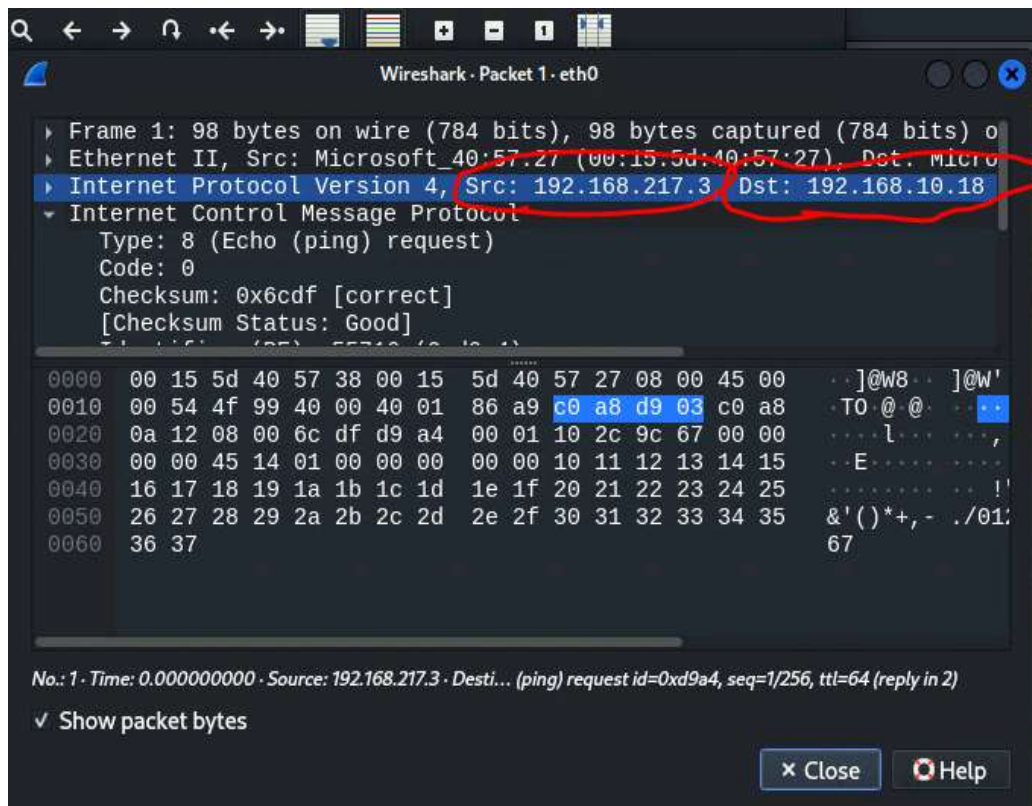
Q1. How many packets are captured in total? How many packets are displayed? There are a total of 82



