

Task A

Question 1

246 Packets were captured

No.	Time	Source	Destination	Protocol	Length
235	55.474597000	192.168.217.2	192.168.217.3	DNS	
236	55.474606800	192.168.217.2	192.168.217.3	DNS	
237	64.901664000	192.168.217.3	192.168.10.18	ICMP	
238	64.905513500	192.168.10.18	192.168.217.3	ICMP	
239	65.903448100	192.168.217.3	192.168.10.18	ICMP	
240	65.910757700	192.168.10.18	192.168.217.3	ICMP	
241	66.904623200	192.168.217.3	192.168.10.18	ICMP	
242	66.908390200	192.168.10.18	192.168.217.3	ICMP	
243	67.910376900	192.168.217.3	192.168.10.18	ICMP	
244	67.913959400	192.168.10.18	192.168.217.3	ICMP	
245	68.911854200	192.168.217.3	192.168.10.18	ICMP	
246	68.939699600	192.168.10.18	192.168.217.3	ICMP	

Question 2.

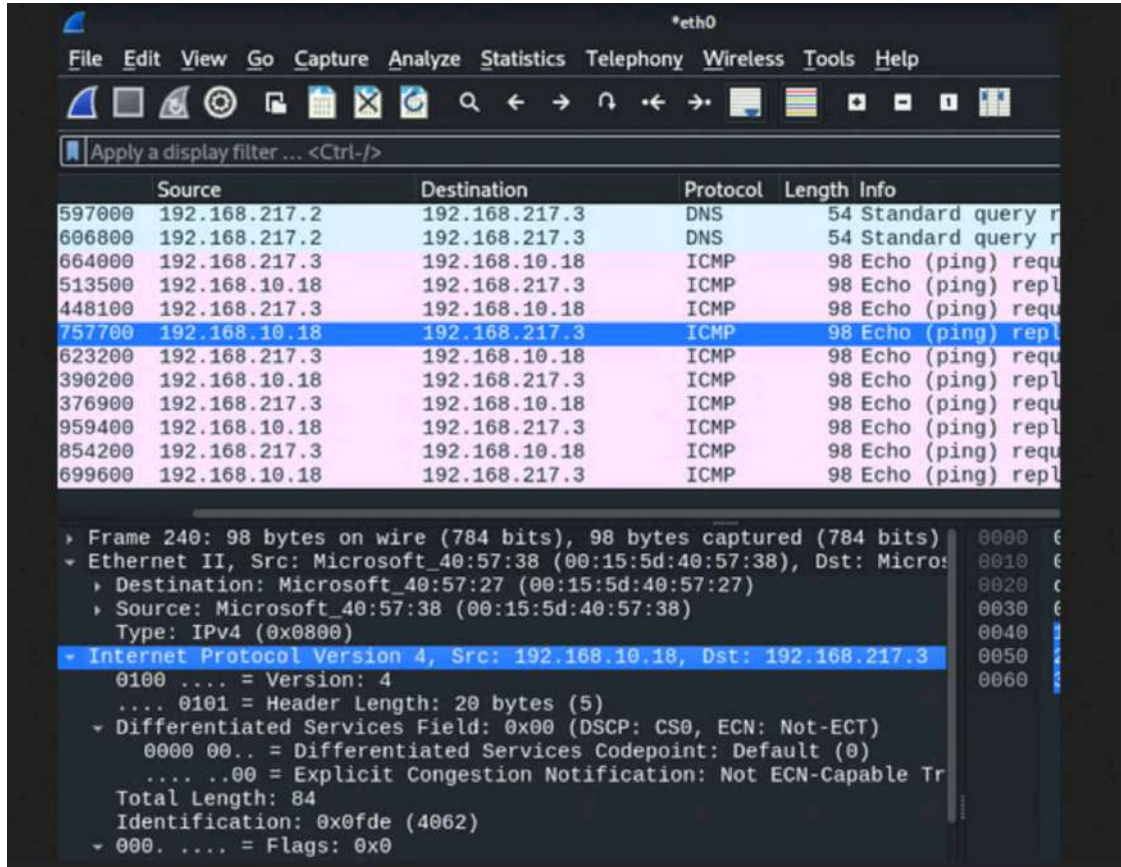
I used the ICMP filter below.

