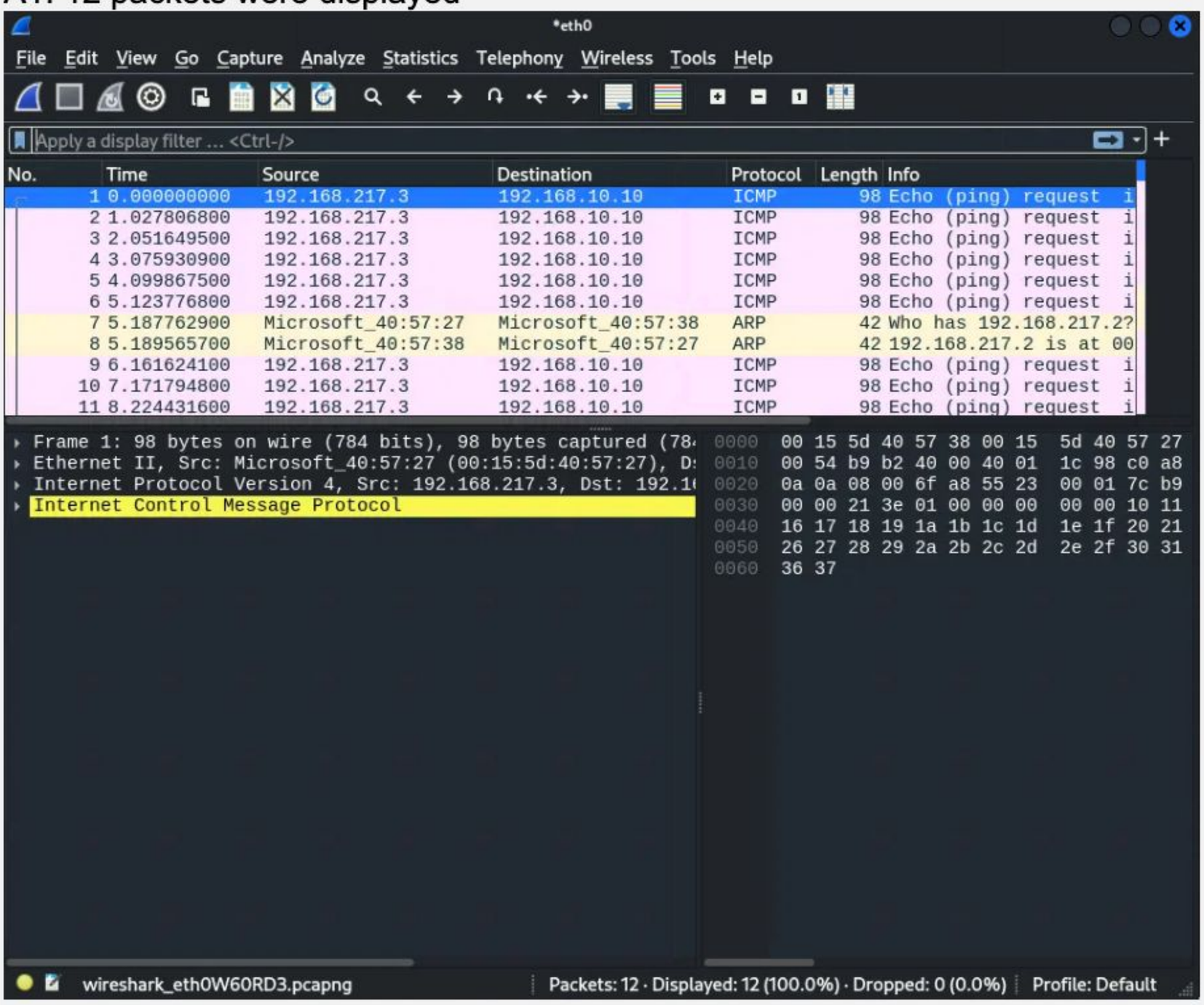
Q1

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

A1: 12 packets were displayed

