Analyzing Data Link and Network Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 02

Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

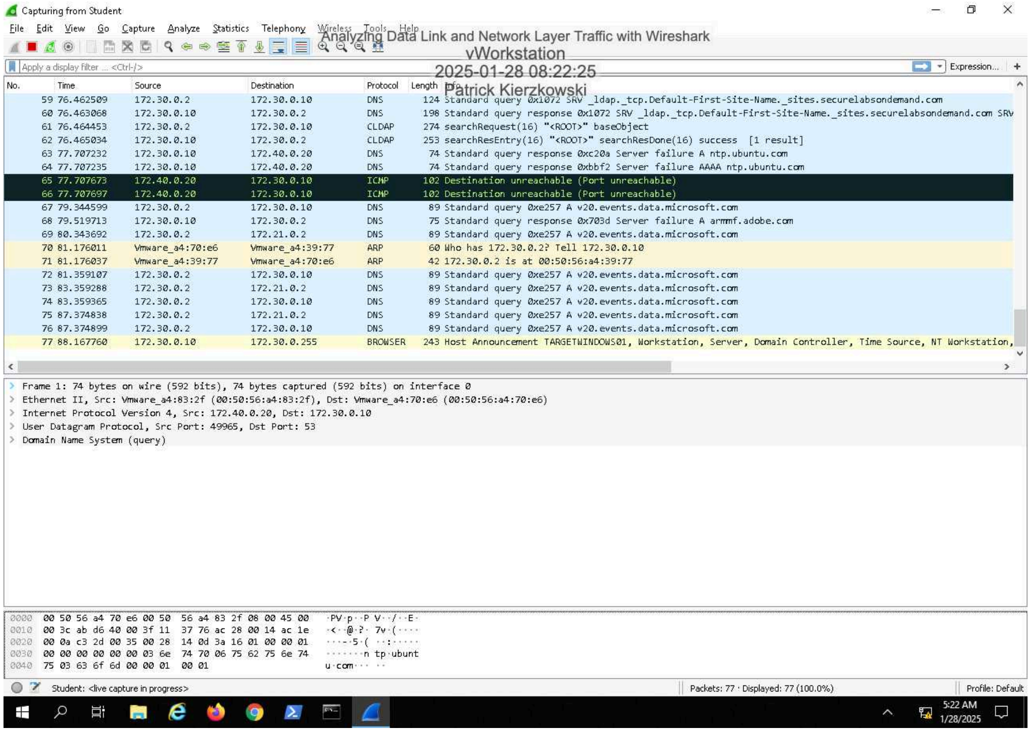
Time on Task:	Progress:
23 hours, 21 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:45 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**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 08:22:25
Patrick Kierzkowski

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

```
No.  Time       Source           Destination      Protocol  Length Info
  59 76.462509  172.30.0.2       172.30.0.10      DNS       124 Standard query 0x1072 SRV _ldap._tcp.Default-First-Site-Name._sites.securelabsondemand.com
  60 76.463068  172.30.0.10      172.30.0.2       DNS       198 Standard query response 0x1072 SRV _ldap._tcp.Default-First-Site-Name._sites.securelabsondemand.com SRV
  61 76.464453  172.30.0.2       172.30.0.10      CLDAP     274 searchRequest(16) "<ROOT>" baseObject
  62 76.465034  172.30.0.10      172.30.0.2       CLDAP     253 searchResEntry(16) "<ROOT>" searchResDone(16) success  [1 result]
  63 77.707232  172.30.0.10      172.40.0.20      DNS        74 Standard query response 0xc20a Server failure A ntp.ubuntu.com
  64 77.707235  172.30.0.10      172.40.0.20      DNS        74 Standard query response 0xbbf2 Server failure AAAA ntp.ubuntu.com
  65 77.707673  172.40.0.20      172.30.0.10      ICMP      102 Destination unreachable (Port unreachable)
  66 77.707697  172.40.0.20      172.30.0.10      ICMP      102 Destination unreachable (Port unreachable)
  67 79.344599  172.30.0.2       172.30.0.10      DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  68 79.519713  172.30.0.10      172.30.0.2       DNS        75 Standard query response 0x703d Server failure A armmf.adobe.com
  69 80.343692  172.30.0.2       172.21.0.2       DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  70 81.176011  Vmware_a4:70:e6  Vmware_a4:39:77  ARP        60 Who has 172.30.0.2? Tell 172.30.0.10
  71 81.176037  Vmware_a4:39:77  Vmware_a4:70:e6  ARP        42 172.30.0.2 is at 00:50:56:a4:39:77
  72 81.359107  172.30.0.2       172.30.0.10      DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  73 83.359288  172.30.0.2       172.21.0.2       DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  74 83.359365  172.30.0.2       172.30.0.10      DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  75 87.374838  172.30.0.2       172.21.0.2       DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  76 87.374899  172.30.0.2       172.30.0.10      DNS        89 Standard query 0xe257 A v20.events.data.microsoft.com
  77 88.167760  172.30.0.10      172.30.0.255     BROWSER   243 Host Announcement TARGETWINDOWS01, Workstation, Server, Domain Controller, Time Source, NT Workstation,
```