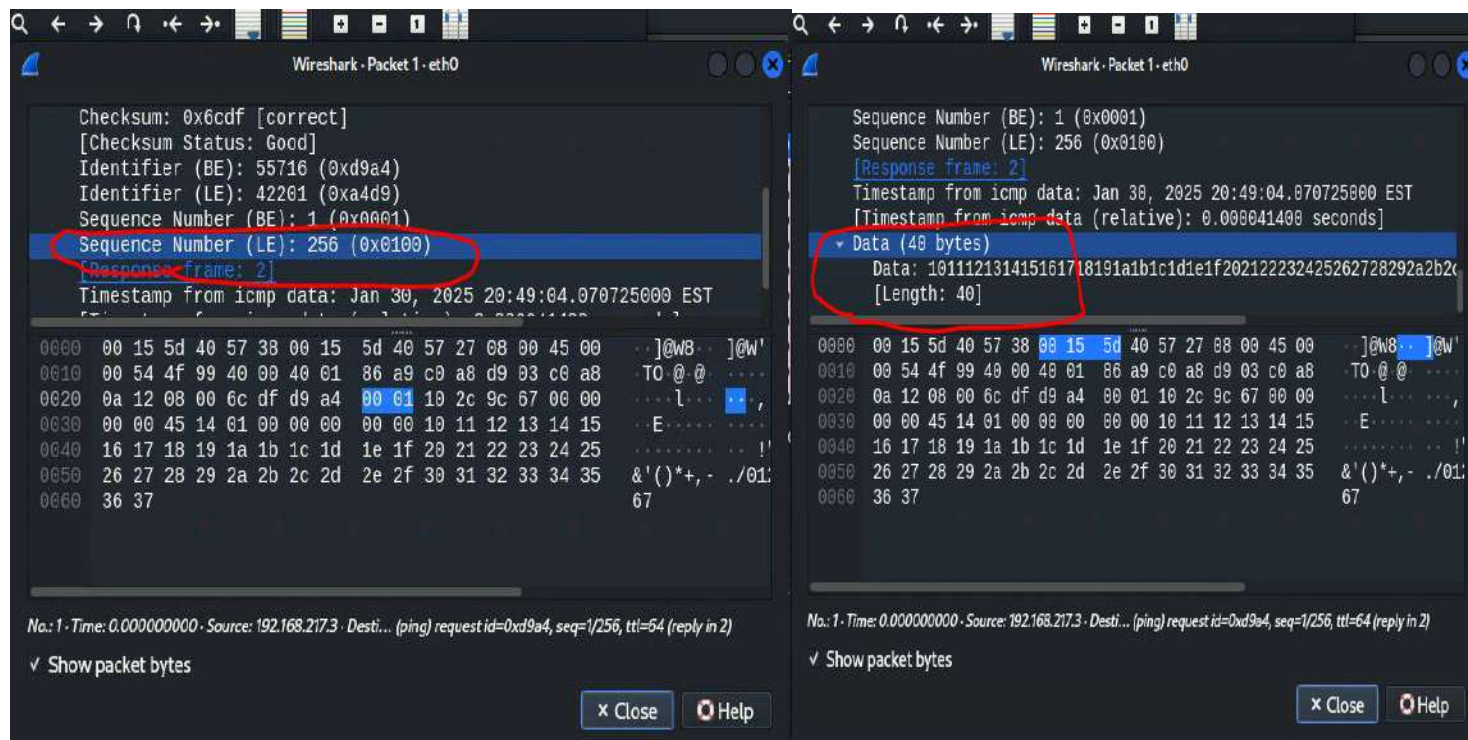
packets captured and displayed on the eth0 interface from the ping.



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.



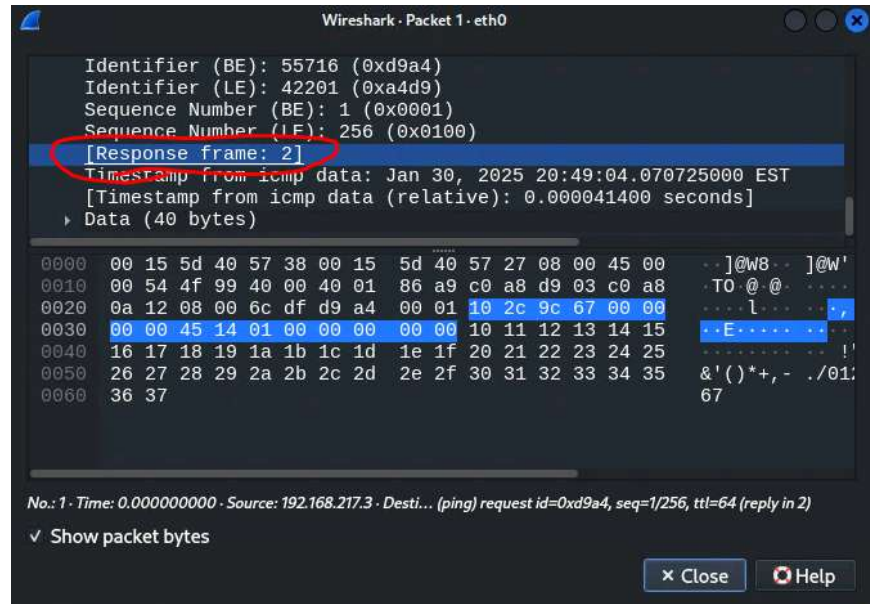
Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time? Above is