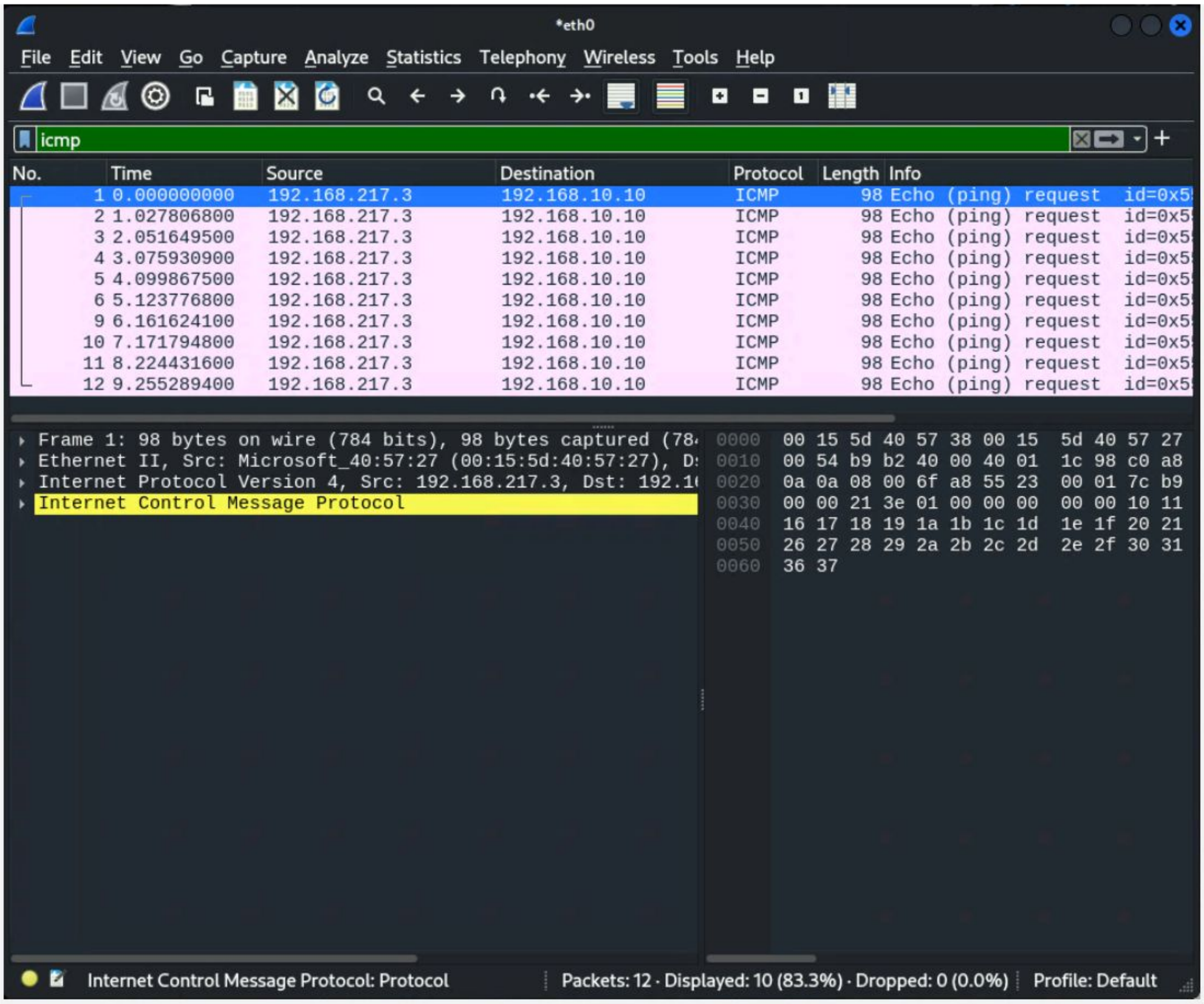


Q2

. Apply “ICMP” as a display filter in Wiresharkicmp

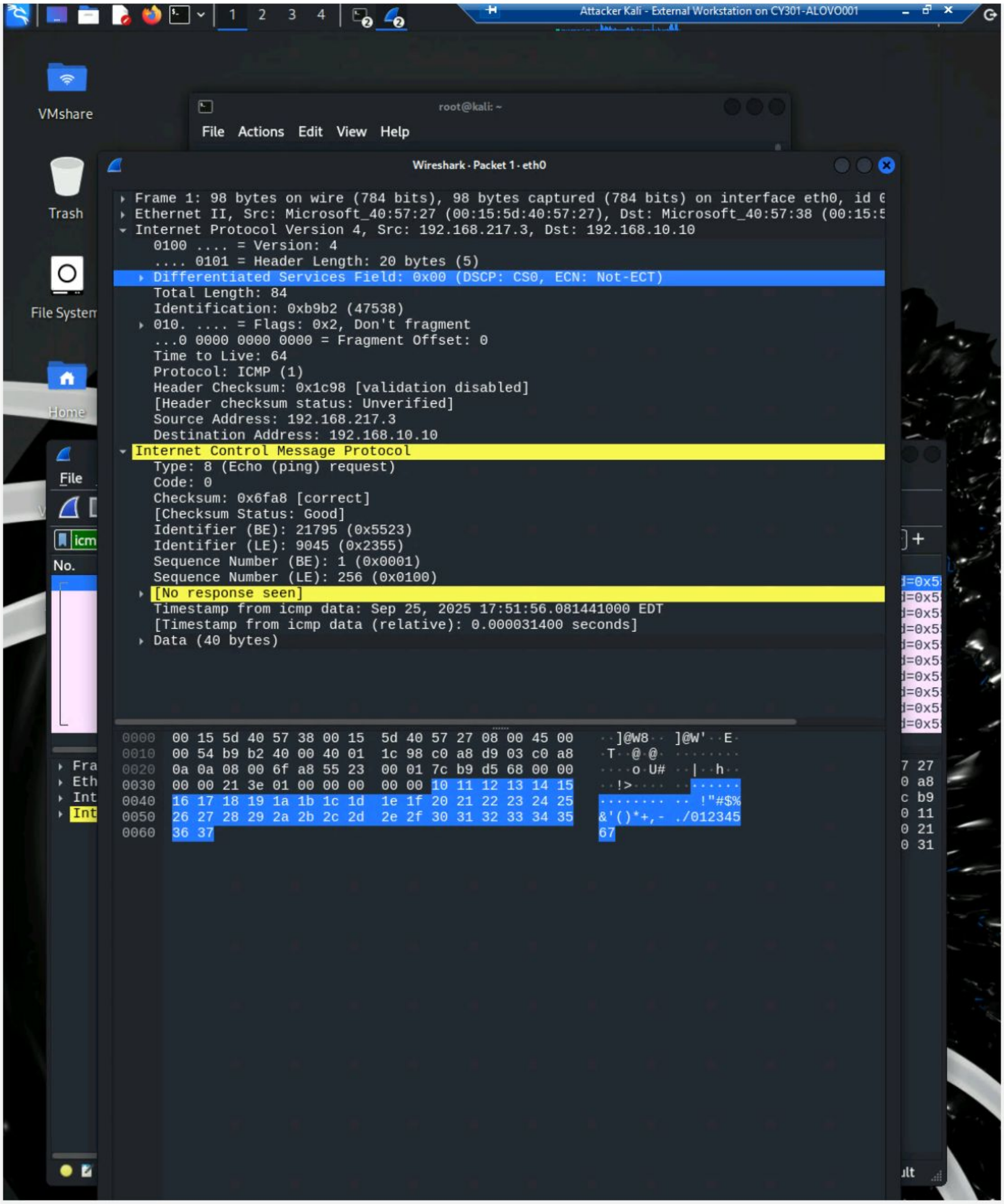
. Then repeat the previous question (Q1).

Answer 2: 12 packets were captured and 10 were displayed



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?