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_a4:83:2f (00:50:56:a4:83:2f), Dst: Vmware_a4:70:e6 (00:50:56:a4:70:e6)
> Internet Protocol Version 4, Src: 172.40.0.20, Dst: 172.30.0.10
> User Datagram Protocol, Src Port: 49965, Dst Port: 53
> Domain Name System (query)
```

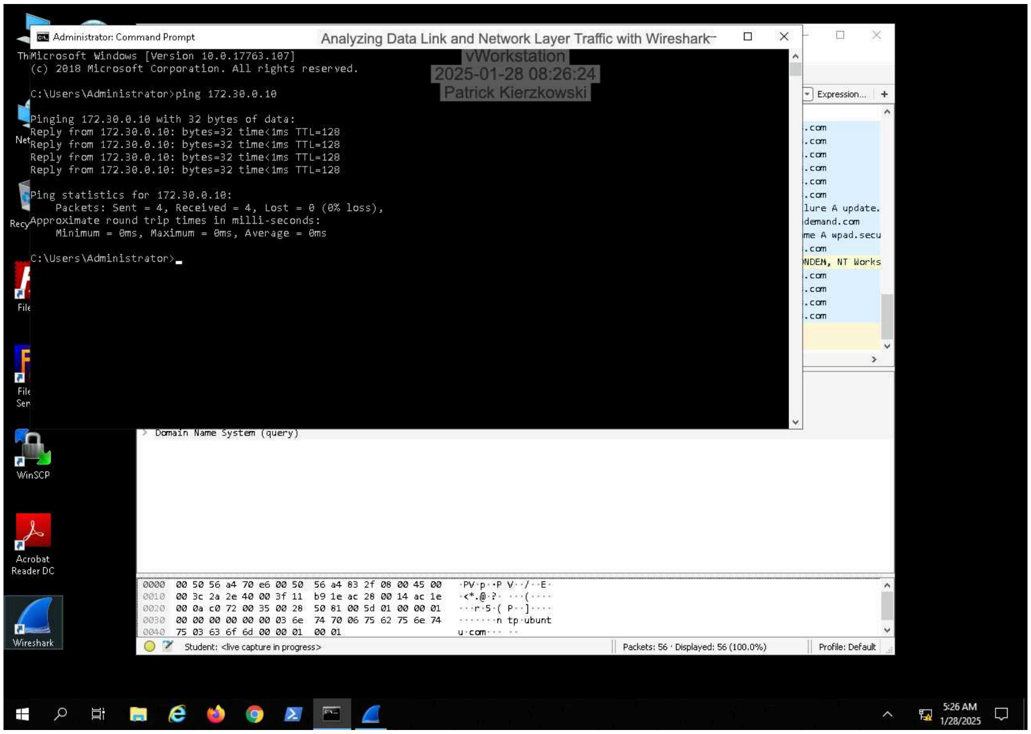
```
0000  00 50 56 a4 70 e6 00 50  56 a4 83 2f 08 00 45 00   ·PV·p··P V··/··E·
0010  00 3c ab d6 40 00 3f 11  37 76 ac 28 00 14 ac 1e   ·<··@·?· 7v·(····
0020  00 0a c3 2d 00 35 00 28  14 0d 3a 16 01 00 00 01   ···-·5·( ··:·····
0030  00 00 00 00 00 00 03 6e  74 70 06 75 62 75 6e 74   ·······n tp·ubunt
0040  75 03 63 6f 6d 00 00 01  00 01                     u·com··· ··
```

Student: <live capture in progress>

Packets: 77 · Displayed: 77 (100.0%)

Profile: Default

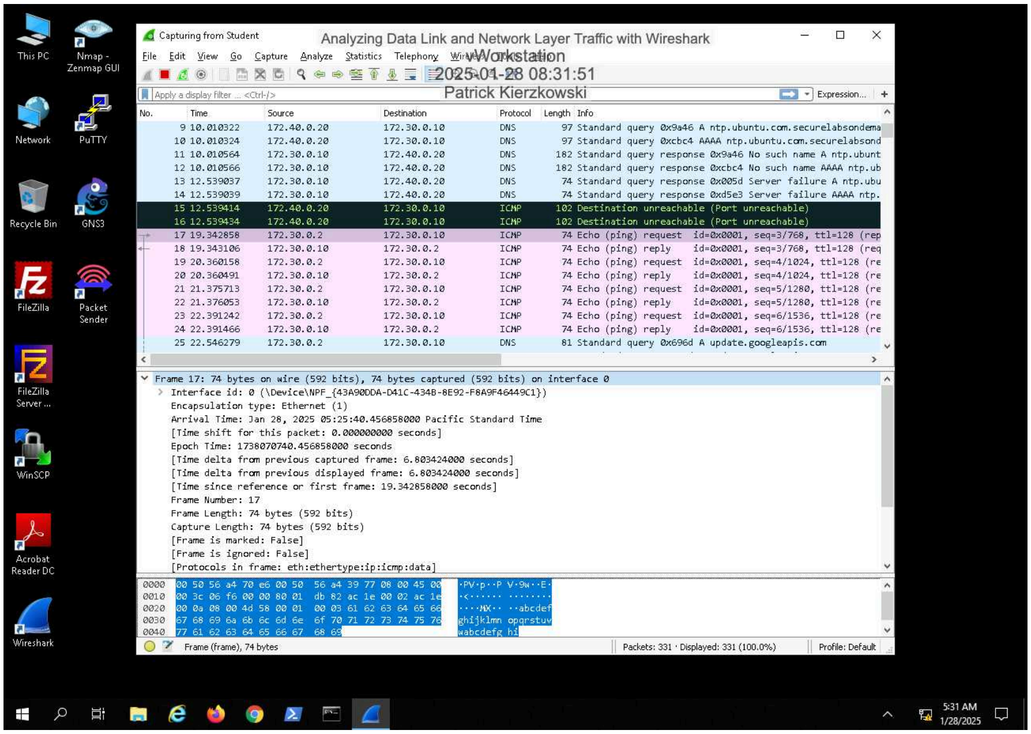
9. **Make a screen capture** showing the **Ping results for 170.30.0.10**.


Administrator: Command Prompt
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 08:26:24
Patrick Kierzkowski
Expression...
WinSCP
Acrobat Reader DC
Wireshark
Student: <live capture in progress>
Packets: 56 · Displayed: 56 (100.0%)
Profile: Default
5:26 AM
1/28/2025

