Analyzing Data Link and Network Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 02

Student:	Email:
Haileab Tadele Bekele	haileabbekele0@gmail.com

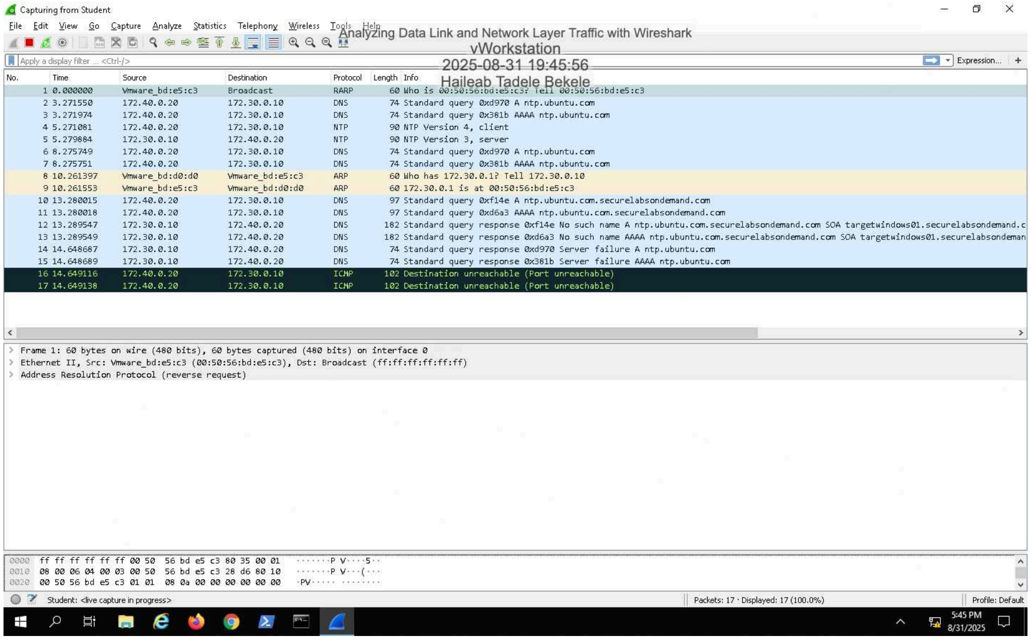
Time on Task:	Progress:
2 hours, 40 minutes	100%

Report Generated: Sunday, August 31, 2025 at 11:13 PM

Section 1: Hands-On Demonstration

Part 1: Explore the Wireshark Application and Capture Network Traffic

6. **Make a screen capture** showing the **captured packets in Wireshark**.



Capturing from Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 19:45:56
Haileab Tadele Bekele

```
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   Vmware_bd:e5:c3    Broadcast          RARP      60 Who is 00:50:56:bd:e5:c3? Tell 00:50:56:bd:e5:c3
   2 3.271550   172.40.0.20        172.30.0.10        DNS       74 Standard query 0xd970 A ntp.ubuntu.com
   3 3.271974   172.40.0.20        172.30.0.10        DNS       74 Standard query 0x381b AAAA ntp.ubuntu.com
   4 5.271081   172.40.0.20        172.30.0.10        NTP       90 NTP Version 4, client
   5 5.279884   172.30.0.10        172.40.0.20        NTP       90 NTP Version 3, server
   6 8.275749   172.40.0.20        172.30.0.10        DNS       74 Standard query 0xd970 A ntp.ubuntu.com
   7 8.275751   172.40.0.20        172.30.0.10        DNS       74 Standard query 0x381b AAAA ntp.ubuntu.com
   8 10.261397  Vmware_bd:d0:d0    Vmware_bd:e5:c3    ARP       60 Who has 172.30.0.1? Tell 172.30.0.10
   9 10.261553  Vmware_bd:e5:c3    Vmware_bd:d0:d0    ARP       60 172.30.0.1 is at 00:50:56:bd:e5:c3
  10 13.280015  172.40.0.20        172.30.0.10        DNS       97 Standard query 0xf14e A ntp.ubuntu.com.securelabsondemand.com
  11 13.280018  172.40.0.20        172.30.0.10        DNS       97 Standard query 0xd6a3 AAAA ntp.ubuntu.com.securelabsondemand.com
  12 13.289547  172.30.0.10        172.40.0.20        DNS      182 Standard query response 0xf14e No such name A ntp.ubuntu.com.securelabsondemand.com SOA targetwindows01.securelabsondemand.c
  13 13.289549  172.30.0.10        172.40.0.20        DNS      182 Standard query response 0xd6a3 No such name AAAA ntp.ubuntu.com.securelabsondemand.com SOA targetwindows01.securelabsondeman
  14 14.648687  172.30.0.10        172.40.0.20        DNS       74 Standard query response 0xd970 Server failure A ntp.ubuntu.com
  15 14.648689  172.30.0.10        172.40.0.20        DNS       74 Standard query response 0x381b Server failure AAAA ntp.ubuntu.com
  16 14.649116  172.40.0.20        172.30.0.10        ICMP     102 Destination unreachable (Port unreachable)
  17 14.649138  172.40.0.20        172.30.0.10        ICMP     102 Destination unreachable (Port unreachable)
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (reverse request)
```

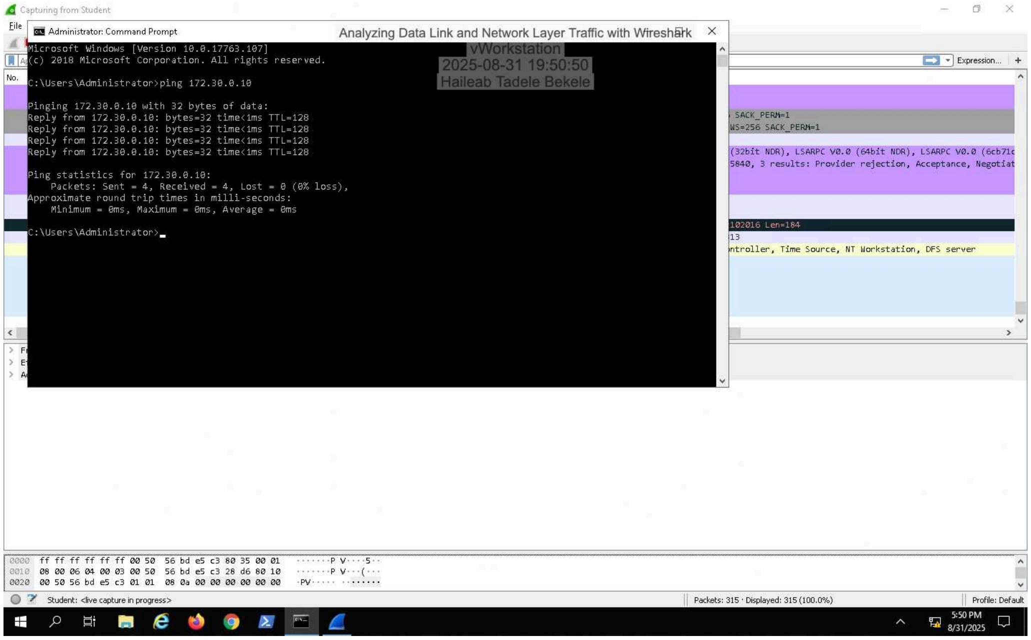
```
0000  ff ff ff ff ff ff 00 50  56 bd e5 c3 80 35 00 01   ·······P V····5··
0010  08 00 06 04 00 03 00 50  56 bd e5 c3 28 d6 80 10   ·······P V···(···
0020  00 50 56 bd e5 c3 01 01  08 0a 00 00 00 00 00 00   ·PV····· ········
```

Student: <live capture in progress>

Packets: 17 · Displayed: 17 (100.0%)

Profile: Default

9. **Make a screen capture** showing the **Ping results for 170.30.0.10**.



Administrator: Command Prompt

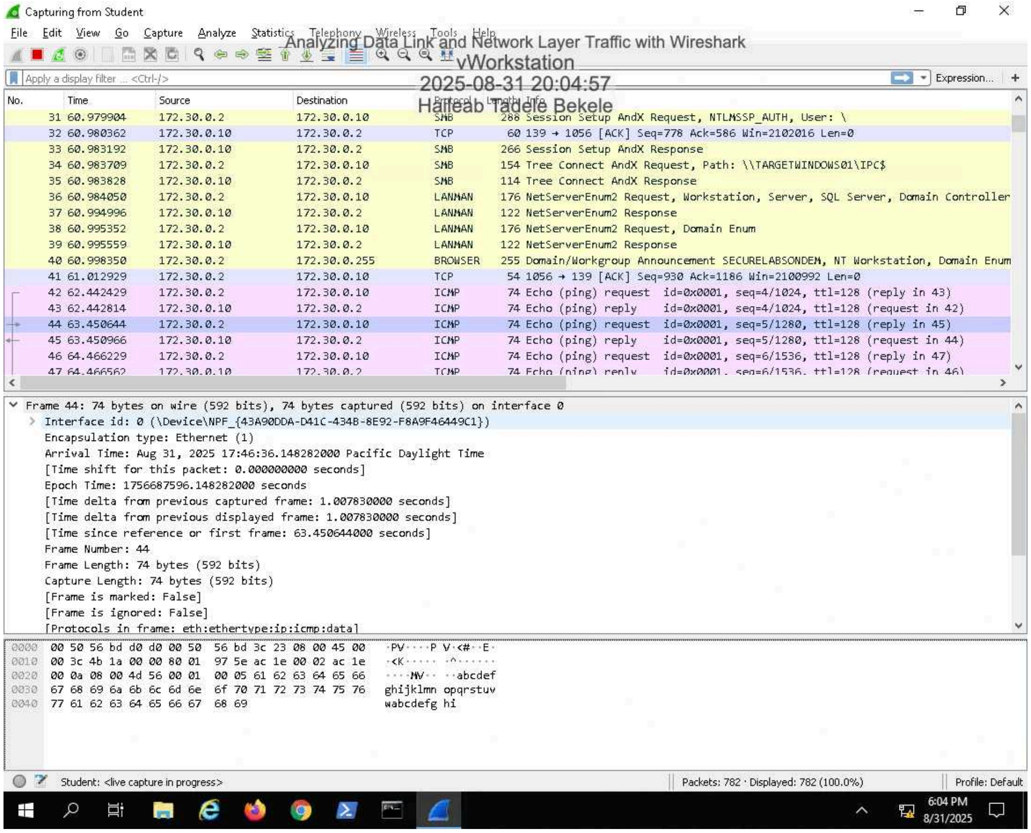
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 19:50:50
Haileab Tadele Bekele

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.30.0.10

Pinging 172.30.0.10 with 32 bytes of data:
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Student: <live capture in progress>
Packets: 315 · Displayed: 315 (100.0%)
Profile: Default

5:50 PM
8/31/2025

14. **Make a screen capture** showing the **Packet details related to time**.



Capturing from Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:04:57
Haileab Tadele Bekele

```
No.  Time       Source        Destination   Protocol Length Info
  31 60.979904  172.30.0.2    172.30.0.10   SMB      288 Session Setup AndX Request, NTLMSSP_AUTH, User: \
  32 60.980362  172.30.0.10   172.30.0.2    TCP       60 139 → 1056 [ACK] Seq=778 Ack=586 Win=2102016 Len=0
  33 60.983192  172.30.0.10   172.30.0.2    SMB      266 Session Setup AndX Response
  34 60.983709  172.30.0.2    172.30.0.10   SMB      154 Tree Connect AndX Request, Path: \\TARGETWINDOWS01\IPC$
  35 60.983828  172.30.0.10   172.30.0.2    SMB      114 Tree Connect AndX Response
  36 60.984050  172.30.0.2    172.30.0.10   LANMAN   176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller
  37 60.994996  172.30.0.10   172.30.0.2    LANMAN   122 NetServerEnum2 Response
  38 60.995352  172.30.0.2    172.30.0.10   LANMAN   176 NetServerEnum2 Request, Domain Enum
  39 60.995559  172.30.0.10   172.30.0.2    LANMAN   122 NetServerEnum2 Response
  40 60.998350  172.30.0.2    172.30.0.255  BROWSER  255 Domain/Workgroup Announcement SECURELABSONDEM, NT Workstation, Domain Enum
  41 61.012929  172.30.0.2    172.30.0.10   TCP       54 1056 → 139 [ACK] Seq=930 Ack=1186 Win=2100992 Len=0
  42 62.442429  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 43)
  43 62.442814  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=128 (request in 42)
  44 63.450644  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 45)
  45 63.450966  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=128 (request in 44)
  46 64.466229  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 47)
  47 64.466562  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=128 (request in 46)
```