Source Address: 192.168.217.3
Destination Address: 192.168.10.10
Sequence Number (BE): 1 (0x0001)
Data Size: 40 bytes
Response time: No Response seen

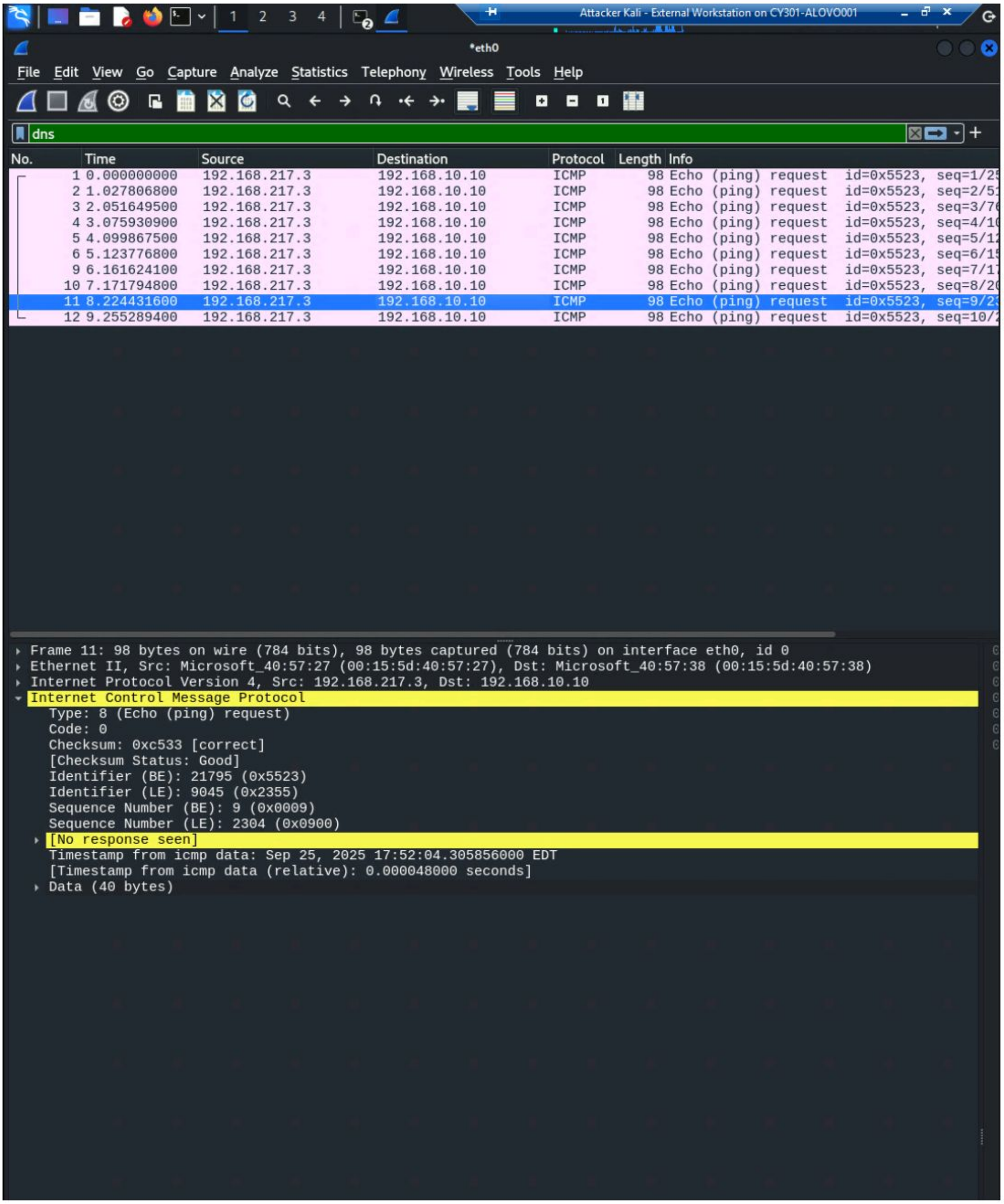

Attacker Kali - External Workstation on CY301-ALOVO001
1 2 3 4
VMshare
Trash
File System
Home
root@kali: ~
File Actions Edit View Help
Wireshark · Packet 1 · eth0
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: Microsoft_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft_40:57:38 (00:15:5
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xb9b2 (47538)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x1c98 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.217.3
Destination Address: 192.168.10.10
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x6fa8 [correct]
[Checksum Status: Good]
Identifier (BE): 21795 (0x5523)
Identifier (LE): 9045 (0x2355)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[No response seen]