```
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>_
```

```
> Domain Name System (query)

0000  00 50 56 a4 70 e6 00 50  56 a4 83 2f 08 00 45 00   ·PV·p··P V··/··E·
0010  00 3c 2a 2e 40 00 3f 11  b9 1e ac 28 00 14 ac 1e   ·<*.@·?· ···(····
0020  00 0a c0 72 00 35 00 28  50 81 00 5d 01 00 00 01   ···r·5·( P··]····
0030  00 00 00 00 00 00 03 6e  74 70 06 75 62 75 6e 74   ·······n tp·ubunt
0040  75 03 63 6f 6d 00 00 01  00 01                     u·com··· ··
```

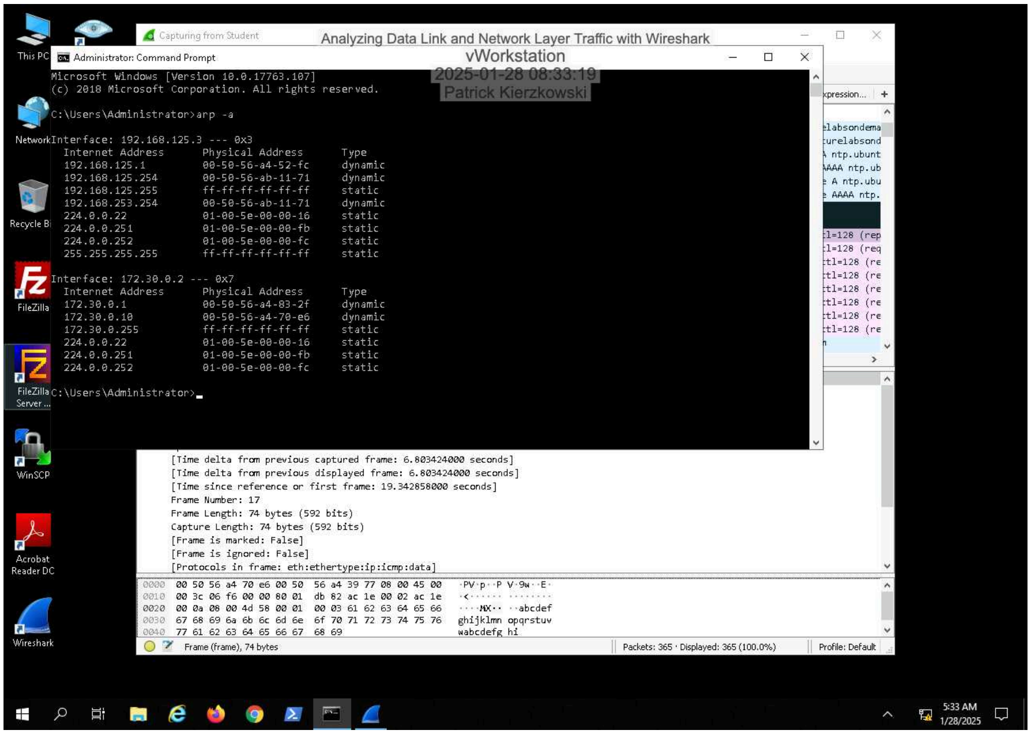
14. **Make a screen capture** showing the **Packet details related to time**.