No.	Time	Source	Destination	Protocol	Length	Info
114	934.216375400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) r
115	934.229797300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) r
116	935.030006300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) r
117	935.030056000	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) r
118	935.217161300	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) r
119	935.220902000	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) r
120	936.037748700	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) r
121	936.037795500	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) r
122	937.051836600	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) r
123	937.051902900	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) r

Frame 70: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), 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

Question 3

The source IP is **192.168.10.18** and the destination IP is **192.168.217.3** as highlighted below.

**Question 4**

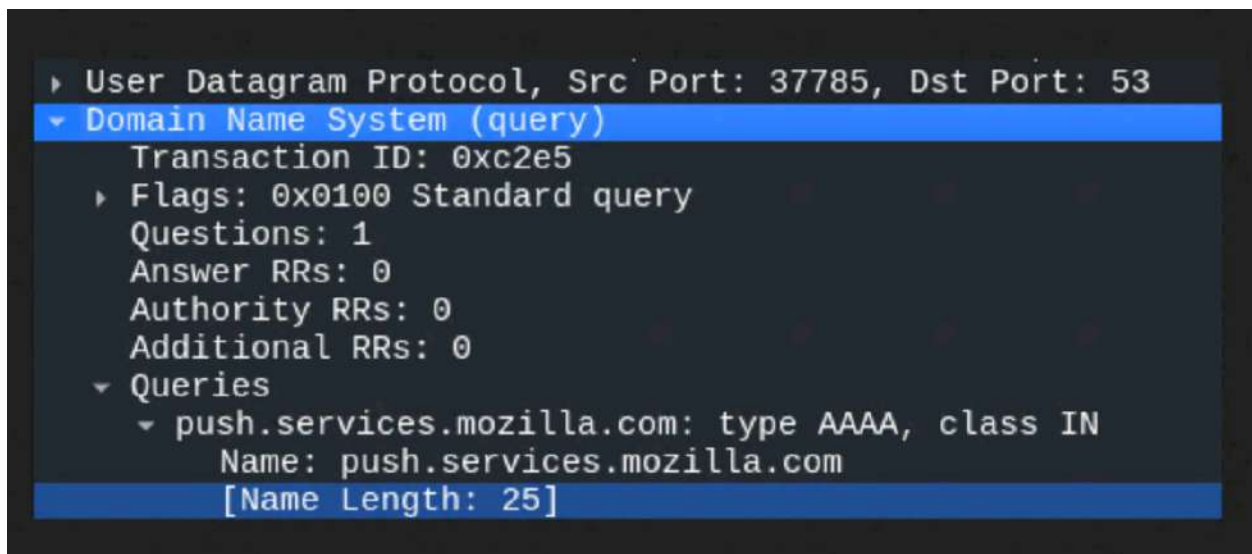
I used the DNS filter to view all of the DNS packets below. There were a total of 236 DNS packets.

No.	Time	Source	Destination	Protocol
224	50.162191100	192.168.217.2	192.168.217.3	DNS
225	50.445685700	192.168.217.3	192.168.217.2	DNS
226	50.445716900	192.168.217.3	192.168.217.2	DNS
227	50.449160500	192.168.217.2	192.168.217.3	DNS
228	50.449170600	192.168.217.2	192.168.217.3	DNS
229	55.156947200	192.168.217.3	192.168.217.2	DNS
230	55.156973200	192.168.217.3	192.168.217.2	DNS
231	55.159869600	192.168.217.2	192.168.217.3	DNS
232	55.159879900	192.168.217.2	192.168.217.3	DNS
233	55.457995200	192.168.217.3	192.168.217.2	DNS
234	55.458027600	192.168.217.3	192.168.217.2	DNS
235	55.474597000	192.168.217.2	192.168.217.3	DNS
236	55.474606800	192.168.217.2	192.168.217.3	DNS

Question 5.

The domain name the host is trying to resolve is mozilla.com.