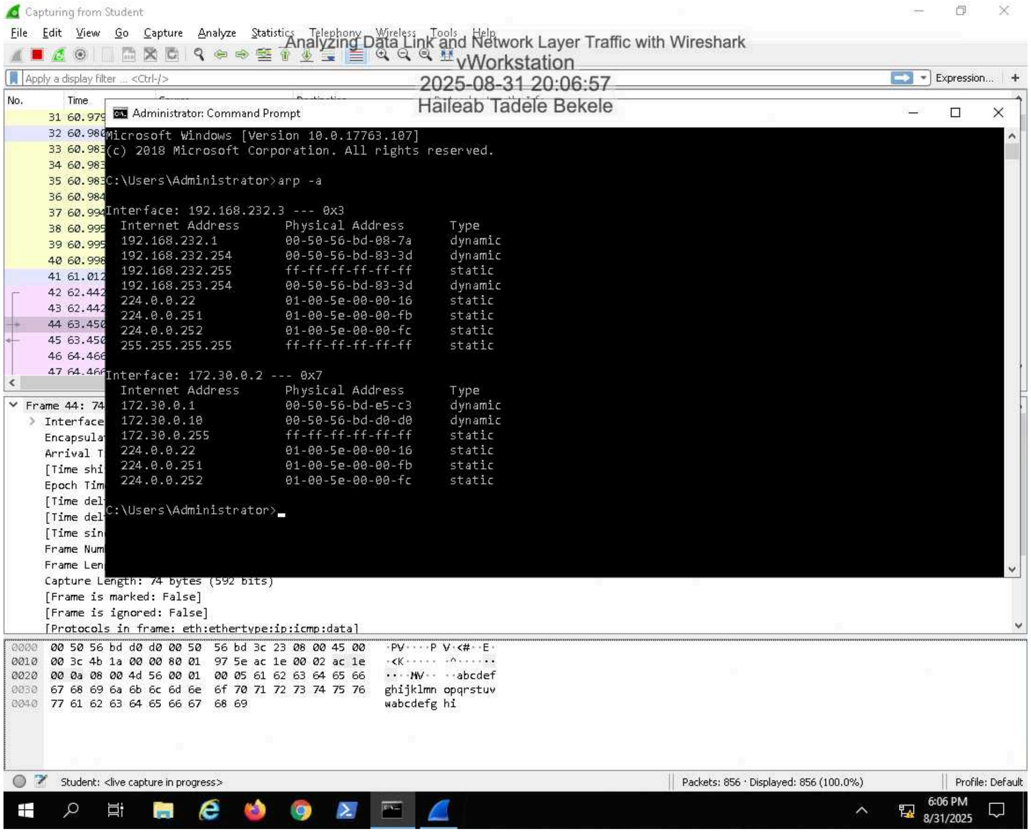
```
Frame 44: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  > Interface id: 0 (\Device\NPF_{43A90DDA-D41C-434B-8E92-F8A9F46449C1})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 31, 2025 17:46:36.148282000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1756687596.148282000 seconds
    [Time delta from previous captured frame: 1.007830000 seconds]
    [Time delta from previous displayed frame: 1.007830000 seconds]
    [Time since reference or first frame: 63.450644000 seconds]
    Frame Number: 44
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
```

```
0000  00 50 56 bd d0 d0 00 50  56 bd 3c 23 08 00 45 00   ·PV····P V·<#··E·
0010  00 3c 4b 1a 00 00 80 01  97 5e ac 1e 00 02 ac 1e   ·<K····· ·^······
0020  00 0a 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   ····MV·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Student: <live capture in progress>
Packets: 782 · Displayed: 782 (100.0%)
Profile: Default

6:04 PM
8/31/2025

17. **Make a screen capture** showing the **ARP table for the vWorkstation**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:06:57
Haileab Tadele Bekele

Capturing from Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Administrator: Command Prompt

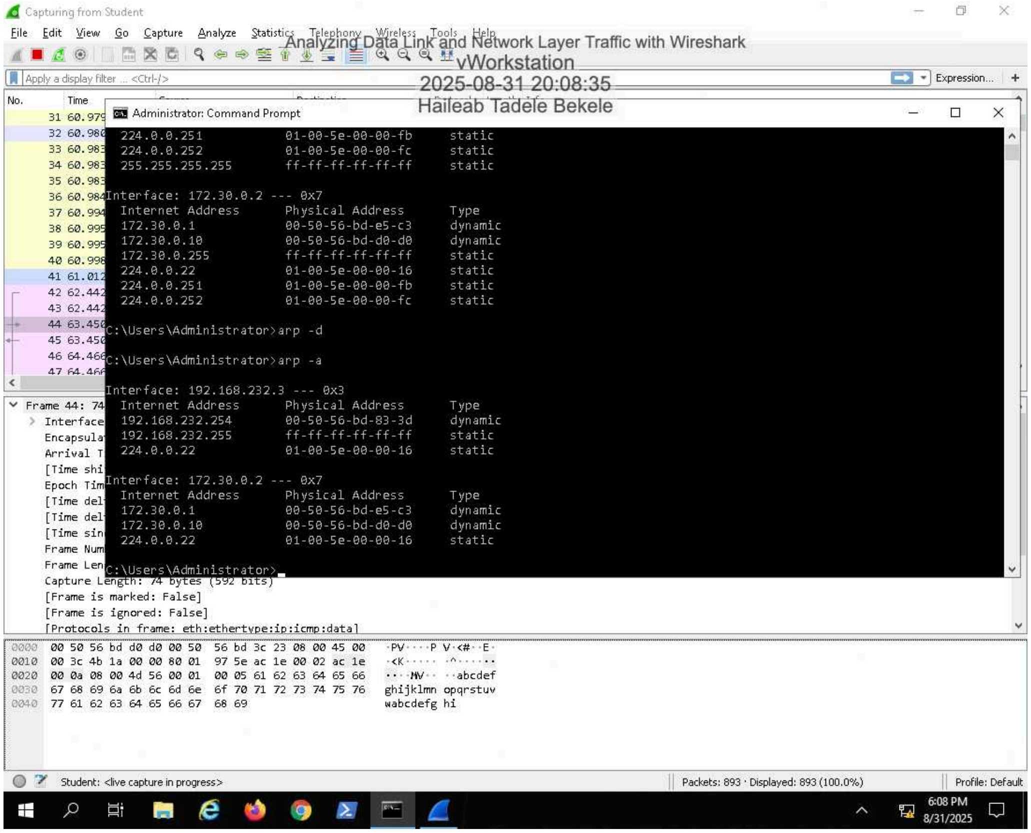
```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -a

Interface: 192.168.232.3 --- 0x3
  Internet Address      Physical Address      Type
  192.168.232.1         00-50-56-bd-08-7a     dynamic
  192.168.232.254       00-50-56-bd-83-3d     dynamic
  192.168.232.255       ff-ff-ff-ff-ff-ff     static
  192.168.253.254       00-50-56-bd-83-3d     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.30.0.2 --- 0x7
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-bd-e5-c3     dynamic
  172.30.0.10           00-50-56-bd-d0-d0     dynamic
  172.30.0.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

C:\Users\Administrator>
```

```
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
```

```
0000  00 50 56 bd d0 d0 00 50  56 bd 3c 23 08 00 45 00   ·PV····P V·<#··E·
0010  00 3c 4b 1a 00 00 80 01  97 5e ac 1e 00 02 ac 1e   ·<K····· ·^······
0020  00 0a 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   ····MV·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Student: <live capture in progress>
Packets: 856 · Displayed: 856 (100.0%)
Profile: Default
6:06 PM
8/31/2025

20. **Make a screen capture** showing the **cleared ARP table on the vWorkstation**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:08:35
Haileab Tadele Bekele

```
 224.0.0.251           01-00-5e-00-00-fb     static
 224.0.0.252           01-00-5e-00-00-fc     static
 255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.30.0.2 --- 0x7
 Internet Address      Physical Address      Type
 172.30.0.1            00-50-56-bd-e5-c3     dynamic
 172.30.0.10           00-50-56-bd-d0-d0     dynamic
 172.30.0.255          ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     static
 224.0.0.251           01-00-5e-00-00-fb     static
 224.0.0.252           01-00-5e-00-00-fc     static

C:\Users\Administrator>arp -d

C:\Users\Administrator>arp -a

Interface: 192.168.232.3 --- 0x3
 Internet Address      Physical Address      Type
 192.168.232.254       00-50-56-bd-83-3d     dynamic
 192.168.232.255       ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.30.0.2 --- 0x7
 Internet Address      Physical Address      Type
 172.30.0.1            00-50-56-bd-e5-c3     dynamic
 172.30.0.10           00-50-56-bd-d0-d0     dynamic
 224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>
```

```
31 60.979
32 60.980
33 60.983
34 60.983
35 60.983
36 60.984
37 60.994
38 60.995
39 60.995
40 60.998
41 61.012
42 62.442
43 62.442
44 63.450
45 63.450
46 64.466
47 64.466
```

```
Frame 44: 74
  Interface
  Encapsula
  Arrival T
  [Time shi
  Epoch Tim
  [Time del
  [Time del
  [Time sin
  Frame Num
  Frame Len
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:icmp:data]
```

```
0000  00 50 56 bd d0 d0 00 50  56 bd 3c 23 08 00 45 00   ·PV····P V·<#··E·
0010  00 3c 4b 1a 00 00 80 01  97 5e ac 1e 00 02 ac 1e   ·<K····· ·^······
0020  00 0a 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   ····MV·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

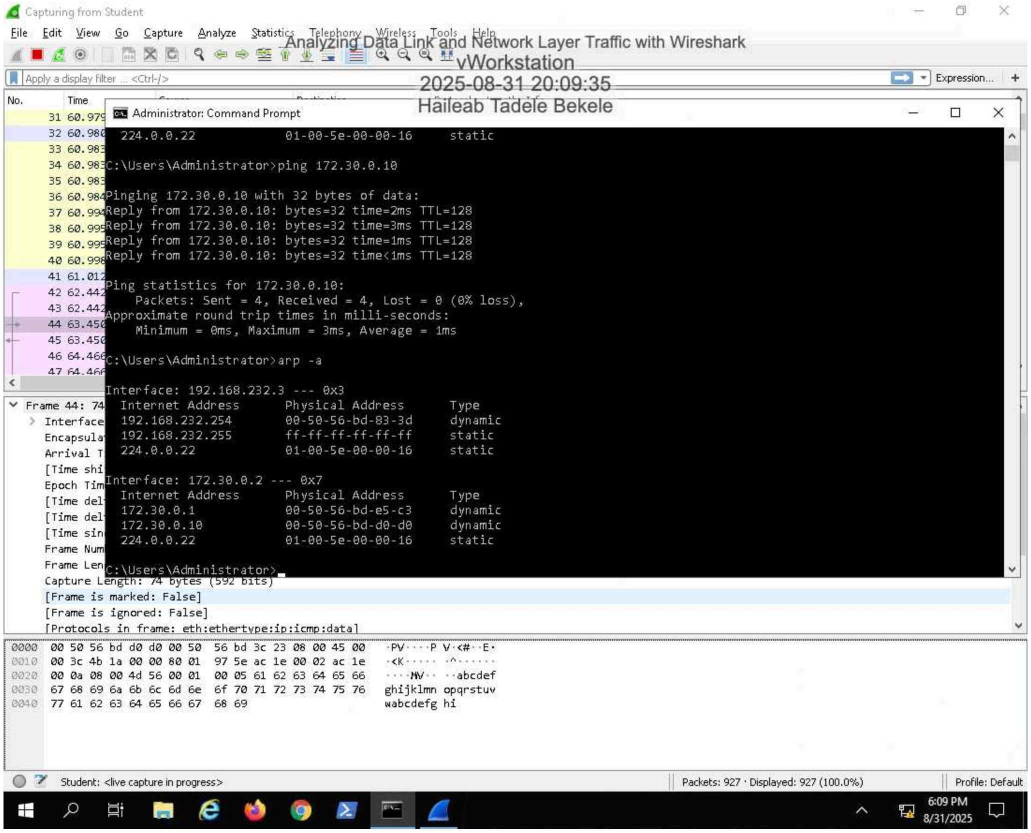
Student: <live capture in progress>

Packets: 893 · Displayed: 893 (100.0%)

Profile: Default

6:08 PM
8/31/2025

21. **Make a screen capture** showing the **updated ARP table with the new 172.30.0.10 entry**.


Capturing from Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Administrator: Command Prompt

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:09:35
Haileab Tadele Bekele

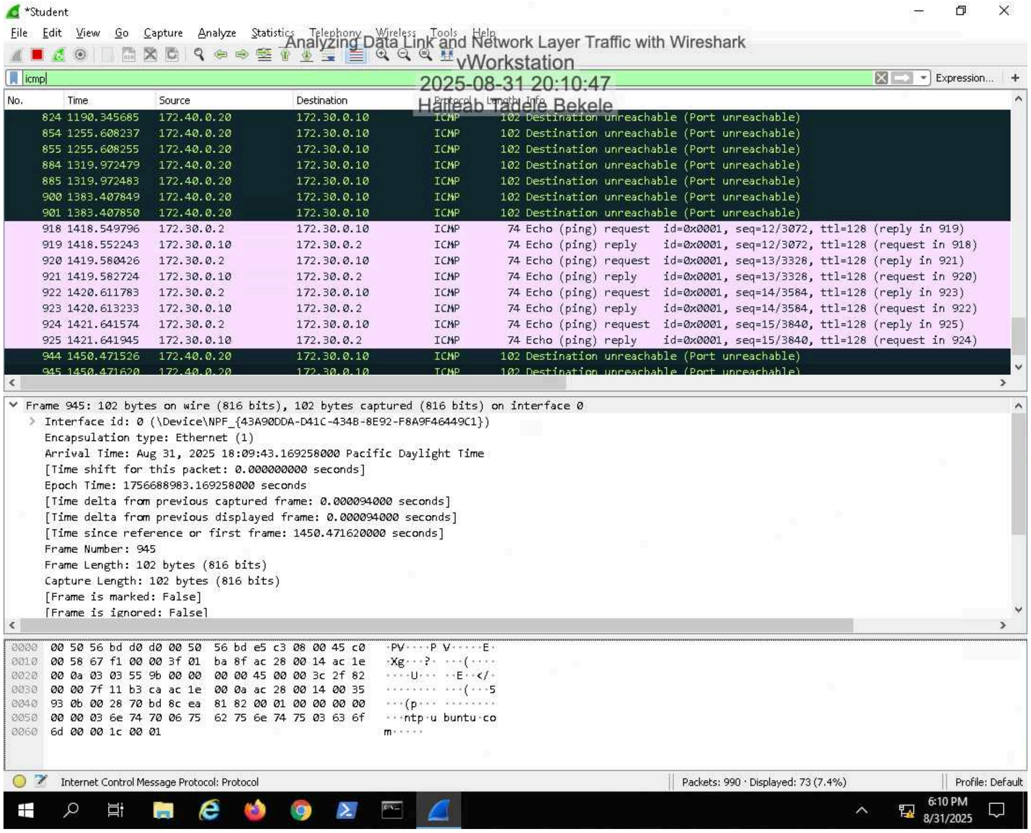
```
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>ping 172.30.0.10