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

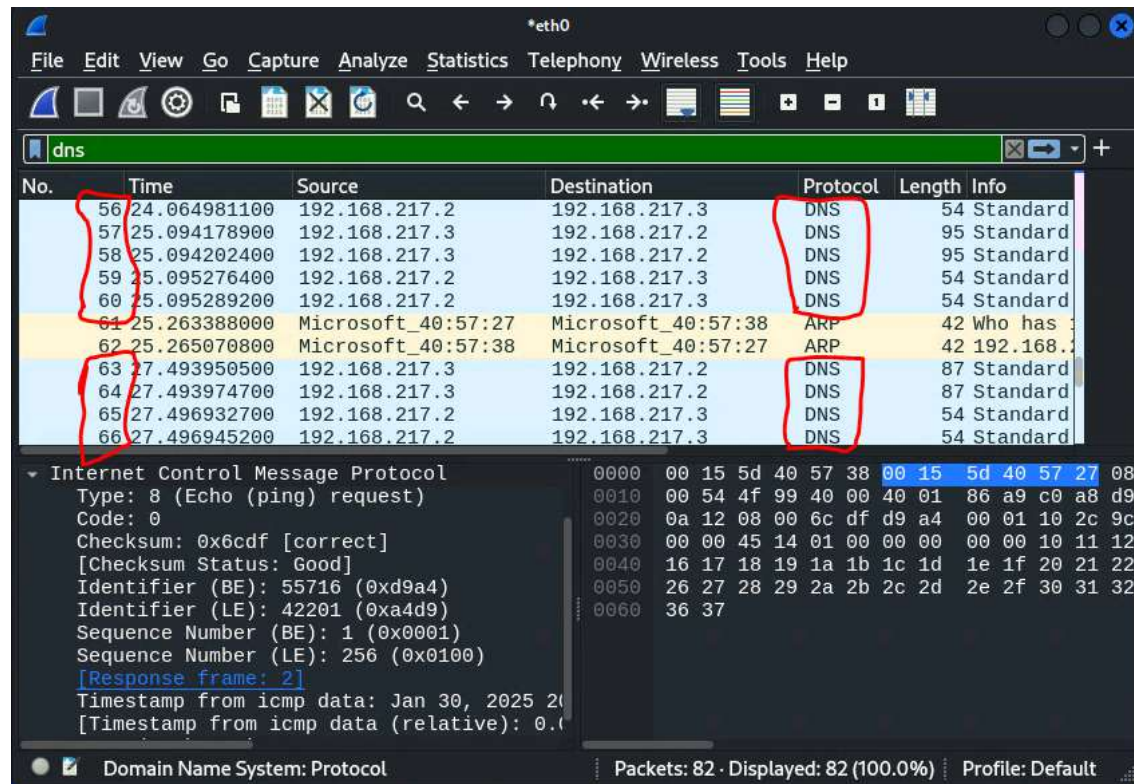
The left screenshot is the sequence number, and the right screenshot is the data size, which both can be found under the packet's information list.

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



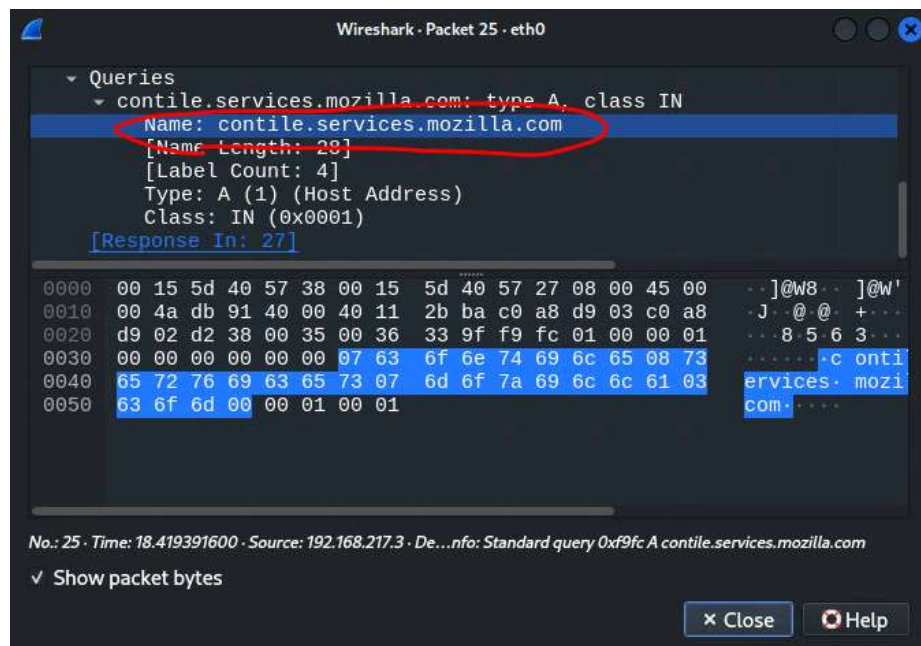
Q4. Apply "DNS" as a display filter in Wireshark. How many packets are displayed?