The source IP is the IP of the VM at **192.168.217.3** and the source port is **37785**. The destination IP is **192.168.217.2** and the destination port is **53**. Since we are using a lab that doesn't have internet access the default network gateway is the destination IP.

**Question 6**

The DNS response was refused due to the inability to touch the internet. The Source IP is **192.168.217.2** and the source port is **53**. The Destination IP is **192.168.217.3** and the destination port is **50717**

pcap1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 0

No.	Time	Source	Destination	Protocol
1	0.000000000	192.168.217.3	192.168.217.2	DNS
2	0.000028200	192.168.217.3	192.168.217.2	DNS
3	0.002538700	192.168.217.2	192.168.217.3	DNS
4	0.002548200	192.168.217.2	192.168.217.3	DNS
25	5.003341900	192.168.217.3	192.168.217.2	DNS
26	5.003382800	192.168.217.3	192.168.217.2	DNS
27	5.004915400	192.168.217.2	192.168.217.3	DNS
28	5.004923600	192.168.217.2	192.168.217.3	DNS

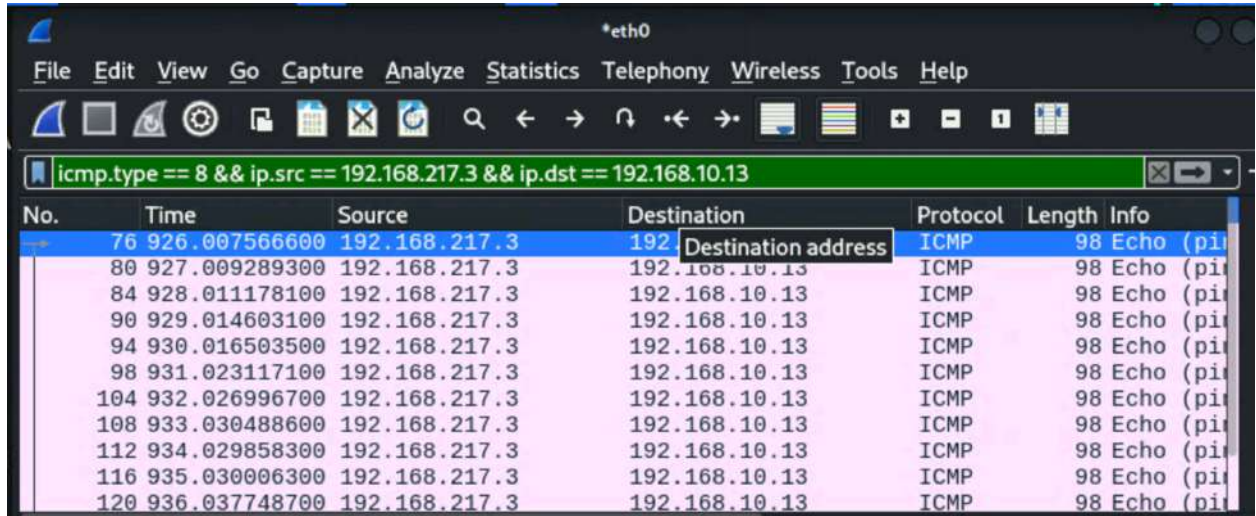
Frame 27: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on
Ethernet II, Src: Microsoft_40:57:38 (00:15:5d:40:57:38), Dst: Micros
Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
User Datagram Protocol, Src Port: 53, Dst Port: 50717
Domain Name System (response)
Transaction ID: 0x0366
Flags: 0x8105 Standard query response, Refused
Questions: 0
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
[\[Request In: 25\]](#)
[Time: 0.001573500 seconds]