Pinging 172.30.0.10 with 32 bytes of data:
Reply from 172.30.0.10: bytes=32 time=2ms TTL=128
Reply from 172.30.0.10: bytes=32 time=3ms TTL=128
Reply from 172.30.0.10: bytes=32 time=1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Users\Administrator>arp -a

Interface: 192.168.232.3 --- 0x3
  Internet Address      Physical Address      Type
  192.168.232.254       00-50-56-bd-83-3d     dynamic
  192.168.232.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.30.0.2 --- 0x7
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-bd-e5-c3     dynamic
  172.30.0.10           00-50-56-bd-d0-d0     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>
```

```
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
```

```
0000  00 50 56 bd d0 d0 00 50  56 bd 3c 23 08 00 45 00   ·PV····P V·<#··E·
0010  00 3c 4b 1a 00 00 80 01  97 5e ac 1e 00 02 ac 1e   ·<K····· ·^······
0020  00 0a 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   ····MV·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Student: <live capture in progress>
Packets: 927 · Displayed: 927 (100.0%)
Profile: Default
6:09 PM
8/31/2025

26. **Make a screen capture** showing the **filtered list of ICMP packets**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:10:47
Haileab Tadele Bekele

icmp

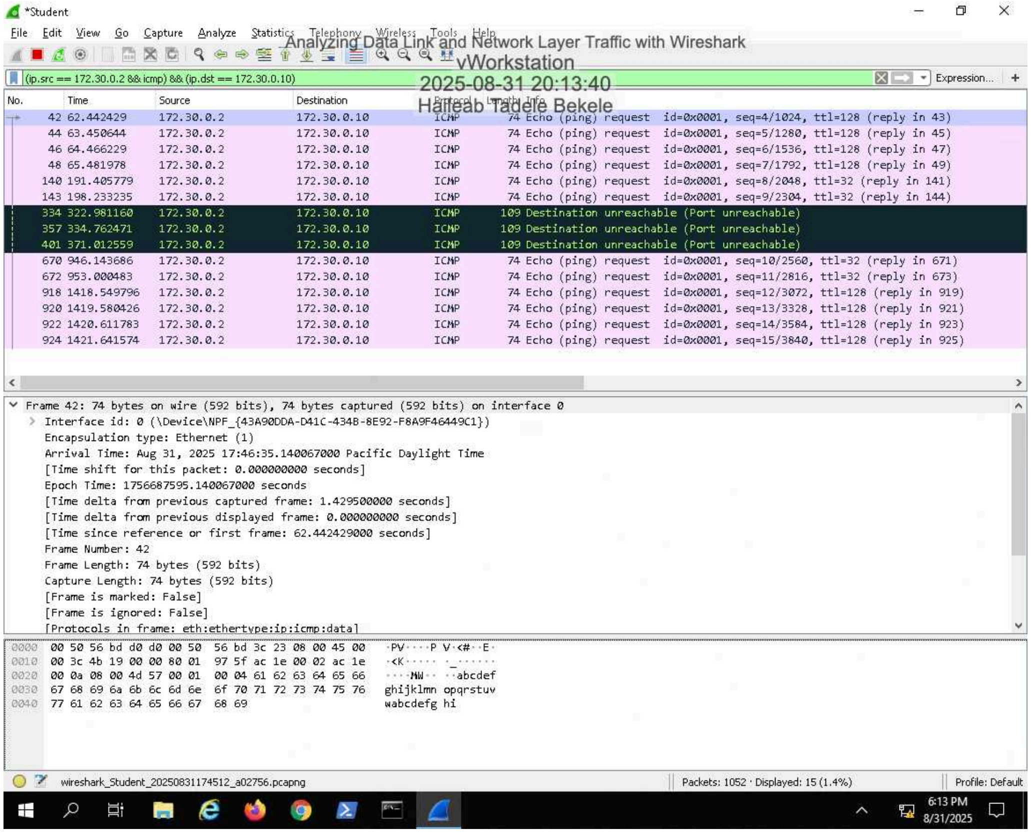
```
No.     Time         Source        Destination   Protocol Length Info
    824 1190.345685  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    854 1255.608237  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    855 1255.608255  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    884 1319.972479  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    885 1319.972483  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    900 1383.407849  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    901 1383.407850  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    918 1418.549796  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (reply in 919)
    919 1418.552243  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=128 (request in 918)
    920 1419.580426  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 921)
    921 1419.582724  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=128 (request in 920)
    922 1420.611783  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply in 923)
    923 1420.613233  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=128 (request in 922)
    924 1421.641574  172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 925)
    925 1421.641945  172.30.0.10   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=128 (request in 924)
    944 1450.471526  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    945 1450.471620  172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
```

```
v Frame 945: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
  > Interface id: 0 (\Device\NPF_{43A90DDA-D41C-434B-8E92-F8A9F46449C1})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 31, 2025 18:09:43.169258000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1756688983.169258000 seconds
    [Time delta from previous captured frame: 0.000094000 seconds]
    [Time delta from previous displayed frame: 0.000094000 seconds]
    [Time since reference or first frame: 1450.471620000 seconds]
    Frame Number: 945
    Frame Length: 102 bytes (816 bits)
    Capture Length: 102 bytes (816 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

```
0000  00 50 56 bd d0 d0 00 50  56 bd e5 c3 08 00 45 c0   ·PV····P V·····E·
0010  00 58 67 f1 00 00 3f 01  ba 8f ac 28 00 14 ac 1e   ·Xg···?· ···(····
0020  00 0a 03 03 55 9b 00 00  00 00 45 00 00 3c 2f 82   ····U··· ··E··</·
0030  00 00 7f 11 b3 ca ac 1e  00 0a ac 28 00 14 00 35   ········ ···(···5
0040  93 0b 00 28 70 bd 8c ea  81 82 00 01 00 00 00 00   ···(p··· ········
0050  00 00 03 6e 74 70 06 75  62 75 6e 74 75 03 63 6f   ···ntp·u buntu·co
0060  6d 00 00 1c 00 01                                  m·····
```

Internet Control Message Protocol: Protocol

30. **Make a screen capture** showing the **ICMP Packets with the src of 172.30.0.2 and dst of 172.30.0.10**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:13:40
Haileab Tadele Bekele

(ip.src == 172.30.0.2 && icmp) && (ip.dst == 172.30.0.10)

```
No.   Time          Source        Destination   Protocol Length Info
   42 62.442429     172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 43)
   44 63.450644     172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 45)
   46 64.466229     172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 47)
   48 65.481978     172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 49)
  140 191.405779    172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=32 (reply in 141)
  143 198.233235    172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=32 (reply in 144)
  334 322.981160    172.30.0.2    172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
  357 334.762471    172.30.0.2    172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
  401 371.012559    172.30.0.2    172.30.0.10   ICMP     109 Destination unreachable (Port unreachable)
  670 946.143686    172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=32 (reply in 671)
  672 953.000483    172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=32 (reply in 673)
  918 1418.549796   172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (reply in 919)
  920 1419.580426   172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 921)
  922 1420.611783   172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply in 923)
  924 1421.641574   172.30.0.2    172.30.0.10   ICMP      74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 925)
```

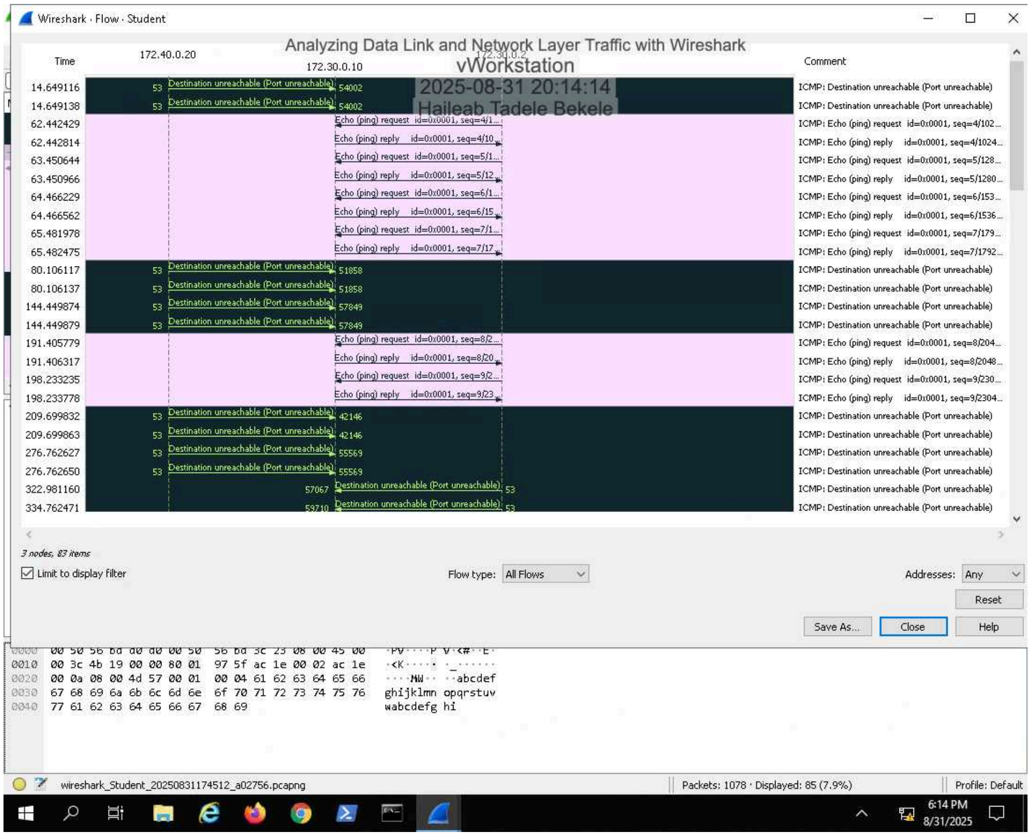
```
Frame 42: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  > Interface id: 0 (\Device\NPF_{43A90DDA-D41C-434B-8E92-F8A9F46449C1})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 31, 2025 17:46:35.140067000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1756687595.140067000 seconds
    [Time delta from previous captured frame: 1.429500000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 62.442429000 seconds]
    Frame Number: 42
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
```

```
0000  00 50 56 bd d0 d0 00 50  56 bd 3c 23 08 00 45 00   ·PV····P V·<#··E·
0010  00 3c 4b 19 00 00 80 01  97 5f ac 1e 00 02 ac 1e   ·<K····· ·_······
0020  00 0a 08 00 4d 57 00 01  00 04 61 62 63 64 65 66   ····MW·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

wireshark_Student_20250831174512_a02756.pcapng | Packets: 1052 · Displayed: 15 (1.4%) | Profile: Default

6:13 PM
8/31/2025

35. **Make a screen capture** showing the **Flow Graph limited to display filter** (ICMP packets).