Timestamp from icmp data: Sep 25, 2025 17:51:56.081441000 EDT
[Timestamp from icmp data (relative): 0.000031400 seconds]
Data (40 bytes)
0000 00 15 5d 40 57 38 00 15 5d 40 57 27 08 00 45 00 ..]@W8..]@W'..E.
0010 00 54 b9 b2 40 00 40 01 1c 98 c0 a8 d9 03 c0 a8 .T..@.@. ....
0020 0a 0a 08 00 6f a8 55 23 00 01 7c b9 d5 68 00 00 ....o.U# ..|..h..
0030 00 00 21 3e 01 00 00 00 00 00 10 11 12 13 14 15 ..!>.... ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .... !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67
File
icm
No.

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

Q5.
Find a DNS query
.
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 for
IP:port

Q
6.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 fr
DNS server?

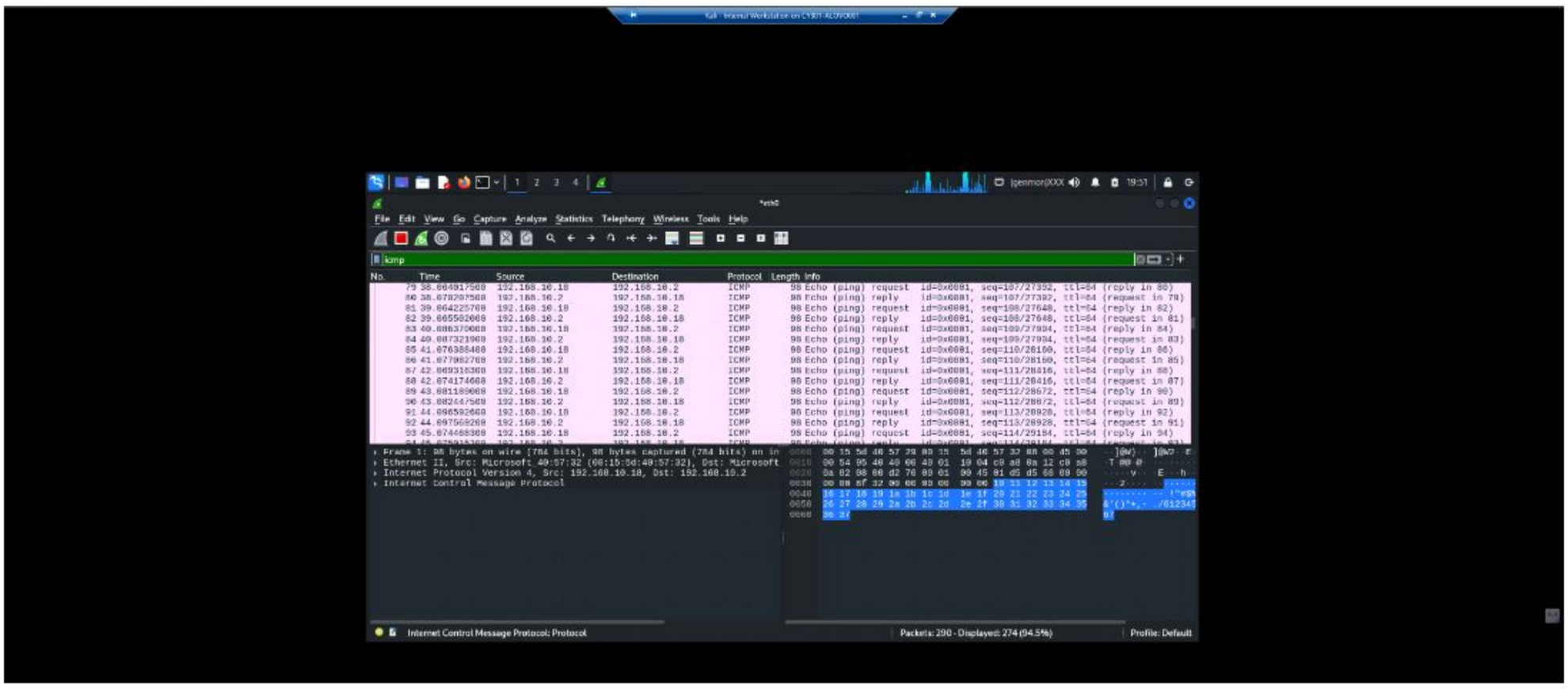
Answer: For Q5 and Q6 not DNS could not be filled because no DNS queries could be generated and i tried external domains and i got server unreachable