Activate

Task B

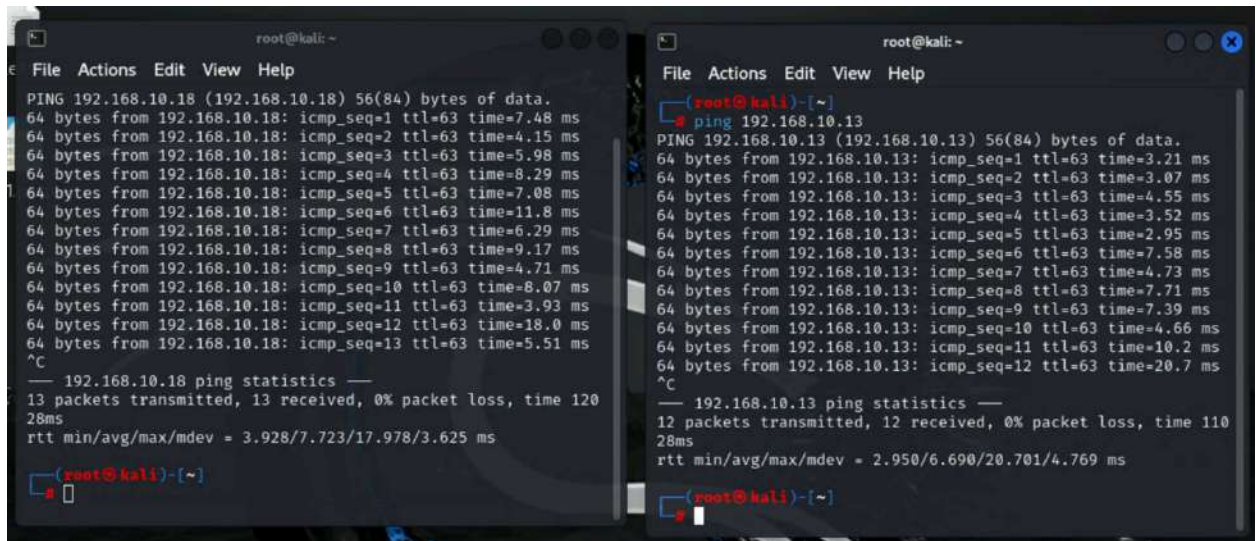
Question 1

- A. I launched wireshark as instructed from the Internal Kali VM



No.	Time	Source	Destination	Protocol	Length	Info
76	926.007566600	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
80	927.009289300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
84	928.011178100	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
90	929.014603100	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
94	930.016503500	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
98	931.023117100	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
104	932.026996700	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
108	933.030488600	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
112	934.029858300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
116	935.030006300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
120	936.037748700	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request

- B. I opened two CLI terminals and pinged both vm's for a few seconds.