Wireshark · Flow · Student

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:14:14
Haileab Tadele Bekele

Time	172.40.0.20		172.30.0.10		172.30.0.2	Comment
14.649116	53	Destination unreachable (Port unreachable)	54002			ICMP: Destination unreachable (Port unreachable)
14.649138	53	Destination unreachable (Port unreachable)	54002			ICMP: Destination unreachable (Port unreachable)
62.442429				Echo (ping) request id=0x0001, seq=4/1...		ICMP: Echo (ping) request id=0x0001, seq=4/102...
62.442814				Echo (ping) reply id=0x0001, seq=4/10...		ICMP: Echo (ping) reply id=0x0001, seq=4/1024...
63.450644				Echo (ping) request id=0x0001, seq=5/1...		ICMP: Echo (ping) request id=0x0001, seq=5/128...
63.450966				Echo (ping) reply id=0x0001, seq=5/12...		ICMP: Echo (ping) reply id=0x0001, seq=5/1280...
64.466229				Echo (ping) request id=0x0001, seq=6/1...		ICMP: Echo (ping) request id=0x0001, seq=6/153...
64.466562				Echo (ping) reply id=0x0001, seq=6/15...		ICMP: Echo (ping) reply id=0x0001, seq=6/1536...
65.481978				Echo (ping) request id=0x0001, seq=7/1...		ICMP: Echo (ping) request id=0x0001, seq=7/179...
65.482475				Echo (ping) reply id=0x0001, seq=7/17...		ICMP: Echo (ping) reply id=0x0001, seq=7/1792...
80.106117	53	Destination unreachable (Port unreachable)	51858			ICMP: Destination unreachable (Port unreachable)
80.106137	53	Destination unreachable (Port unreachable)	51858			ICMP: Destination unreachable (Port unreachable)
144.449874	53	Destination unreachable (Port unreachable)	57849			ICMP: Destination unreachable (Port unreachable)
144.449879	53	Destination unreachable (Port unreachable)	57849			ICMP: Destination unreachable (Port unreachable)
191.405779				Echo (ping) request id=0x0001, seq=8/2...		ICMP: Echo (ping) request id=0x0001, seq=8/204...
191.406317				Echo (ping) reply id=0x0001, seq=8/20...		ICMP: Echo (ping) reply id=0x0001, seq=8/2048...
198.233235				Echo (ping) request id=0x0001, seq=9/2...		ICMP: Echo (ping) request id=0x0001, seq=9/230...
198.233778				Echo (ping) reply id=0x0001, seq=9/23...		ICMP: Echo (ping) reply id=0x0001, seq=9/2304...
209.699832	53	Destination unreachable (Port unreachable)	42146			ICMP: Destination unreachable (Port unreachable)
209.699863	53	Destination unreachable (Port unreachable)	42146			ICMP: Destination unreachable (Port unreachable)
276.762627	53	Destination unreachable (Port unreachable)	55569			ICMP: Destination unreachable (Port unreachable)
276.762650	53	Destination unreachable (Port unreachable)	55569			ICMP: Destination unreachable (Port unreachable)
322.981160			57067	Destination unreachable (Port unreachable)	53	ICMP: Destination unreachable (Port unreachable)
334.762471			59710	Destination unreachable (Port unreachable)	53	ICMP: Destination unreachable (Port unreachable)

3 nodes, 83 items

☑ Limit to display filter

Flow type: All Flows

Addresses: Any

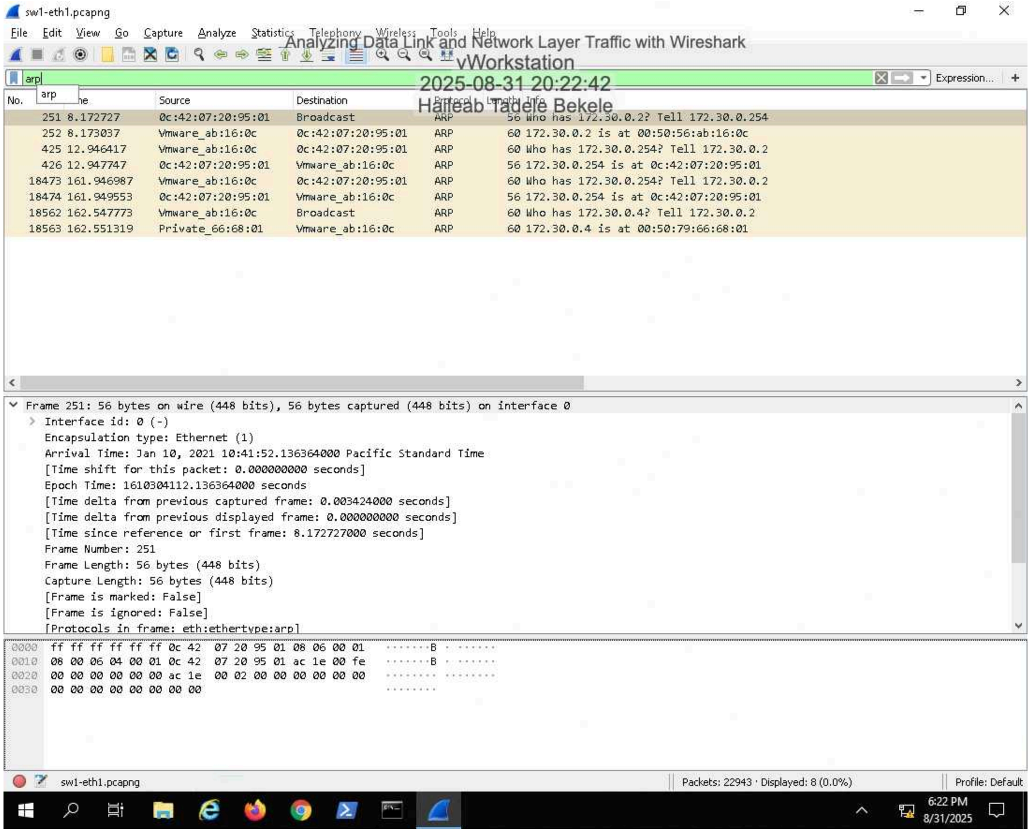
```
0000  00 50 56 bd d0 d0 00 50  56 bd 3c 23 08 00 45 00   ·PV····P V·<#··E·
0010  00 3c 4b 19 00 00 80 01  97 5f ac 1e 00 02 ac 1e   ·<K····· ·_······
0020  00 0a 08 00 4d 57 00 01  00 04 61 62 63 64 65 66   ····MW·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

wireshark_Student_20250831174512_a02756.pcapng | Packets: 1078 · Displayed: 85 (7.9%) | Profile: Default

6:14 PM
8/31/2025

Part 2: Explore a Wireshark Capture File

4. **Make a screen capture** showing the **ARP Packet List from your pcap file**.


sw1-eth1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
arp
6:22 PM
8/31/2025

arp

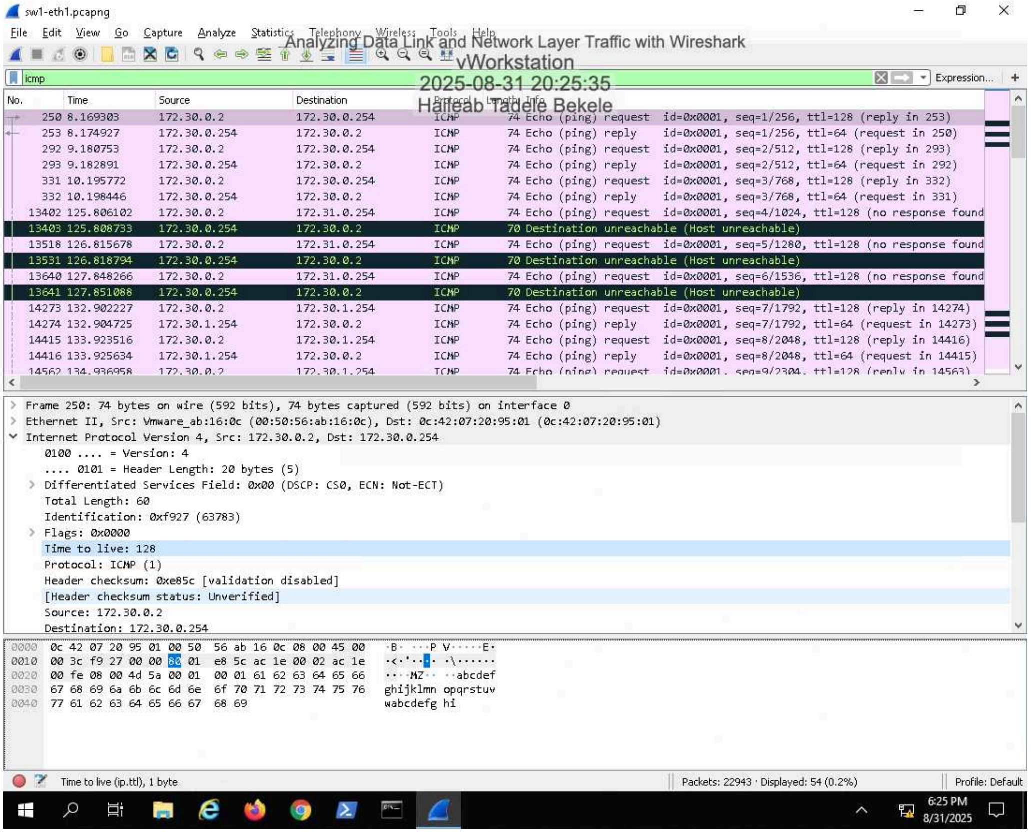
```
No.   Time         Source              Destination         Protocol  Length  Info
  251 8.172727     0c:42:07:20:95:01   Broadcast           ARP       56 Who has 172.30.0.2? Tell 172.30.0.254
  252 8.173037     Vmware_ab:16:0c     0c:42:07:20:95:01   ARP       60 172.30.0.2 is at 00:50:56:ab:16:0c
  425 12.946417    Vmware_ab:16:0c     0c:42:07:20:95:01   ARP       60 Who has 172.30.0.254? Tell 172.30.0.2
  426 12.947747    0c:42:07:20:95:01   Vmware_ab:16:0c     ARP       56 172.30.0.254 is at 0c:42:07:20:95:01
18473 161.946987   Vmware_ab:16:0c     0c:42:07:20:95:01   ARP       60 Who has 172.30.0.254? Tell 172.30.0.2
18474 161.949553   0c:42:07:20:95:01   Vmware_ab:16:0c     ARP       56 172.30.0.254 is at 0c:42:07:20:95:01
18562 162.547773   Vmware_ab:16:0c     Broadcast           ARP       60 Who has 172.30.0.4? Tell 172.30.0.2
18563 162.551319   Private_66:68:01    Vmware_ab:16:0c     ARP       60 172.30.0.4 is at 00:50:79:66:68:01
```

```
Frame 251: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
  > Interface id: 0 (-)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 10, 2021 10:41:52.136364000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1610304112.136364000 seconds
    [Time delta from previous captured frame: 0.003424000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.172727000 seconds]
    Frame Number: 251
    Frame Length: 56 bytes (448 bits)
    Capture Length: 56 bytes (448 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
```

```
0000  ff ff ff ff ff ff 0c 42  07 20 95 01 08 06 00 01   ·······B ·······
0010  08 00 06 04 00 01 0c 42  07 20 95 01 ac 1e 00 fe   ·······B ·······
0020  00 00 00 00 00 00 ac 1e  00 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00                            ········
```

sw1-eth1.pcapng | Packets: 22943 · Displayed: 8 (0.0%) | Profile: Default

12. **Make a screen capture** showing the **Time to live field value for packet 21314**.



```
No.     Time        Source          Destination     Protocol Length Info
  250   8.169303    172.30.0.2      172.30.0.254    ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 253)
  253   8.174927    172.30.0.254    172.30.0.2      ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (request in 250)
  292   9.180753    172.30.0.2      172.30.0.254    ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 293)
  293   9.182891    172.30.0.254    172.30.0.2      ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (request in 292)
  331   10.195772   172.30.0.2      172.30.0.254    ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 332)
  332   10.198446   172.30.0.254    172.30.0.2      ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (request in 331)
13402   125.806102  172.30.0.2      172.31.0.254    ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (no response found
13403   125.808733  172.30.0.254    172.30.0.2      ICMP     70 Destination unreachable (Host unreachable)
13518   126.815678  172.30.0.2      172.31.0.254    ICMP     74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (no response found
13531   126.818794  172.30.0.254    172.30.0.2      ICMP     70 Destination unreachable (Host unreachable)
13640   127.848266  172.30.0.2      172.31.0.254    ICMP     74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (no response found
13641   127.851088  172.30.0.254    172.30.0.2      ICMP     70 Destination unreachable (Host unreachable)
14273   132.902227  172.30.0.2      172.30.1.254    ICMP     74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 14274)
14274   132.904725  172.30.1.254    172.30.0.2      ICMP     74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=64 (request in 14273)
14415   133.923516  172.30.0.2      172.30.1.254    ICMP     74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 14416)
14416   133.925634  172.30.1.254    172.30.0.2      ICMP     74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=64 (request in 14415)
14562   134.936958  172.30.0.2      172.30.1.254    ICMP     74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=128 (reply in 14563)
```

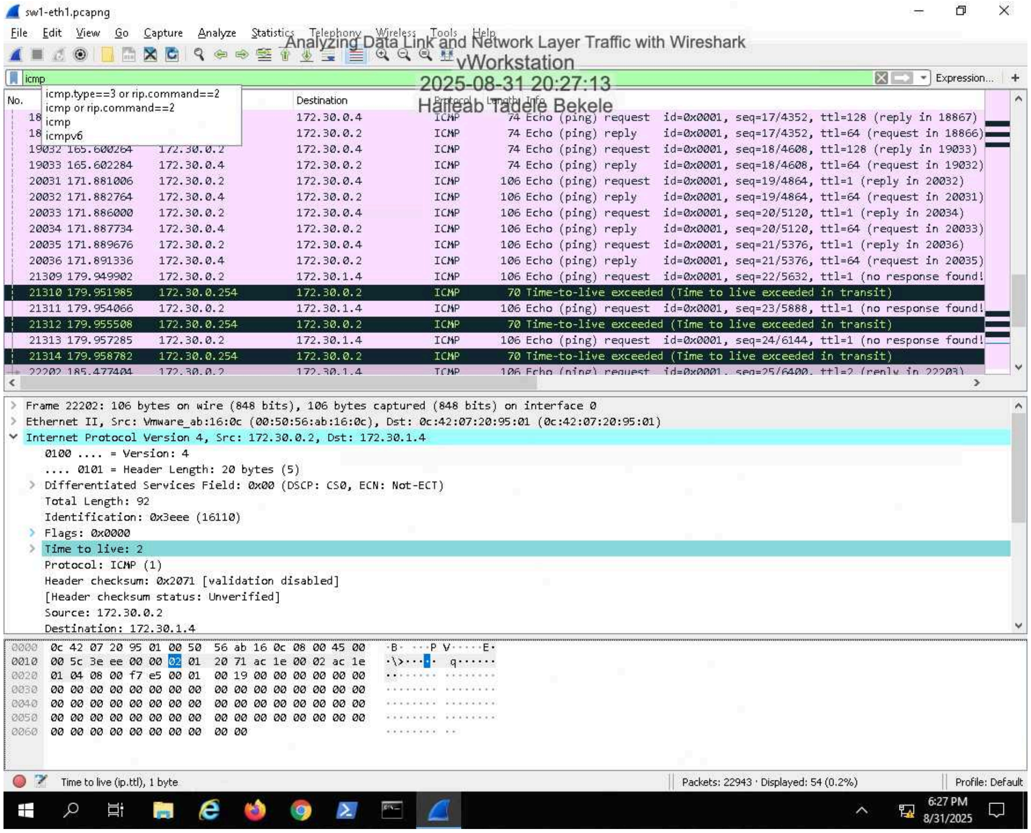
```
> Frame 250: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_ab:16:0c (00:50:56:ab:16:0c), Dst: 0c:42:07:20:95:01 (0c:42:07:20:95:01)
v Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xf927 (63783)
  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xe85c [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.0.2
    Destination: 172.30.0.254
```