Attacker Kali - External Workstation on CY301-ALOVO001
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=1/25
2 1.027806800 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=2/51
3 2.051649500 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=3/76
4 3.075930900 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=4/10
5 4.099867500 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=5/12
6 5.123776800 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=6/15
9 6.161624100 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=7/17
10 7.171794800 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=8/20
11 8.224431600 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=9/23
12 9.255289400 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x5523, seq=10/2
Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: Microsoft_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft_40:57:38 (00:15:5d:40:57:38)
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.10
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xc533 [correct]
[Checksum Status: Good]
Identifier (BE): 21795 (0x5523)
Identifier (LE): 9045 (0x2355)
Sequence Number (BE): 9 (0x0009)
Sequence Number (LE): 2304 (0x0900)
[No response seen]
Timestamp from icmp data: Sep 25, 2025 17:52:04.305856000 EDT
[Timestamp from icmp data (relative): 0.000048000 seconds]
Data (40 bytes)

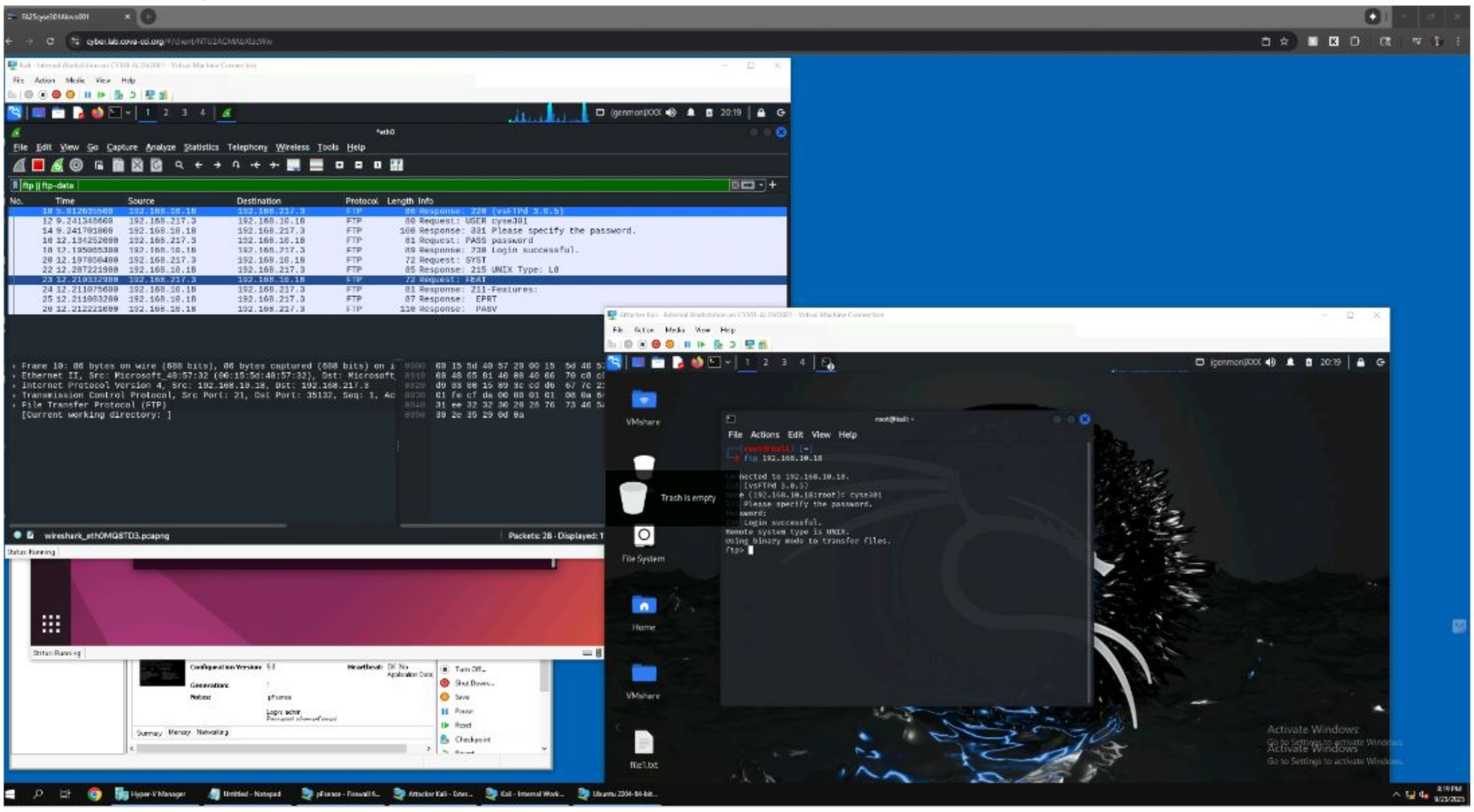
TASK B

B1

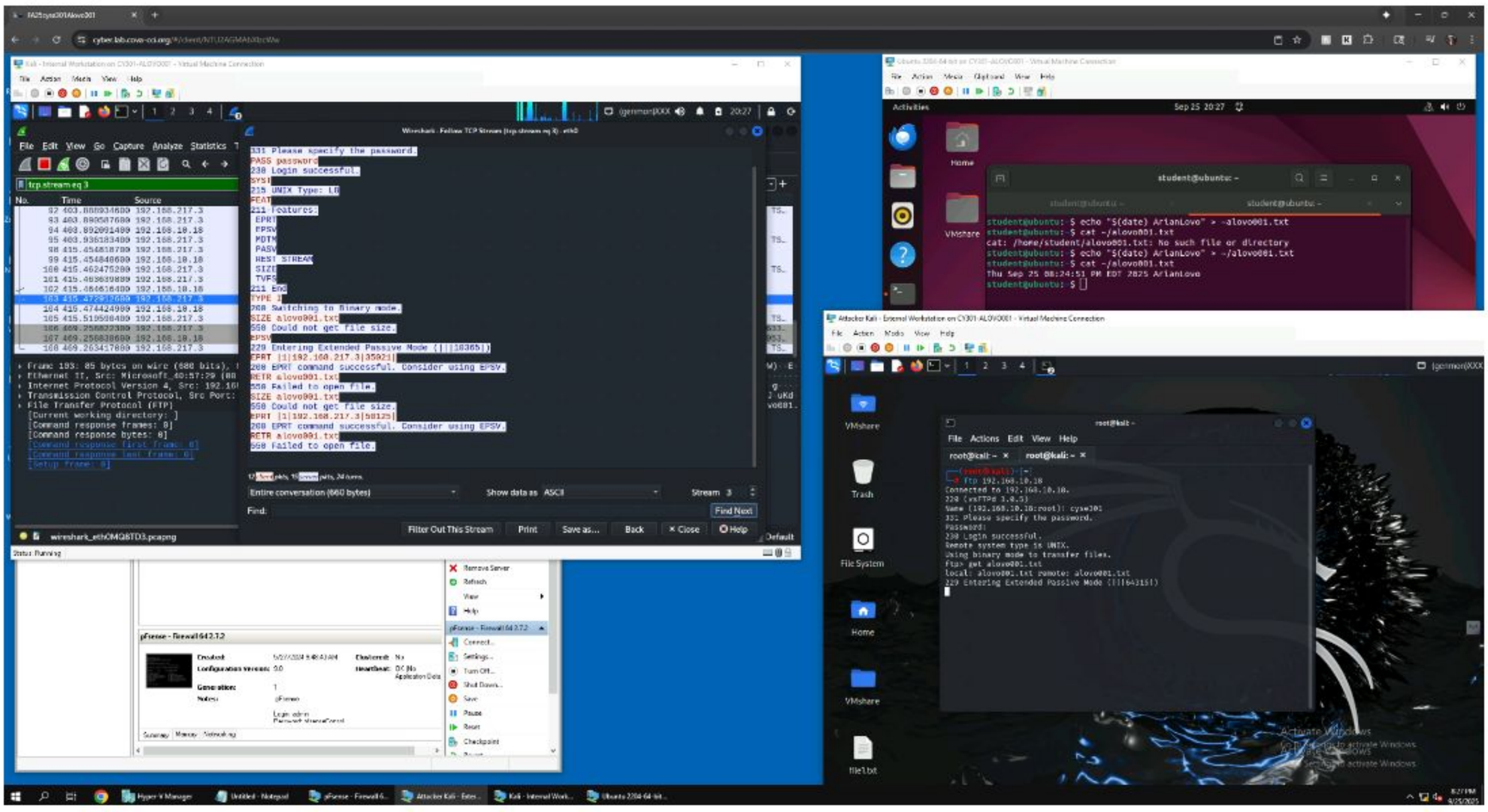
ICMP traffic



Ftp server login



Task c


Wireshark · Follow TCP Stream (tcp.stream eq 3) · eth0
tcp.stream eq 3
No. Time Source
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211 Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
211 End
TYPE I
200 Switching to Binary mode.
SIZE alovo001.txt
550 Could not get file size.
EPSV
229 Entering Extended Passive Mode (|||18365|)
EPRT |1|192.168.217.3|35021|
200 EPRT command successful. Consider using EPSV.
RETR alovo001.txt
550 Failed to open file.
SIZE alovo001.txt
550 Could not get file size.
EPRT |1|192.168.217.3|58125|
200 EPRT command successful. Consider using EPSV.
RETR alovo001.txt
550 Failed to open file.
Entire conversation (660 bytes)
Show data as ASCII
Stream 3
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
wireshark_eth0MQ8TD3.pcapng
Default
Status: Running
pfSense - Firewall 64 2.7.2
Remove Server
Refresh
View
Help
Connect...
Settings...
Turn Off...
Shut Down...
Save
Pause
Reset
Checkpoint
Activities
Sep 25 20:27
Home
VMshare
student@ubuntu: ~
student@ubuntu: $ echo "$(date) ArianLovo" > ~alovo001.txt
student@ubuntu:~$ cat ~/alovo001.txt
cat: /home/student/alovo001.txt: No such file or directory
student@ubuntu: $ echo "$(date) ArianLovo" > ~/alovo001.txt
student@ubuntu:~$ cat ~/alovo001.txt
Thu Sep 25 08:24:51 PM EDT 2025 ArianLovo
student@ubuntu: $
Attacker Kali - External Workstation on CY301-ALOVO001 - Virtual Machine Connection
File Actions Edit View Help
root@kali: ~
root@kali: ~
Trash
File System
Home
VMshare
file1.txt
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): cyse301
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get alovo001.txt
local: alovo001.txt remote: alovo001.txt
229 Entering Extended Passive Mode (|||64315|)
Activate Windows