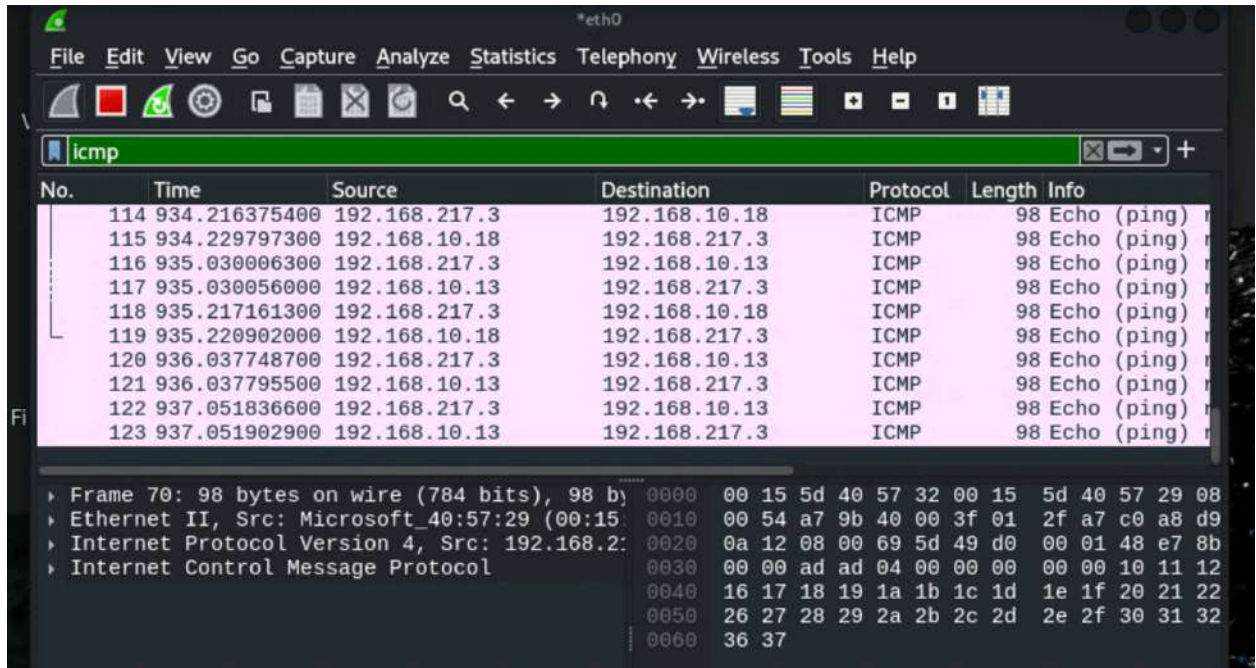


```

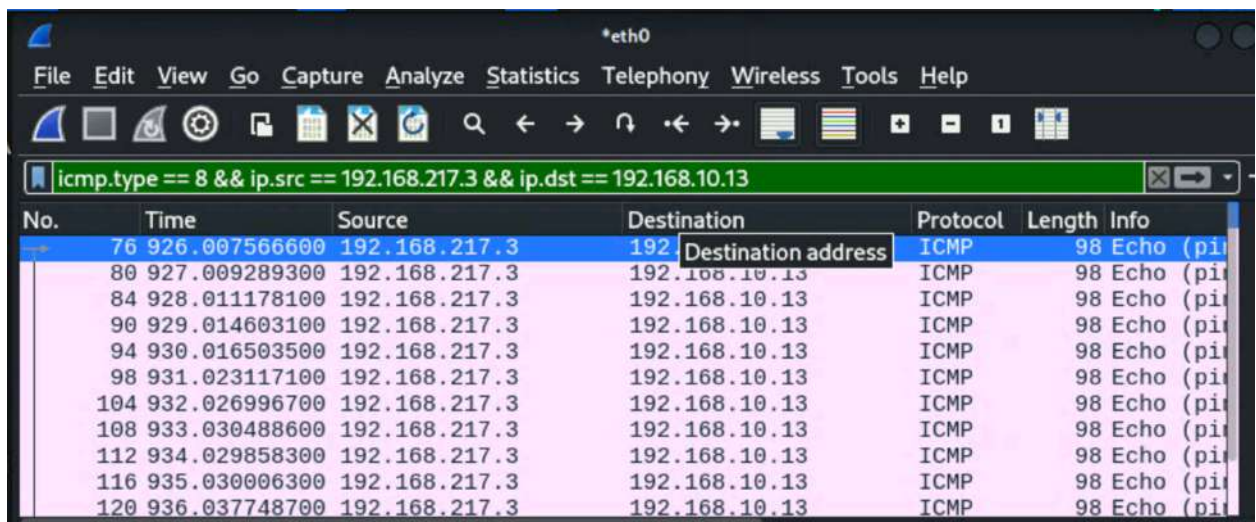
root@kali: ~
File Actions Edit View Help
PING 192.168.10.18 (192.168.10.18) 56(84) bytes of data:
64 bytes from 192.168.10.18: icmp_seq=1 ttl=63 time=7.48 ms
64 bytes from 192.168.10.18: icmp_seq=2 ttl=63 time=4.15 ms
64 bytes from 192.168.10.18: icmp_seq=3 ttl=63 time=5.98 ms
64 bytes from 192.168.10.18: icmp_seq=4 ttl=63 time=8.29 ms
64 bytes from 192.168.10.18: icmp_seq=5 ttl=63 time=7.08 ms
64 bytes from 192.168.10.18: icmp_seq=6 ttl=63 time=11.8 ms
64 bytes from 192.168.10.18: icmp_seq=7 ttl=63 time=6.29 ms
64 bytes from 192.168.10.18: icmp_seq=8 ttl=63 time=9.17 ms
64 bytes from 192.168.10.18: icmp_seq=9 ttl=63 time=4.71 ms
64 bytes from 192.168.10.18: icmp_seq=10 ttl=63 time=8.07 ms
64 bytes from 192.168.10.18: icmp_seq=11 ttl=63 time=3.93 ms
64 bytes from 192.168.10.18: icmp_seq=12 ttl=63 time=18.0 ms
64 bytes from 192.168.10.18: icmp_seq=13 ttl=63 time=5.51 ms
^C
  -- 192.168.10.18 ping statistics --
  13 packets transmitted, 13 received, 0% packet loss, time 120
 28ms
 rtt min/avg/max/mdev = 3.928/7.723/17.978/3.625 ms

root@kali: ~
File Actions Edit View Help
(root@kali)~# ping 192.168.10.13
PING 192.168.10.13 (192.168.10.13) 56(84) bytes of data:
64 bytes from 192.168.10.13: icmp_seq=1 ttl=63 time=3.21 ms
64 bytes from 192.168.10.13: icmp_seq=2 ttl=63 time=3.07 ms
64 bytes from 192.168.10.13: icmp_seq=3 ttl=63 time=4.55 ms
64 bytes from 192.168.10.13: icmp_seq=4 ttl=63 time=3.52 ms
64 bytes from 192.168.10.13: icmp_seq=5 ttl=63 time=2.95 ms
64 bytes from 192.168.10.13: icmp_seq=6 ttl=63 time=7.58 ms
64 bytes from 192.168.10.13: icmp_seq=7 ttl=63 time=4.73 ms
64 bytes from 192.168.10.13: icmp_seq=8 ttl=63 time=7.71 ms
64 bytes from 192.168.10.13: icmp_seq=9 ttl=63 time=7.39 ms
64 bytes from 192.168.10.13: icmp_seq=10 ttl=63 time=4.66 ms
64 bytes from 192.168.10.13: icmp_seq=11 ttl=63 time=10.2 ms
64 bytes from 192.168.10.13: icmp_seq=12 ttl=63 time=20.7 ms
^C
  -- 192.168.10.13 ping statistics --
  12 packets transmitted, 12 received, 0% packet loss, time 110
 28ms
 rtt min/avg/max/mdev = 2.950/6.690/20.701/4.769 ms
  