```
0000  0c 42 07 20 95 01 00 50  56 ab 16 0c 08 00 45 00   ·B· ···P V·····E·
0010  00 3c f9 27 00 00 80 01  e8 5c ac 1e 00 02 ac 1e   ·<·'····  ·\······
0020  00 fe 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ····MZ··  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Time to live (ip.ttl), 1 byte | Packets: 22943 · Displayed: 54 (0.2%) | Profile: Default

6:25 PM
8/31/2025

15. **Make a screen capture** showing the **Time to live field for packet 22202**.


sw1-eth1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 20:27:13
Haileab Tadele Bekele
Expression...
+
6:27 PM
8/31/2025

icmp

icmp.type==3 or rip.command==2
icmp or rip.command==2
icmp
icmpv6

```
No.                                  Destination   Protocol Length Info
   18                                172.30.0.4    ICMP      74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=128 (reply in 18867)
   18                                172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=64 (request in 18866)
19032 165.600264   172.30.0.2        172.30.0.4    ICMP      74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=128 (reply in 19033)
19033 165.602284   172.30.0.4        172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=18/4608, ttl=64 (request in 19032)
20031 171.881006   172.30.0.2        172.30.0.4    ICMP     106 Echo (ping) request  id=0x0001, seq=19/4864, ttl=1 (reply in 20032)
20032 171.882764   172.30.0.4        172.30.0.2    ICMP     106 Echo (ping) reply    id=0x0001, seq=19/4864, ttl=64 (request in 20031)
20033 171.886000   172.30.0.2        172.30.0.4    ICMP     106 Echo (ping) request  id=0x0001, seq=20/5120, ttl=1 (reply in 20034)
20034 171.887734   172.30.0.4        172.30.0.2    ICMP     106 Echo (ping) reply    id=0x0001, seq=20/5120, ttl=64 (request in 20033)
20035 171.889676   172.30.0.2        172.30.0.4    ICMP     106 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1 (reply in 20036)
20036 171.891336   172.30.0.4        172.30.0.2    ICMP     106 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=64 (request in 20035)
21309 179.949902   172.30.0.2        172.30.1.4    ICMP     106 Echo (ping) request  id=0x0001, seq=22/5632, ttl=1 (no response found!
21310 179.951985   172.30.0.254      172.30.0.2    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
21311 179.954066   172.30.0.2        172.30.1.4    ICMP     106 Echo (ping) request  id=0x0001, seq=23/5888, ttl=1 (no response found!
21312 179.955508   172.30.0.254      172.30.0.2    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
21313 179.957285   172.30.0.2        172.30.1.4    ICMP     106 Echo (ping) request  id=0x0001, seq=24/6144, ttl=1 (no response found!
21314 179.958782   172.30.0.254      172.30.0.2    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
22202 185.477404   172.30.0.2        172.30.1.4    ICMP     106 Echo (ping) request  id=0x0001, seq=25/6400, ttl=2 (reply in 22203)
```

```
> Frame 22202: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Vmware_ab:16:0c (00:50:56:ab:16:0c), Dst: 0c:42:07:20:95:01 (0c:42:07:20:95:01)
v Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.1.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x3eee (16110)
  > Flags: 0x0000
  > Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0x2071 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.0.2
    Destination: 172.30.1.4
```

```
0000  0c 42 07 20 95 01 00 50  56 ab 16 0c 08 00 45 00   ·B· ···P V·····E·
0010  00 5c 3e ee 00 00 02 01  20 71 ac 1e 00 02 ac 1e   ·\>···········
0020  01 04 08 00 f7 e5 00 01  00 19 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Time to live (ip.ttl), 1 byte | Packets: 22943 · Displayed: 54 (0.2%) | Profile: Default

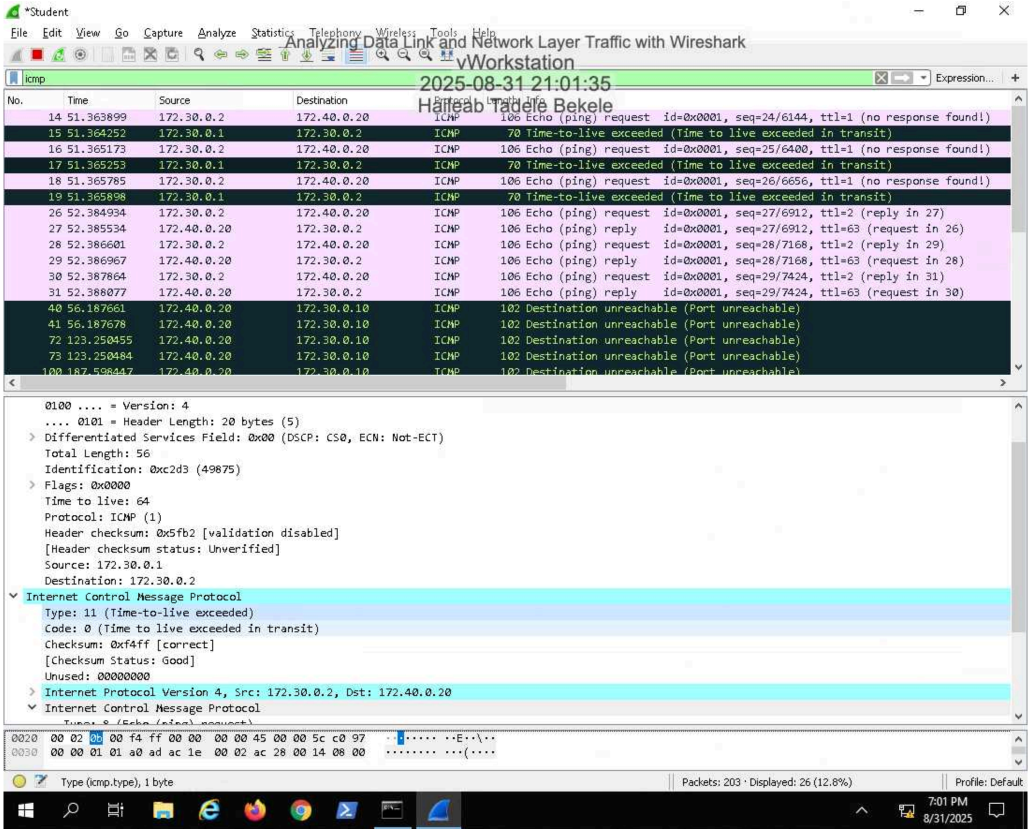
24. **Record** the VLAN ID of the 172.30.0.0/24 network.

3

Section 2: Applied Learning

Part 1: Explore the Wireshark Application and Capture Network Traffic

9. **Make a screen capture** showing the **Echo request Type in the Packet Details view**.



icmp

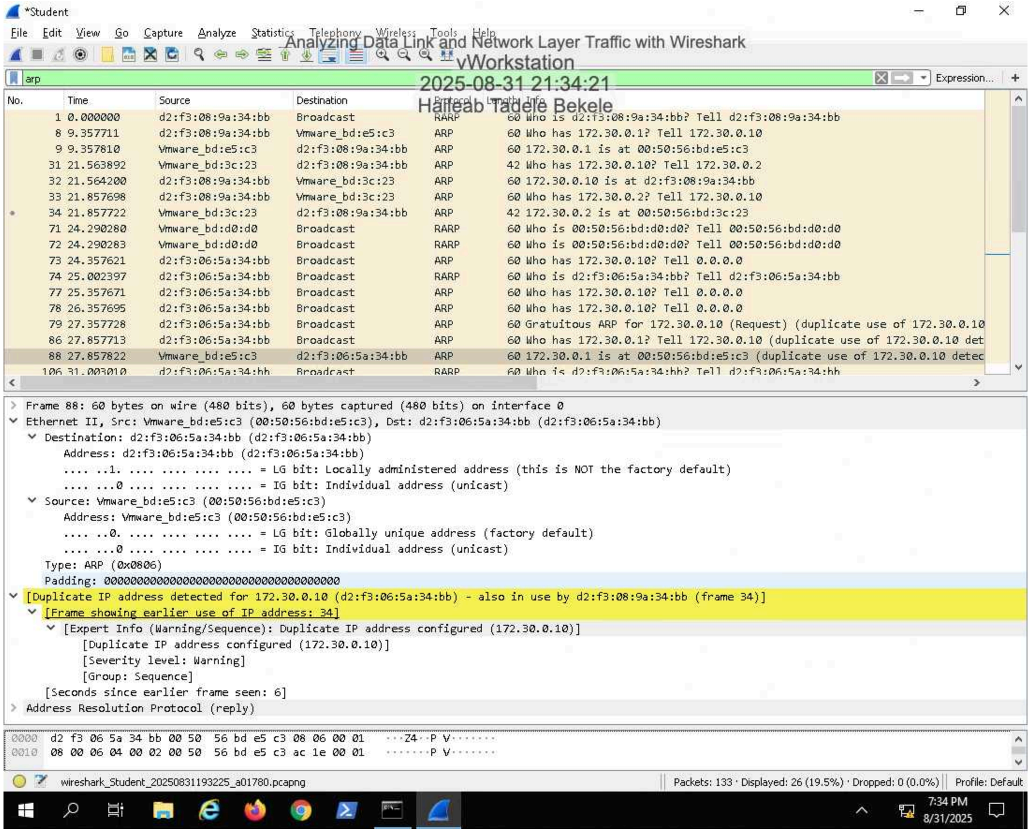
```
No.     Time          Source        Destination   Protocol Length Info
     14 51.363899     172.30.0.2    172.40.0.20   ICMP     106 Echo (ping) request  id=0x0001, seq=24/6144, ttl=1 (no response found!)
     15 51.364252     172.30.0.1    172.30.0.2    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
     16 51.365173     172.30.0.2    172.40.0.20   ICMP     106 Echo (ping) request  id=0x0001, seq=25/6400, ttl=1 (no response found!)
     17 51.365253     172.30.0.1    172.30.0.2    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
     18 51.365785     172.30.0.2    172.40.0.20   ICMP     106 Echo (ping) request  id=0x0001, seq=26/6656, ttl=1 (no response found!)
     19 51.365898     172.30.0.1    172.30.0.2    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
     26 52.384934     172.30.0.2    172.40.0.20   ICMP     106 Echo (ping) request  id=0x0001, seq=27/6912, ttl=2 (reply in 27)
     27 52.385534     172.40.0.20   172.30.0.2    ICMP     106 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=63 (request in 26)
     28 52.386601     172.30.0.2    172.40.0.20   ICMP     106 Echo (ping) request  id=0x0001, seq=28/7168, ttl=2 (reply in 29)
     29 52.386967     172.40.0.20   172.30.0.2    ICMP     106 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=63 (request in 28)
     30 52.387864     172.30.0.2    172.40.0.20   ICMP     106 Echo (ping) request  id=0x0001, seq=29/7424, ttl=2 (reply in 31)
     31 52.388077     172.40.0.20   172.30.0.2    ICMP     106 Echo (ping) reply    id=0x0001, seq=29/7424, ttl=63 (request in 30)
     40 56.187661     172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
     41 56.187678     172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
     72 123.250455    172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
     73 123.250484    172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
    100 187.598447    172.40.0.20   172.30.0.10   ICMP     102 Destination unreachable (Port unreachable)
```