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.

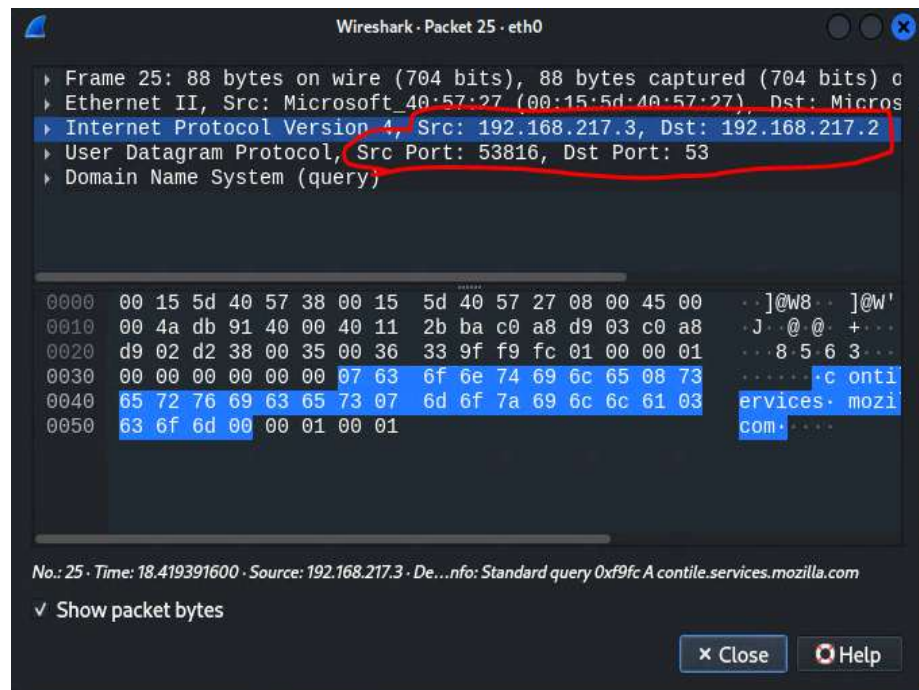


Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

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.



```
Wireshark · Packet 25 · eth0

▼ Domain Name System (query)
  Transaction ID: 0xf9fc
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ contile.services.mozilla.com: type A, class IN
      Name: contile.services.mozilla.com
0000  00 15 5d 40 57 38 00 15 5d 40 57 27 08 00 45 00  ..]@w8.. ]@w'..E.
0010  00 4a db 91 40 00 40 11 2b ba c0 a8 d9 03 c0 a8  .J..@.@. +.....
0020  d9 02 d2 38 00 35 00 36 33 9f f9 fc 01 00 00 01  ...8-5.6.3.....
0030  00 00 00 00 00 07 63 6f 6e 74 69 6c 65 08 73  .4.....c ontile.s
0040  65 72 76 69 63 65 73 07 6d 6f 7a 69 6c 6c 61 03  ervices. mozilla.
0050  63 6f 6d 00 00 01 00 01  com.....
```

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.

The image shows a Wireshark packet capture window titled "*eth0". The filter bar at the top is set to "icmp". The packet list on the left shows a series of ICMP Echo (ping) packets. The packet details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
849	214.194771600	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) t
850	214.200985900	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) t
851	214.412274500	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) t
852	214.435729100	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) t
853	215.196627300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) t
854	215.210211200	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) t
855	215.414417400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) t
856	215.422474400	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) t
857	216.198108800	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) t
858	216.200272200	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) t

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0
Ethernet II, Src: Microsoft_49:57:27 (08:15:57:00:15:57:27), Dst: 08:00:00:00:00:00
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.13
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

Internet Control Message Protocol: Protocol Packets: 858 · Displayed: 842 (98.1%) Profile: Default

SNIFFING
ICMP
TRAFFIC

1. B.

The image shows a Wireshark packet capture on the eth0 interface. The filter is set to `icmp && ip.src == 192.168.217.3 && ip.dst == 192.168.10.18`. The packet list shows several ICMP Echo (ping) requests. The packet details pane shows the structure of the first frame:

- Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0
- Ethernet II, Src: Microsoft_40:57:27 (00:15:57:00:00:00), Dst: 192.168.10.18 (08:00:20:0a:12:08)
- Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the first frame:

```
0000  00 15 5d 40 57 38 00 15 5d 40 57 27 08 00 00 00 00
0010  00 54 bf 26 40 00 40 01 17 1c c0 a8 d9 00 00 00 00
0020  0a 12 08 00 03 e8 8f b4 00 01 42 27 a4 00 00 00 00
0030  00 00 b0 00 0f 00 00 00 00 00 10 11 12 00 00 00 00
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36
0060  36 37
```

1. A.

The image shows a terminal window on a Kali Linux system. The user has run a series of ping commands to 192.168.10.18, showing the following results:

```
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
```

The user has then run `192.168.10.18 ping statistics`, which shows:

```
363 packets transmitted, 363 received, 0% packet loss, time 362687ms
rtt min/avg/max/mdev = 1.415/10.192/312.699/19.814 ms
```

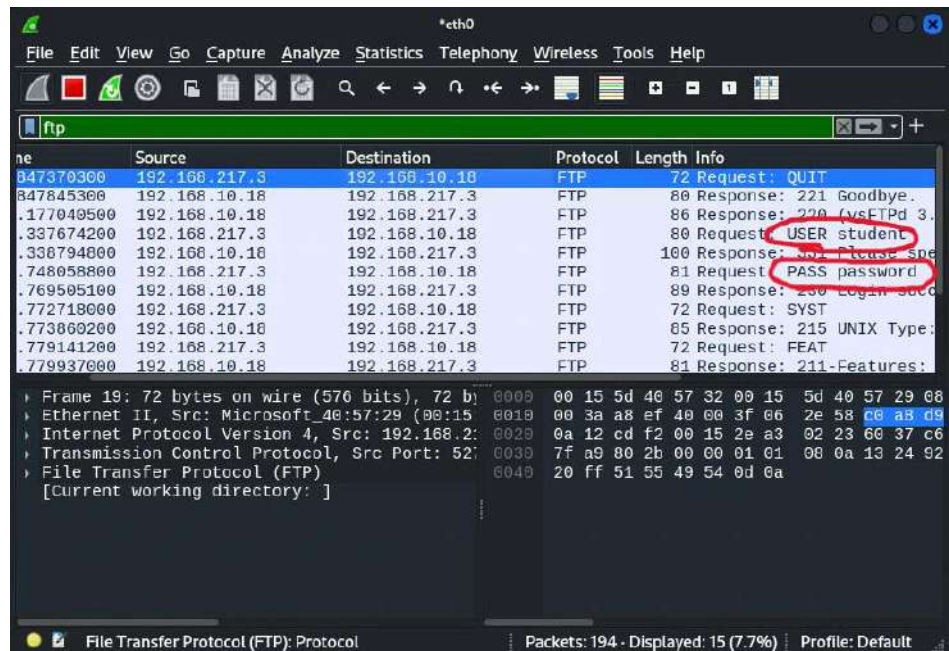
The user has then run `ftp 192.168.10.18`, which shows the following output:

```
(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.
```

2. B. 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.

```
root@kali: ~/Desktop
File Actions Edit View Help
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.

(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): brc26qv
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.

(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): brc26qv
331 Please specify the password.
Password:
012154530 Login incorrect.
ftp: Login failed
ftp> 
```

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

Source	Destination	Protocol	Length	Info
192.168.217.3	192.168.10.18	FTP	80	Request: USER brc26qv
192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify t
192.168.217.3	192.168.10.18	FTP	81	Request: PASS 01215415
192.168.10.18	192.168.217.3	FTP	88	Response: 530 Login incorrect.
192.168.217.3	192.168.10.18	FTP	72	Request: QUIT
192.168.10.18	192.168.217.3	FTP	80	Response: 221 Goodbye.
192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPD 3.0.5)
192.168.217.3	192.168.10.18	FTP	80	Request: USER brc26qv
192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify t
192.168.217.3	192.168.10.18	FTP	81	Request: PASS 01215415
192.168.10.18	192.168.217.3	FTP	88	Response: 530 Login incorrect.

Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0

Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: 192.168.10.18 (08:00:27:3c:1d:10)

Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18

Transmission Control Protocol, Src Port: 5681, Dst Port: 21

File Transfer Protocol (FTP)

[Current working directory:]

Frame (frame), 72 bytes

Packets: 40 · Displayed: 14 (35.0%) · Dropped: 0 (0.0%)

Profile: Default