```

C. I applied the ICMP packet filter.

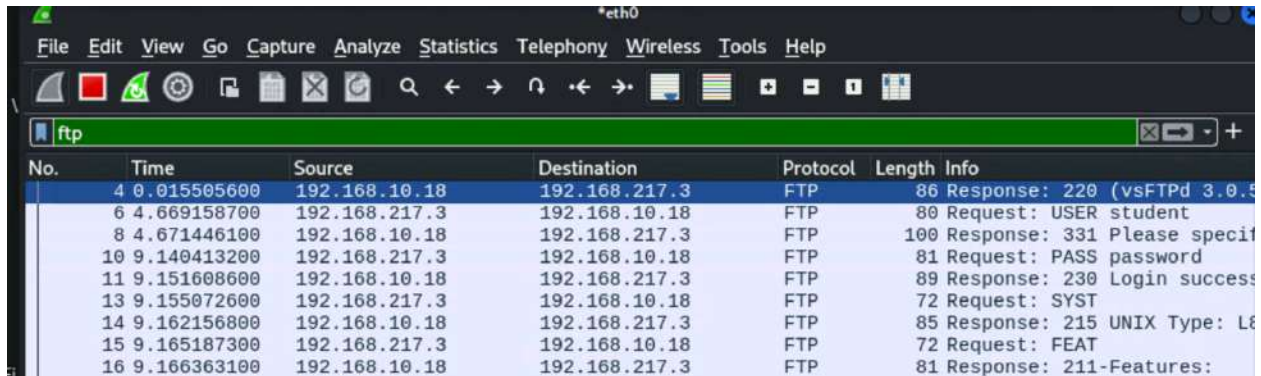


D. I applied a filter that listed ICMP packets with the specifications of the exact source and IP destination with the ip.dst syntax.