```
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
      > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 56
        Identification: 0xc2d3 (49875)
      > Flags: 0x0000
        Time to live: 64
        Protocol: ICMP (1)
        Header checksum: 0x5fb2 [validation disabled]
        [Header checksum status: Unverified]
        Source: 172.30.0.1
        Destination: 172.30.0.2
  v Internet Control Message Protocol
        Type: 11 (Time-to-live exceeded)
        Code: 0 (Time to live exceeded in transit)
        Checksum: 0xf4ff [correct]
        [Checksum Status: Good]
        Unused: 00000000
      > Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.20
      v Internet Control Message Protocol
          Type: 8 (Echo (ping) request)
```

```
0020  00 02 0b 00 f4 ff 00 00  00 00 45 00 00 5c c0 97   ········ ··E··\··
0030  00 00 01 01 a0 ad ac 1e  00 02 ac 28 00 14 08 00   ········ ···(····
```

Type (icmp.type), 1 byte | Packets: 203 · Displayed: 26 (12.8%) | Profile: Default

26. **Make a screen capture** showing the **“Duplicate IP address detected” details and the Frame the original MAC address was identified in**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 21:34:21
Haileab Tadele Bekele

arp

```
No.   Time        Source             Destination        Protocol Length Info
    1 0.000000    d2:f3:08:9a:34:bb  Broadcast          RARP     60 Who is d2:f3:08:9a:34:bb? Tell d2:f3:08:9a:34:bb
    8 9.357711    d2:f3:08:9a:34:bb  Vmware_bd:e5:c3    ARP      60 Who has 172.30.0.1? Tell 172.30.0.10
    9 9.357810    Vmware_bd:e5:c3    d2:f3:08:9a:34:bb  ARP      60 172.30.0.1 is at 00:50:56:bd:e5:c3
   31 21.563892   Vmware_bd:3c:23    d2:f3:08:9a:34:bb  ARP      42 Who has 172.30.0.10? Tell 172.30.0.2
   32 21.564200   d2:f3:08:9a:34:bb  Vmware_bd:3c:23    ARP      60 172.30.0.10 is at d2:f3:08:9a:34:bb
   33 21.857698   d2:f3:08:9a:34:bb  Vmware_bd:3c:23    ARP      60 Who has 172.30.0.2? Tell 172.30.0.10
   34 21.857722   Vmware_bd:3c:23    d2:f3:08:9a:34:bb  ARP      42 172.30.0.2 is at 00:50:56:bd:3c:23
   71 24.290280   Vmware_bd:d0:d0    Broadcast          RARP     60 Who is 00:50:56:bd:d0:d0? Tell 00:50:56:bd:d0:d0
   72 24.290283   Vmware_bd:d0:d0    Broadcast          RARP     60 Who is 00:50:56:bd:d0:d0? Tell 00:50:56:bd:d0:d0
   73 24.357621   d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.10? Tell 0.0.0.0
   74 25.002397   d2:f3:06:5a:34:bb  Broadcast          RARP     60 Who is d2:f3:06:5a:34:bb? Tell d2:f3:06:5a:34:bb
   77 25.357671   d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.10? Tell 0.0.0.0
   78 26.357695   d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.10? Tell 0.0.0.0
   79 27.357728   d2:f3:06:5a:34:bb  Broadcast          ARP      60 Gratuitous ARP for 172.30.0.10 (Request) (duplicate use of 172.30.0.10
   86 27.857713   d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 det
   88 27.857822   Vmware_bd:e5:c3    d2:f3:06:5a:34:bb  ARP      60 172.30.0.1 is at 00:50:56:bd:e5:c3 (duplicate use of 172.30.0.10 detec
  106 31.003010   d2:f3:06:5a:34:bb  Broadcast          RARP     60 Who is d2:f3:06:5a:34:bb? Tell d2:f3:06:5a:34:bb
```

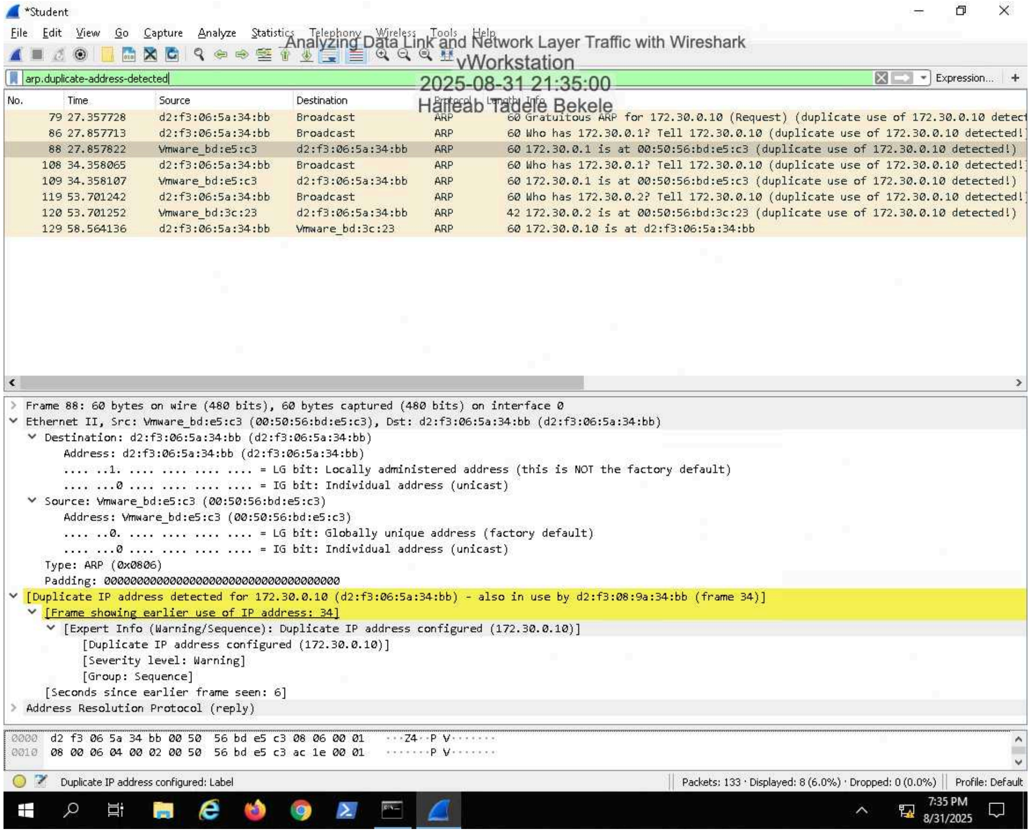
```
> Frame 88: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3), Dst: d2:f3:06:5a:34:bb (d2:f3:06:5a:34:bb)
  v Destination: d2:f3:06:5a:34:bb (d2:f3:06:5a:34:bb)
      Address: d2:f3:06:5a:34:bb (d2:f3:06:5a:34:bb)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
      Address: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v [Duplicate IP address detected for 172.30.0.10 (d2:f3:06:5a:34:bb) - also in use by d2:f3:08:9a:34:bb (frame 34)]
  v [Frame showing earlier use of IP address: 34]
    v [Expert Info (Warning/Sequence): Duplicate IP address configured (172.30.0.10)]
        [Duplicate IP address configured (172.30.0.10)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 6]
> Address Resolution Protocol (reply)
```

```
0000  d2 f3 06 5a 34 bb 00 50  56 bd e5 c3 08 06 00 01   ···Z4··P V·······
0010  08 00 06 04 00 02 00 50  56 bd e5 c3 ac 1e 00 01   ·······P V·······
```

wireshark_Student_20250831193225_a01780.pcapng | Packets: 133 · Displayed: 26 (19.5%) · Dropped: 0 (0.0%) | Profile: Default

7:34 PM
8/31/2025

29. **Make a screen capture** showing **all duplicate IP address detections in the Packet List pane**.



*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 21:35:00
Haileab Tadele Bekele

arp.duplicate-address-detected

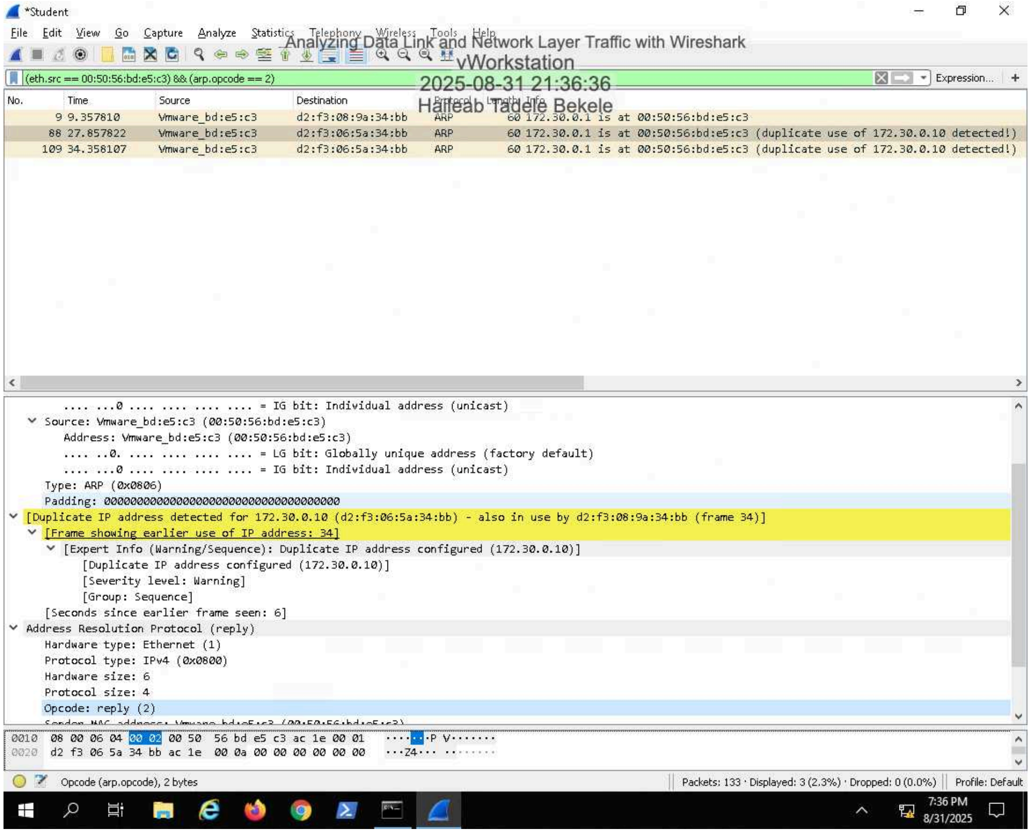
```
No.    Time       Source             Destination        Protocol Length Info
    79 27.357728  d2:f3:06:5a:34:bb  Broadcast          ARP      60 Gratuitous ARP for 172.30.0.10 (Request) (duplicate use of 172.30.0.10 detect
    86 27.857713  d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!
    88 27.857822  Vmware_bd:e5:c3    d2:f3:06:5a:34:bb  ARP      60 172.30.0.1 is at 00:50:56:bd:e5:c3 (duplicate use of 172.30.0.10 detected!)
   108 34.358065  d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!
   109 34.358107  Vmware_bd:e5:c3    d2:f3:06:5a:34:bb  ARP      60 172.30.0.1 is at 00:50:56:bd:e5:c3 (duplicate use of 172.30.0.10 detected!)
   119 53.701242  d2:f3:06:5a:34:bb  Broadcast          ARP      60 Who has 172.30.0.2? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!
   120 53.701252  Vmware_bd:3c:23    d2:f3:06:5a:34:bb  ARP      42 172.30.0.2 is at 00:50:56:bd:3c:23 (duplicate use of 172.30.0.10 detected!)
   129 58.564136  d2:f3:06:5a:34:bb  Vmware_bd:3c:23    ARP      60 172.30.0.10 is at d2:f3:06:5a:34:bb
```

```
> Frame 88: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3), Dst: d2:f3:06:5a:34:bb (d2:f3:06:5a:34:bb)
  v Destination: d2:f3:06:5a:34:bb (d2:f3:06:5a:34:bb)
      Address: d2:f3:06:5a:34:bb (d2:f3:06:5a:34:bb)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
      Address: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v [Duplicate IP address detected for 172.30.0.10 (d2:f3:06:5a:34:bb) - also in use by d2:f3:08:9a:34:bb (frame 34)]
  v [Frame showing earlier use of IP address: 34]
    v [Expert Info (Warning/Sequence): Duplicate IP address configured (172.30.0.10)]
        [Duplicate IP address configured (172.30.0.10)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 6]
> Address Resolution Protocol (reply)
```