```
No.   Time       Source       Destination  Protocol Length Info
    9 10.010322  172.40.0.20  172.30.0.10  DNS       97 Standard query 0x9a46 A ntp.ubuntu.com.securelabsondema
   10 10.010324  172.40.0.20  172.30.0.10  DNS       97 Standard query 0xcbc4 AAAA ntp.ubuntu.com.securelabsond
   11 10.010564  172.30.0.10  172.40.0.20  DNS      182 Standard query response 0x9a46 No such name A ntp.ubunt
   12 10.010566  172.30.0.10  172.40.0.20  DNS      182 Standard query response 0xcbc4 No such name AAAA ntp.ub
   13 12.539037  172.30.0.10  172.40.0.20  DNS       74 Standard query response 0x005d Server failure A ntp.ubu
   14 12.539039  172.30.0.10  172.40.0.20  DNS       74 Standard query response 0xd5e3 Server failure AAAA ntp.
   15 12.539414  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   16 12.539434  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   17 19.342858  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (rep
   18 19.343106  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=128 (req
   19 20.360158  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (re
   20 20.360491  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=128 (re
   21 21.375713  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (re
   22 21.376053  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=128 (re
   23 22.391242  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (re
   24 22.391466  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=128 (re
   25 22.546279  172.30.0.2   172.30.0.10  DNS       81 Standard query 0x696d A update.googleapis.com
```

```
v Frame 17: 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: Jan 28, 2025 05:25:40.456858000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1738070740.456858000 seconds
    [Time delta from previous captured frame: 6.803424000 seconds]
    [Time delta from previous displayed frame: 6.803424000 seconds]
    [Time since reference or first frame: 19.342858000 seconds]
    Frame Number: 17
    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 a4 70 e6 00 50  56 a4 39 77 08 00 45 00   ·PV·p··P V·9w··E·
0010  00 3c 06 f6 00 00 80 01  db 82 ac 1e 00 02 ac 1e   ·<······ ········
0020  00 0a 08 00 4d 58 00 01  00 03 61 62 63 64 65 66   ····MX·· ··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
```

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



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 08:33:19
Patrick Kierzkowski

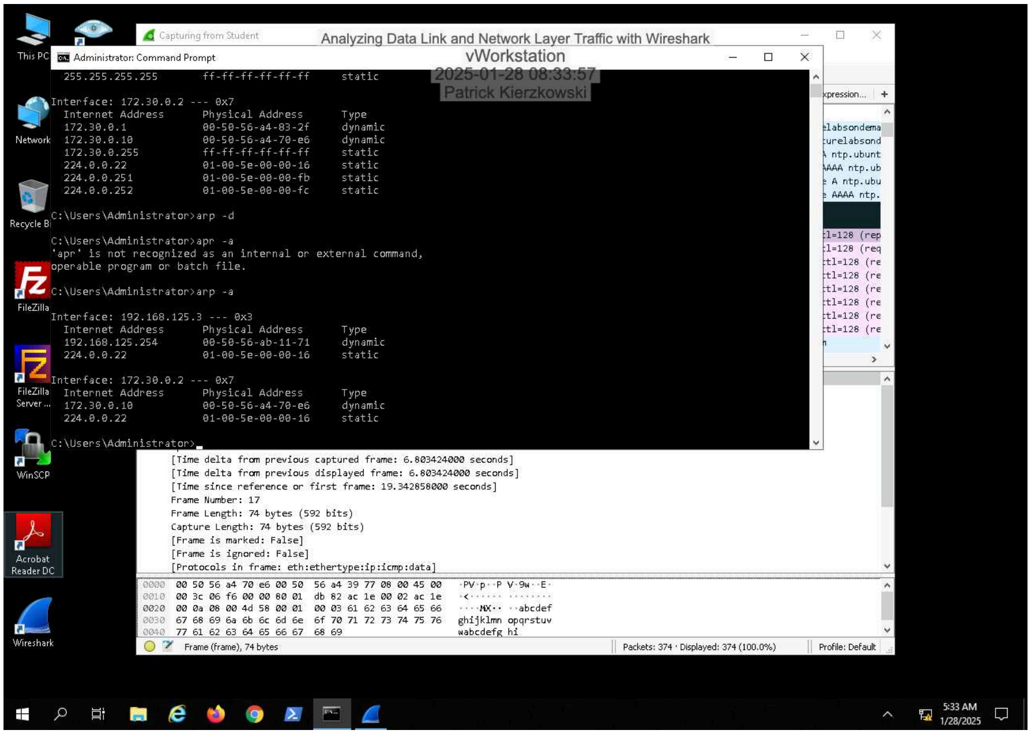
```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -a