Question 2

A. From the CLI I executed `ftp 192.168.10.13` to login to the FTP server. I captured packets while I logged in. I utilized the FTP filter to see the plain text in Wireshark

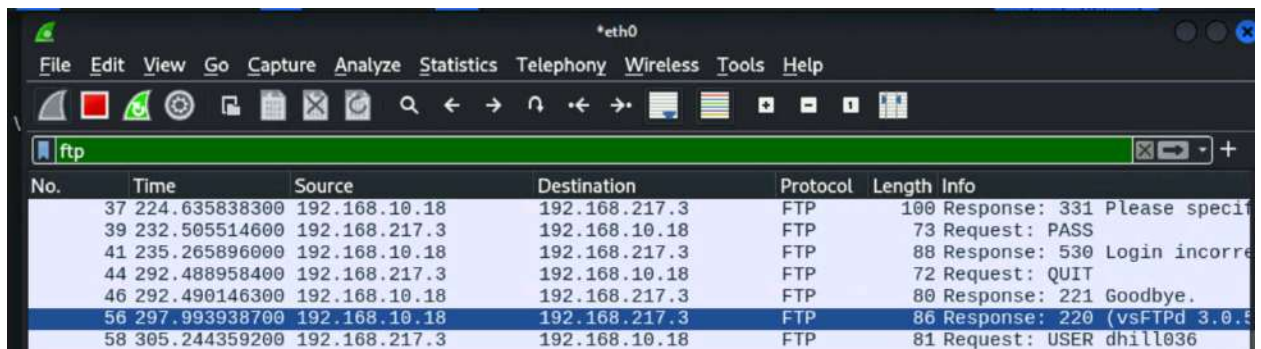


The image shows a Wireshark packet capture window with the filter 'ftp' applied. The packet list shows 16 packets. The first packet is a response from 192.168.10.18 to 192.168.217.3. Subsequent packets show requests for user, password, and system type, followed by responses indicating successful login.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.015505600	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPd 3.0.5)
6	4.669158700	192.168.217.3	192.168.10.18	FTP	80	Request: USER student
8	4.671446100	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify
10	9.140413200	192.168.217.3	192.168.10.18	FTP	81	Request: PASS password
11	9.151608600	192.168.10.18	192.168.217.3	FTP	89	Response: 230 Login success
13	9.155072600	192.168.217.3	192.168.10.18	FTP	72	Request: SYST
14	9.162156800	192.168.10.18	192.168.217.3	FTP	85	Response: 215 UNIX Type: L8
15	9.165187300	192.168.217.3	192.168.10.18	FTP	72	Request: FEAT
16	9.166363100	192.168.10.18	192.168.217.3	FTP	81	Response: 211-Features:

B After utilizing the FTP filter as you can see to the right the input from the VM has been captured and it can be read because it is in plain text. FTP is a non-encrypted protocol so anything passed between two systems on this port the traffic can be sniffed.

C. I repeated the steps again but with my MIDAS ID and through Wireshark you can see that there is a login error. In the image below you can see the request for the user and the source and where I typed in my username. You can also see the failed password attempt but since that password is my live MIDAS ID I intentionally left it out of the image.



The image shows a Wireshark packet capture window with the filter 'ftp' applied. The packet list shows 8 packets. The first packet is a response from 192.168.10.18 to 192.168.217.3. Subsequent packets show requests for user, password, and system type, followed by responses indicating login failure and a goodbye message.

No.	Time	Source	Destination	Protocol	Length	Info
37	224.635838300	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please specify
39	232.505514600	192.168.217.3	192.168.10.18	FTP	73	Request: PASS
41	235.265896000	192.168.10.18	192.168.217.3	FTP	88	Response: 530 Login incorre
44	292.488958400	192.168.217.3	192.168.10.18	FTP	72	Request: QUIT
46	292.490146300	192.168.10.18	192.168.217.3	FTP	80	Response: 221 Goodbye.
56	297.993938700	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPd 3.0.5)
58	305.244359200	192.168.217.3	192.168.10.18	FTP	81	Request: USER dhill036