```
0000  d2 f3 06 5a 34 bb 00 50  56 bd e5 c3 08 06 00 01   ···Z4··P V·······
0010  08 00 06 04 00 02 00 50  56 bd e5 c3 ac 1e 00 01   ·······P V·······
```

Duplicate IP address configured: Label | Packets: 133 · Displayed: 8 (6.0%) · Dropped: 0 (0.0%) | Profile: Default

34. **Make a screen capture** showing the **filtered ARP packets in the Packet List View**.



*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
(eth.src == 00:50:56:bd:e5:c3) && (arp.opcode == 2)
```

```
No.   Time       Source             Destination         Protocol  Length  Info
    9 9.357810   Vmware_bd:e5:c3    d2:f3:08:9a:34:bb   ARP           60  172.30.0.1 is at 00:50:56:bd:e5:c3
   88 27.857822  Vmware_bd:e5:c3    d2:f3:06:5a:34:bb   ARP           60  172.30.0.1 is at 00:50:56:bd:e5:c3 (duplicate use of 172.30.0.10 detected!)
  109 34.358107  Vmware_bd:e5:c3    d2:f3:06:5a:34:bb   ARP           60  172.30.0.1 is at 00:50:56:bd:e5:c3 (duplicate use of 172.30.0.10 detected!)
```

```
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
        Address: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
[Duplicate IP address detected for 172.30.0.10 (d2:f3:06:5a:34:bb) - also in use by d2:f3:08:9a:34:bb (frame 34)]
    [Frame showing earlier use of IP address: 34]
        [Expert Info (Warning/Sequence): Duplicate IP address configured (172.30.0.10)]
            [Duplicate IP address configured (172.30.0.10)]
            [Severity level: Warning]
            [Group: Sequence]
    [Seconds since earlier frame seen: 6]
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Vmware_bd:e5:c3 (00:50:56:bd:e5:c3)
```

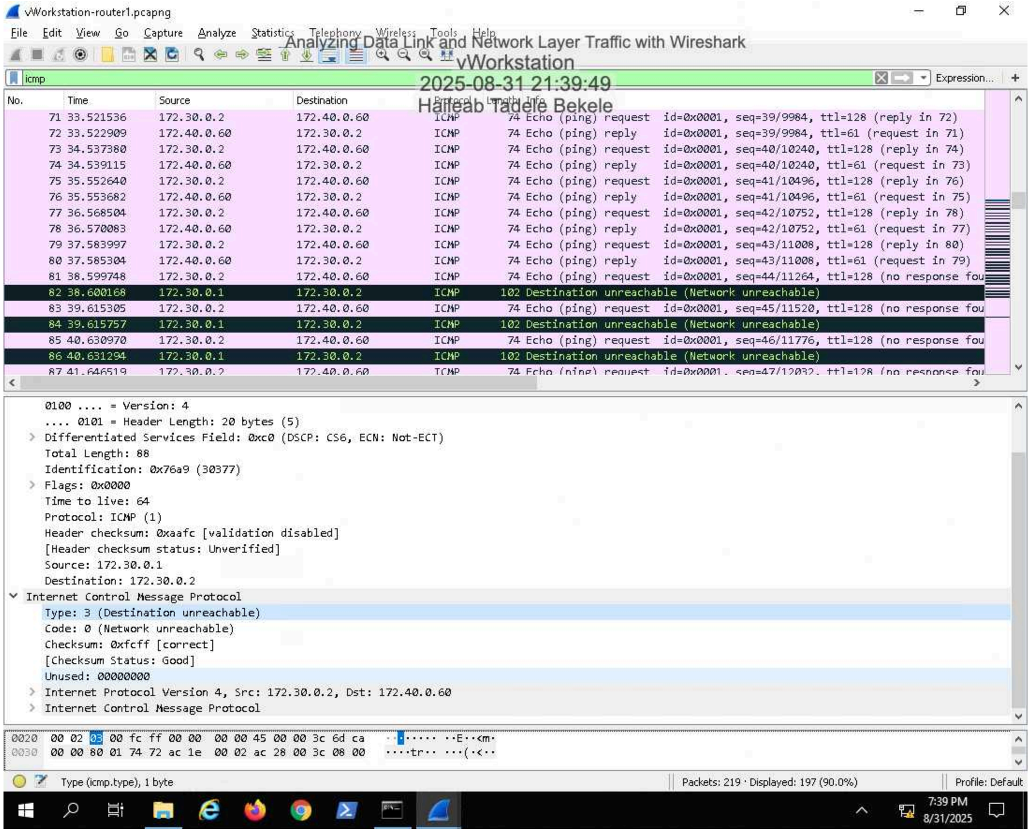
```
0010  08 00 06 04 00 02 00 50  56 bd e5 c3 ac 1e 00 01   ······P V·······
0020  d2 f3 06 5a 34 bb ac 1e  00 0a 00 00 00 00 00 00   ···Z4··· ········
```

Opcode (arp.opcode), 2 bytes | Packets: 133 · Displayed: 3 (2.3%) · Dropped: 0 (0.0%) | Profile: Default

7:36 PM
8/31/2025

Part 2: Explore a Wireshark Capture File

5. **Make a screen capture** showing the **ICMP Type for this packet (Destination unreachable)**.



vWorkstation-router1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 21:39:49
Haileab Tadele Bekele
icmp
Expression...
+

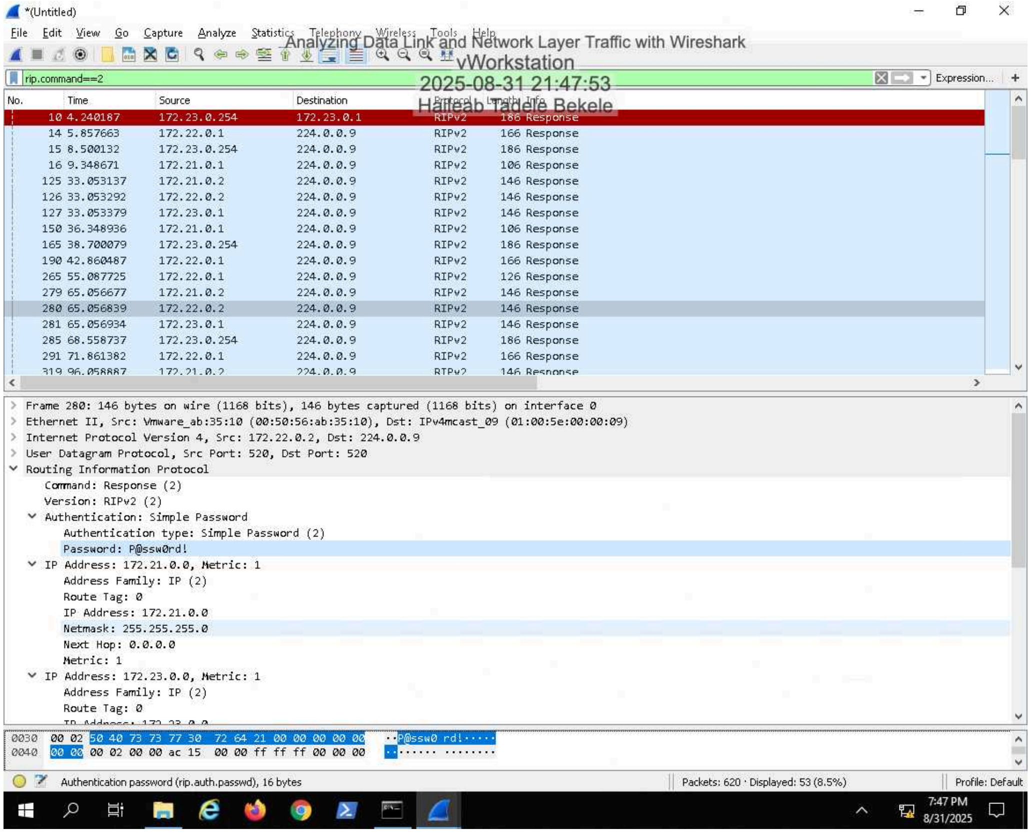
```
No.   Time        Source        Destination   Protocol Length Info
   71 33.521536   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=39/9984, ttl=128 (reply in 72)
   72 33.522909   172.40.0.60   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=39/9984, ttl=61 (request in 71)
   73 34.537380   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=40/10240, ttl=128 (reply in 74)
   74 34.539115   172.40.0.60   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=61 (request in 73)
   75 35.552640   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=41/10496, ttl=128 (reply in 76)
   76 35.553682   172.40.0.60   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=41/10496, ttl=61 (request in 75)
   77 36.568504   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=42/10752, ttl=128 (reply in 78)
   78 36.570083   172.40.0.60   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=42/10752, ttl=61 (request in 77)
   79 37.583997   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=43/11008, ttl=128 (reply in 80)
   80 37.585304   172.40.0.60   172.30.0.2    ICMP      74 Echo (ping) reply    id=0x0001, seq=43/11008, ttl=61 (request in 79)
   81 38.599748   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=44/11264, ttl=128 (no response fou
   82 38.600168   172.30.0.1    172.30.0.2    ICMP     102 Destination unreachable (Network unreachable)
   83 39.615305   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=45/11520, ttl=128 (no response fou
   84 39.615757   172.30.0.1    172.30.0.2    ICMP     102 Destination unreachable (Network unreachable)
   85 40.630970   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=46/11776, ttl=128 (no response fou
   86 40.631294   172.30.0.1    172.30.0.2    ICMP     102 Destination unreachable (Network unreachable)
   87 41.646519   172.30.0.2    172.40.0.60   ICMP      74 Echo (ping) request  id=0x0001, seq=47/12032, ttl=128 (no response fou
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 88
    Identification: 0x76a9 (30377)
  > Flags: 0x0000
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xaafc [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.0.1
    Destination: 172.30.0.2
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 0 (Network unreachable)
    Checksum: 0xfcff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.60
  > Internet Control Message Protocol
```

```
0020  00 02 03 00 fc ff 00 00  00 00 45 00 00 3c 6d ca   ········ ··E··<m·
0030  00 00 80 01 74 72 ac 1e  00 02 ac 28 00 3c 08 00   ····tr·· ···(·<··
```

Type (icmp.type), 1 byte | Packets: 219 · Displayed: 197 (90.0%) | Profile: Default

18. **Make a screen capture** showing the **simple password for packet 280**.


*(Untitled)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 21:47:53
Haileab Tadele Bekele
Expression...
7:47 PM
8/31/2025

rip.command==2

```
No.  Time        Source          Destination   Protocol  Length Info
  10 4.240187    172.23.0.254    172.23.0.1    RIPv2     186 Response
  14 5.857663    172.22.0.1      224.0.0.9     RIPv2     166 Response
  15 8.500132    172.23.0.254    224.0.0.9     RIPv2     186 Response
  16 9.348671    172.21.0.1      224.0.0.9     RIPv2     106 Response
 125 33.053137   172.21.0.2      224.0.0.9     RIPv2     146 Response
 126 33.053292   172.22.0.2      224.0.0.9     RIPv2     146 Response
 127 33.053379   172.23.0.1      224.0.0.9     RIPv2     146 Response
 150 36.348936   172.21.0.1      224.0.0.9     RIPv2     106 Response
 165 38.700079   172.23.0.254    224.0.0.9     RIPv2     186 Response
 190 42.860487   172.22.0.1      224.0.0.9     RIPv2     166 Response
 265 55.087725   172.22.0.1      224.0.0.9     RIPv2     126 Response
 279 65.056677   172.21.0.2      224.0.0.9     RIPv2     146 Response
 280 65.056839   172.22.0.2      224.0.0.9     RIPv2     146 Response
 281 65.056934   172.23.0.1      224.0.0.9     RIPv2     146 Response
 285 68.558737   172.23.0.254    224.0.0.9     RIPv2     186 Response
 291 71.861382   172.22.0.1      224.0.0.9     RIPv2     166 Response
 319 96.058887   172.21.0.2      224.0.0.9     RIPv2     146 Response
```

```
> Frame 280: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
> Ethernet II, Src: Vmware_ab:35:10 (00:50:56:ab:35:10), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 172.22.0.2, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  v Authentication: Simple Password
      Authentication type: Simple Password (2)
      Password: P@ssw0rd!
  v IP Address: 172.21.0.0, Metric: 1
      Address Family: IP (2)
      Route Tag: 0
      IP Address: 172.21.0.0
      Netmask: 255.255.255.0
      Next Hop: 0.0.0.0
      Metric: 1
  v IP Address: 172.23.0.0, Metric: 1
      Address Family: IP (2)
      Route Tag: 0
      IP Address: 172.23.0.0
```

```
0030  00 02 50 40 73 73 77 30  72 64 21 00 00 00 00 00   ··P@ssw0 rd!·····
0040  00 00 00 02 00 00 ac 15  00 00 ff ff ff 00 00 00   ········ ········
```

Authentication password (rip.auth.passwd), 16 bytes | Packets: 620 · Displayed: 53 (8.5%) | Profile: Default