Interface: 192.168.125.3 --- 0x3
  Internet Address      Physical Address      Type
  192.168.125.1         00-50-56-a4-52-fc     dynamic
  192.168.125.254       00-50-56-ab-11-71     dynamic
  192.168.125.255       ff-ff-ff-ff-ff-ff     static
  192.168.253.254       00-50-56-ab-11-71     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-a4-83-2f     dynamic
  172.30.0.10           00-50-56-a4-70-e6     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>_
```

```
[Time delta from previous captured frame: 6.803424000 seconds]
[Time delta from previous displayed frame: 6.803424000 seconds]
[Time since reference or first frame: 19.342858000 seconds]
Frame Number: 17
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 a4 70 e6 00 50  56 a4 39 77 08 00 45 00   ·PV·p··P V·9w··E·
0010  00 3c 06 f6 00 00 80 01  db 82 ac 1e 00 02 ac 1e   ·<······ ········
0020  00 0a 08 00 4d 58 00 01  00 03 61 62 63 64 65 66   ····MX·· ··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
```

Frame (frame), 74 bytes | Packets: 365 · Displayed: 365 (100.0%) | Profile: Default

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



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 08:33:57
Patrick Kierzkowski

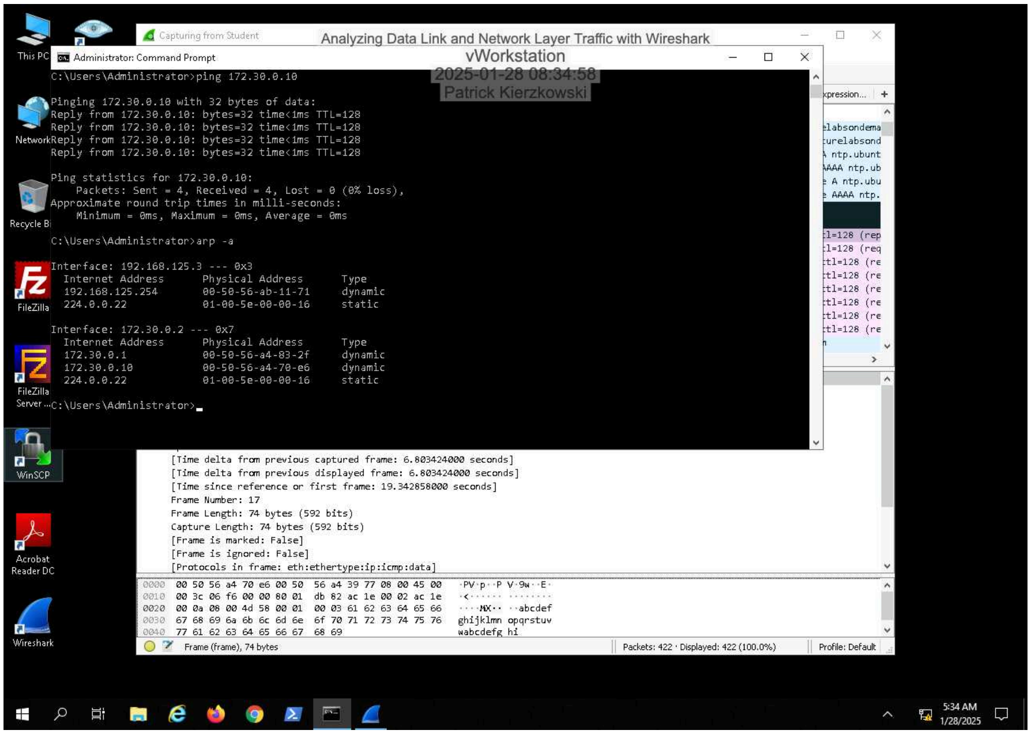
```
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.30.0.2 --- 0x7
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-a4-83-2f     dynamic
  172.30.0.10           00-50-56-a4-70-e6     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>apr -a
'apr' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>arp -a

Interface: 192.168.125.3 --- 0x3
  Internet Address      Physical Address      Type
  192.168.125.254       00-50-56-ab-11-71     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.30.0.2 --- 0x7
  Internet Address      Physical Address      Type
  172.30.0.10           00-50-56-a4-70-e6     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>_
```

```
[Time delta from previous captured frame: 6.803424000 seconds]
[Time delta from previous displayed frame: 6.803424000 seconds]
[Time since reference or first frame: 19.342858000 seconds]
Frame Number: 17
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 a4 70 e6 00 50  56 a4 39 77 08 00 45 00   ·PV·p··P V·9w··E·
0010  00 3c 06 f6 00 00 80 01  db 82 ac 1e 00 02 ac 1e   ·<······ ········
0020  00 0a 08 00 4d 58 00 01  00 03 61 62 63 64 65 66   ····MX·· ··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
```

Frame (frame), 74 bytes | Packets: 374 · Displayed: 374 (100.0%) | Profile: Default

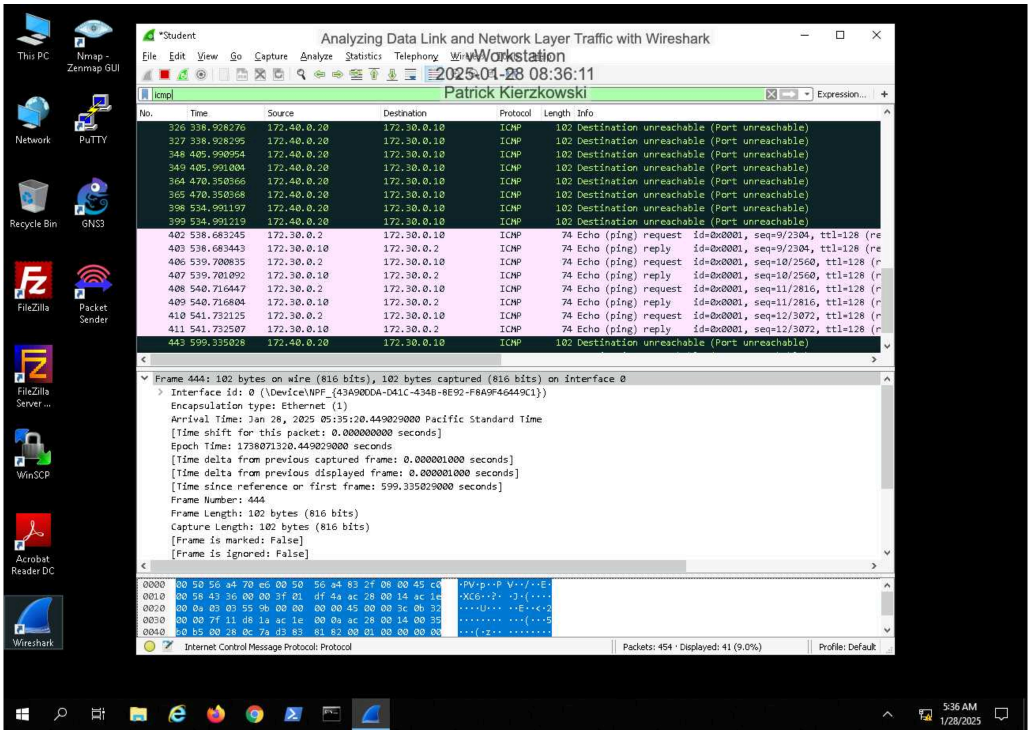
21. **Make a screen capture** showing the **updated ARP table with the new 172.30.0.10 entry**.



```
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>arp -a

Interface: 192.168.125.3 --- 0x3
  Internet Address      Physical Address      Type
  192.168.125.254       00-50-56-ab-11-71     dynamic
  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-a4-83-2f     dynamic
  172.30.0.10           00-50-56-a4-70-e6     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Users\Administrator>_
```

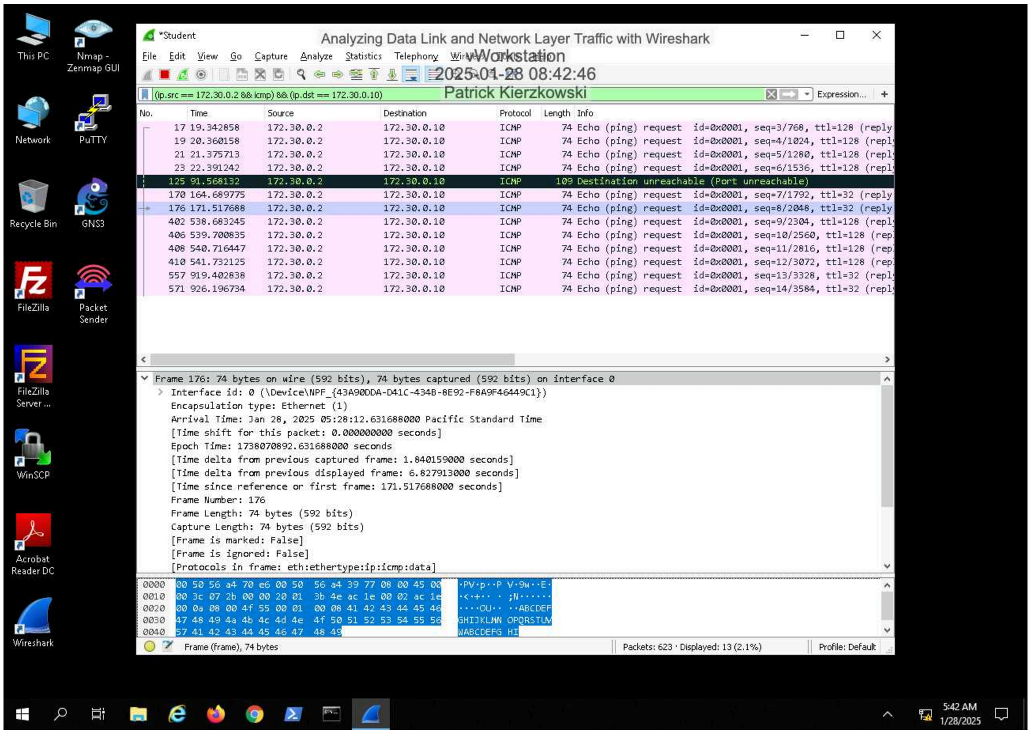
```
    [Time delta from previous captured frame: 6.803424000 seconds]
    [Time delta from previous displayed frame: 6.803424000 seconds]
    [Time since reference or first frame: 19.342858000 seconds]
    Frame Number: 17
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]