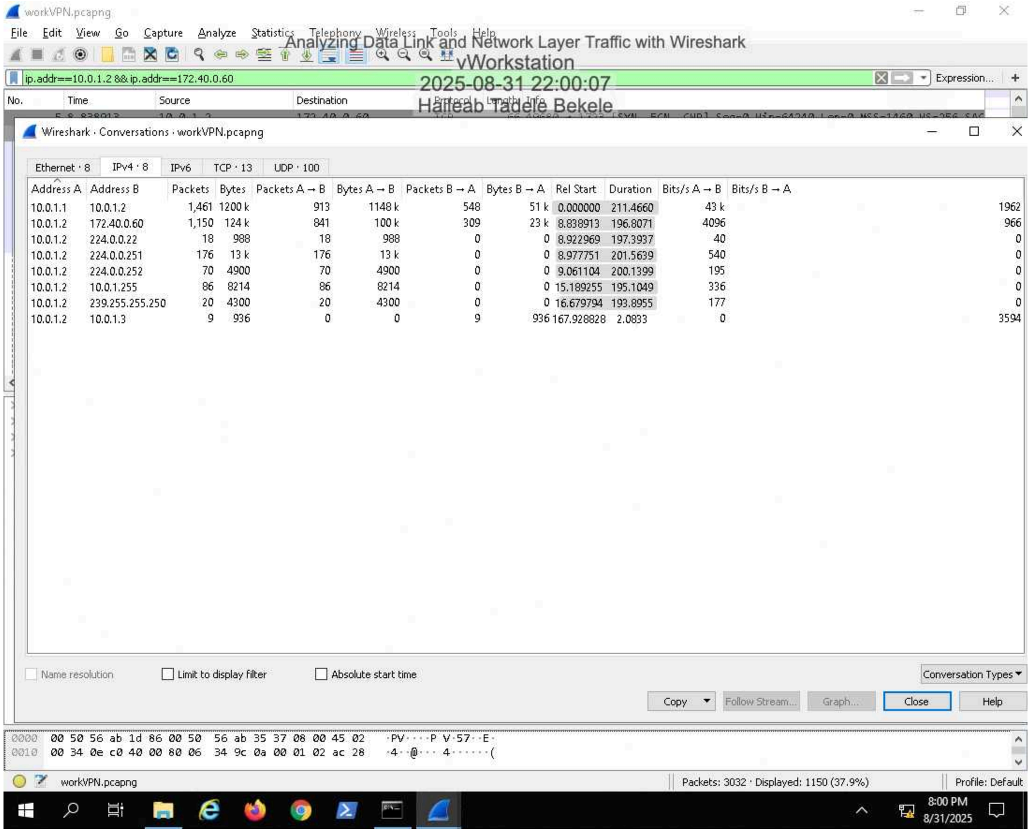
25. **Record** the number of the packet that contains the first corrected RIPv2 simple password**.**

P@ssw0rd!

Section 3: Challenge and Analysis

Part 1: Identify a Rogue Host in a Packet Capture File

Make a screen capture showing the **Packet List View with your applied conversation filter**.


workVPN.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
No. Time Source Destination Protocol Length Info
Wireshark · Conversations · workVPN.pcapng
Ethernet · 8
IPv4 · 8
IPv6
TCP · 13
UDP · 100
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help
8:00 PM
8/31/2025

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 22:00:07
Haileab Tadele Bekele

ip.addr==10.0.1.2 && ip.addr==172.40.0.60

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.0.1.1	10.0.1.2	1,461	1200 k	913	1148 k	548	51 k	0.000000	211.4660	43 k	1962
10.0.1.2	172.40.0.60	1,150	124 k	841	100 k	309	23 k	8.838913	196.8071	4096	966
10.0.1.2	224.0.0.22	18	988	18	988	0	0	8.922969	197.3937	40	0
10.0.1.2	224.0.0.251	176	13 k	176	13 k	0	0	8.977751	201.5639	540	0
10.0.1.2	224.0.0.252	70	4900	70	4900	0	0	9.061104	200.1399	195	0
10.0.1.2	10.0.1.255	86	8214	86	8214	0	0	15.189255	195.1049	336	0
10.0.1.2	239.255.255.250	20	4300	20	4300	0	0	16.679794	193.8955	177	0
10.0.1.2	10.0.1.3	9	936	0	0	9	936	167.928828	2.0833	0	3594

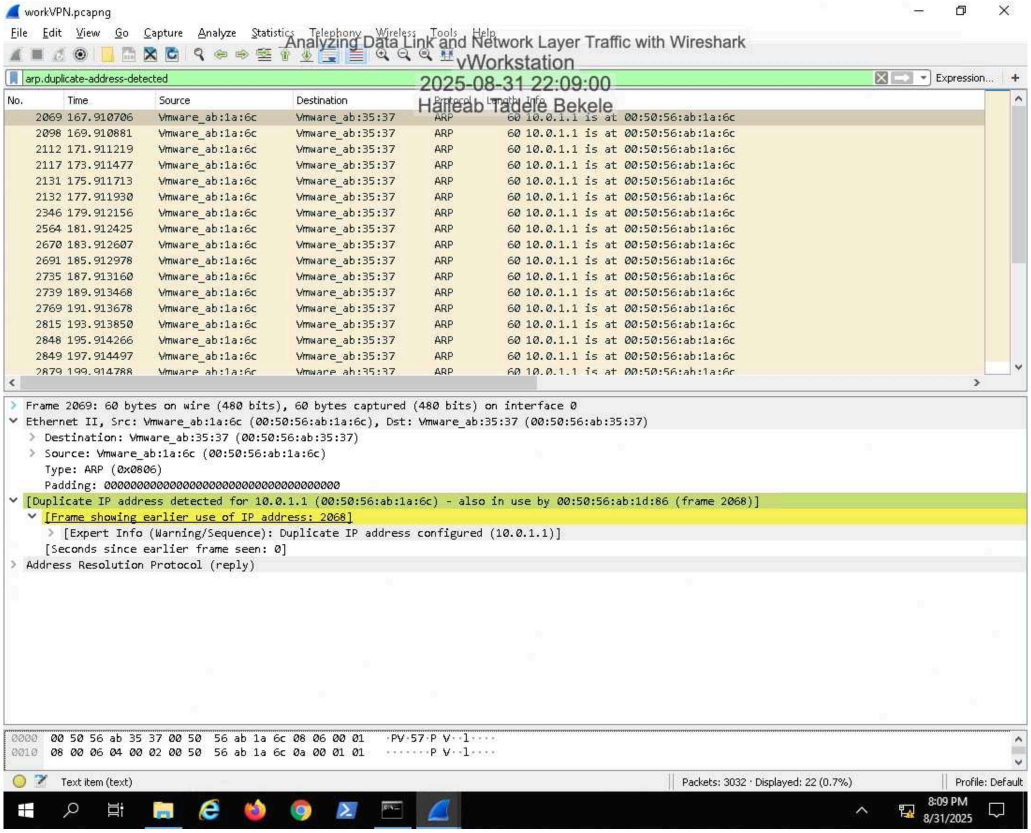
□ Name resolution □ Limit to display filter □ Absolute start time

```
0000  00 50 56 ab 1d 86 00 50  56 ab 35 37 08 00 45 02   ·PV····P V·57··E·
0010  00 34 0e c0 40 00 80 06  34 9c 0a 00 01 02 ac 28   ·4··@··· 4······(
```

workVPN.pcapng | Packets: 3032 · Displayed: 1150 (37.9%) | Profile: Default

Part 2: Detect an ARP Poisoning Event in a Packet Capture File

Make a screen capture showing the **“Duplicate IP address detected for…” details in the Packet Details View**.


workVPN.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 22:09:00
Haileab Tadele Bekele
Expression…
Text item (text)
Packets: 3032 · Displayed: 22 (0.7%)
Profile: Default
8:09 PM
8/31/2025

arp.duplicate-address-detected

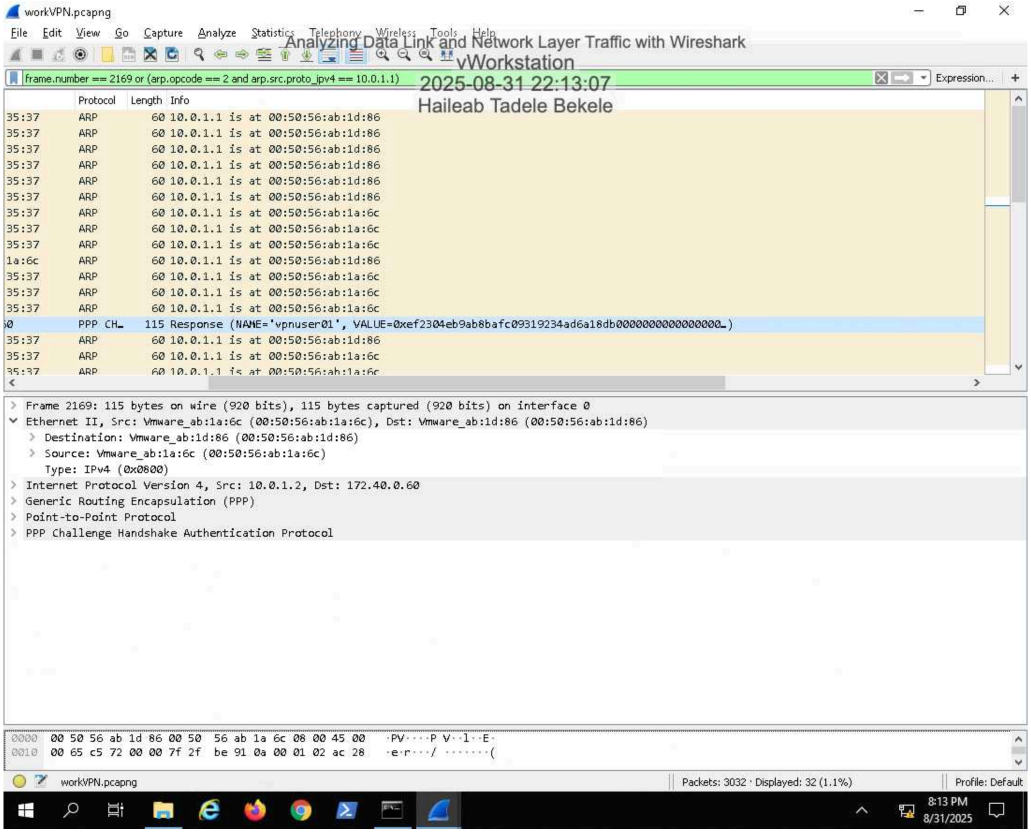
```
No.   Time        Source            Destination       Protocol Length Info
 2069 167.910706  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2098 169.910881  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2112 171.911219  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2117 173.911477  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2131 175.911713  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2132 177.911930  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2346 179.912156  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2564 181.912425  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2670 183.912607  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2691 185.912978  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2735 187.913160  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2739 189.913468  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2769 191.913678  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2815 193.913850  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2848 195.914266  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2849 197.914497  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2879 199.914788  Vmware_ab:1a:6c   Vmware_ab:35:37   ARP      60 10.0.1.1 is at 00:50:56:ab:1a:6c
```

```
> Frame 2069: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: Vmware_ab:1a:6c (00:50:56:ab:1a:6c), Dst: Vmware_ab:35:37 (00:50:56:ab:35:37)
  > Destination: Vmware_ab:35:37 (00:50:56:ab:35:37)
  > Source: Vmware_ab:1a:6c (00:50:56:ab:1a:6c)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v [Duplicate IP address detected for 10.0.1.1 (00:50:56:ab:1a:6c) - also in use by 00:50:56:ab:1d:86 (frame 2068)]
  v [Frame showing earlier use of IP address: 2068]
    > [Expert Info (Warning/Sequence): Duplicate IP address configured (10.0.1.1)]
    [Seconds since earlier frame seen: 0]
> Address Resolution Protocol (reply)
```

```
0000  00 50 56 ab 35 37 00 50  56 ab 1a 6c 08 06 00 01   ·PV·57·P V··l····
0010  08 00 06 04 00 02 00 50  56 ab 1a 6c 0a 00 01 01   ·······P V··l····
```

Part 3: Determine if VPN Login Information was Compromised

Make a screen capture showing the **ARP responses that came before the login packet**.


workVPN.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-08-31 22:13:07
Haileab Tadele Bekele

```
frame.number == 2169 or (arp.opcode == 2 and arp.src.proto_ipv4 == 10.0.1.1)
```

```
         Protocol  Length Info
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
1a:6c    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
60       PPP CH…     115 Response (NAME='vpnuser01', VALUE=0xef2304eb9ab8bafc09319234ad6a18db0000000000000000…)
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1d:86
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
35:37    ARP          60 10.0.1.1 is at 00:50:56:ab:1a:6c
```

```
> Frame 2169: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 0
v Ethernet II, Src: Vmware_ab:1a:6c (00:50:56:ab:1a:6c), Dst: Vmware_ab:1d:86 (00:50:56:ab:1d:86)
  > Destination: Vmware_ab:1d:86 (00:50:56:ab:1d:86)
  > Source: Vmware_ab:1a:6c (00:50:56:ab:1a:6c)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.0.1.2, Dst: 172.40.0.60
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
> PPP Challenge Handshake Authentication Protocol
```

```
0000  00 50 56 ab 1d 86 00 50  56 ab 1a 6c 08 00 45 00   ·PV····P V··l··E·
0010  00 65 c5 72 00 00 7f 2f  be 91 0a 00 01 02 ac 28   ·e·r···/ ·······(
```

workVPN.pcapng | Packets: 3032 · Displayed: 32 (1.1%) | Profile: Default

8:13 PM
8/31/2025