0000  00 50 56 a4 70 e6 00 50  56 a4 39 77 08 00 45 00   ·PV·p··P V·9w··E·
0010  00 3c 06 f6 00 00 80 01  db 82 ac 1e 00 02 ac 1e   ·<······ ········
0020  00 0a 08 00 4d 58 00 01  00 03 61 62 63 64 65 66   ····MX·· ··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

Frame (frame), 74 bytes    Packets: 422 · Displayed: 422 (100.0%)    Profile: Default
```

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



```
icmp

No.  Time        Source       Destination  Protocol Length Info
 326 338.928276  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 327 338.928295  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 348 405.990954  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 349 405.991004  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 364 470.350366  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 365 470.350368  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 398 534.991197  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 399 534.991219  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
 402 538.683245  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=128 (re
 403 538.683443  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=128 (re
 406 539.700835  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=128 (r
 407 539.701092  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=128 (r
 408 540.716447  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=128 (r
 409 540.716804  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=128 (r
 410 541.732125  172.30.0.2   172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (r
 411 541.732507  172.30.0.10  172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=128 (r
 443 599.335028  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)

v Frame 444: 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: Jan 28, 2025 05:35:20.449029000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1738071320.449029000 seconds
    [Time delta from previous captured frame: 0.000001000 seconds]
    [Time delta from previous displayed frame: 0.000001000 seconds]
    [Time since reference or first frame: 599.335029000 seconds]
    Frame Number: 444
    Frame Length: 102 bytes (816 bits)
    Capture Length: 102 bytes (816 bits)
    [Frame is marked: False]
    [Frame is ignored: False]

0000  00 50 56 a4 70 e6 00 50  56 a4 83 2f 08 00 45 c0   ·PV·p··P V··/··E·
0010  00 58 43 36 00 00 3f 01  df 4a ac 28 00 14 ac 1e   ·XC6··?· ·J·(····
0020  00 0a 03 03 55 9b 00 00  00 00 45 00 00 3c 0b 32   ····U··· ··E··<·2
0030  00 00 7f 11 d8 1a ac 1e  00 0a ac 28 00 14 00 35   ········ ···(···5
0040  b0 b5 00 28 0c 7a d3 83  81 82 00 01 00 00 00 00   ···(·z·· ········

Internet Control Message Protocol: Protocol    Packets: 454 · Displayed: 41 (9.0%)    Profile: Default
```

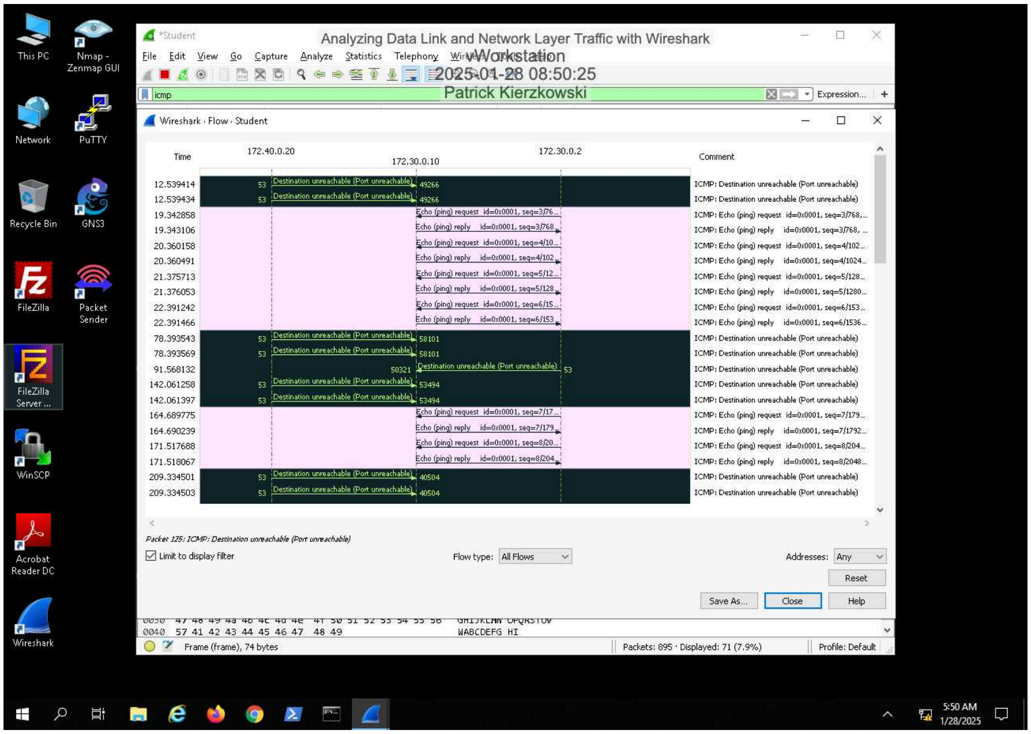
30. **Make a screen capture** showing the **ICMP Packets with the src of 172.30.0.2 and dst of 172.30.0.10**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 08:42:46
Patrick Kierzkowski

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

No.  Time        Source      Destination  Protocol Length Info
 17  19.342858   172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply
 19  20.360158   172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (repl
 21  21.375713   172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (repl
 23  22.391242   172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (repl
125  91.568132   172.30.0.2  172.30.0.10  ICMP     109 Destination unreachable (Port unreachable)
170  164.689775  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=32 (reply
176  171.517688  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=32 (reply
402  538.683245  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=128 (repl
406  539.700835  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=128 (rep
408  540.716447  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=128 (rep
410  541.732125  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (rep
557  919.402838  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=32 (repl
571  926.196734  172.30.0.2  172.30.0.10  ICMP      74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=32 (repl

Frame 176: 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: Jan 28, 2025 05:28:12.631688000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1738070892.631688000 seconds
    [Time delta from previous captured frame: 1.840159000 seconds]
    [Time delta from previous displayed frame: 6.827913000 seconds]
    [Time since reference or first frame: 171.517688000 seconds]
    Frame Number: 176
    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 a4 70 e6 00 50  56 a4 39 77 08 00 45 00   ·PV·p··P V·9w··E·
0010  00 3c 07 2b 00 00 20 01  3b 4e ac 1e 00 02 ac 1e   ·<·+·· · ;N······
0020  00 0a 08 00 4f 55 00 01  00 08 41 42 43 44 45 46   ····OU·· ··ABCDEF
0030  47 48 49 4a 4b 4c 4d 4e  4f 50 51 52 53 54 55 56   GHIJKLMN OPQRSTUV
0040  57 41 42 43 44 45 46 47  48 49                     WABCDEFG HI

Frame (frame), 74 bytes        Packets: 623 · Displayed: 13 (2.1%)        Profile: Default
```

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

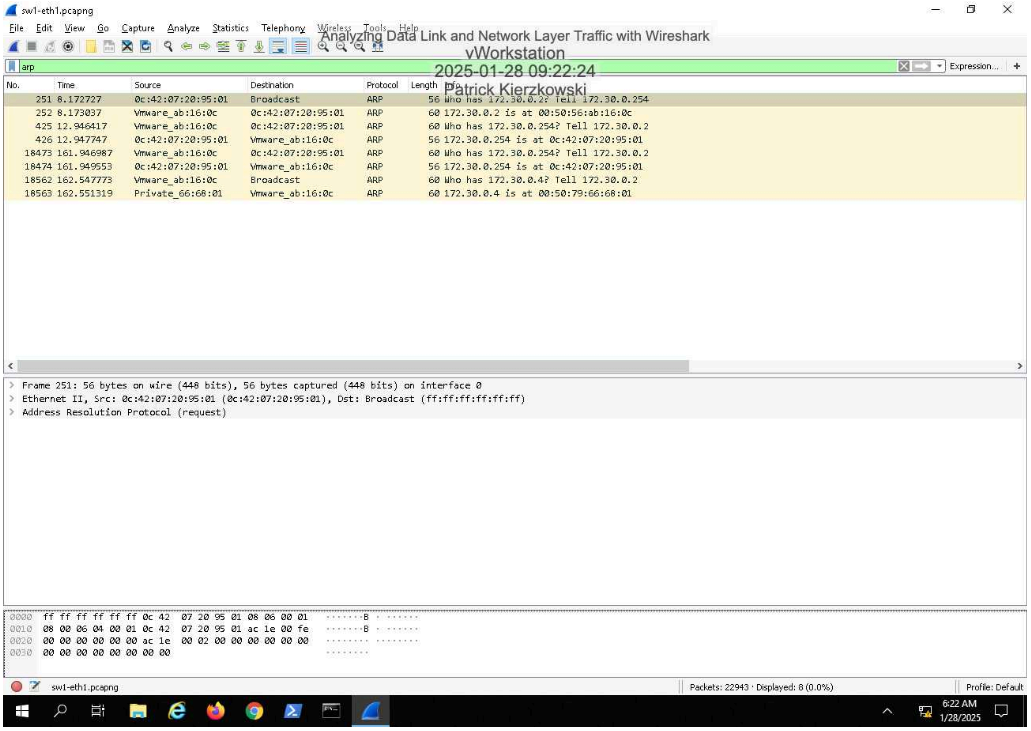


Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 08:50:25
Patrick Kierzkowski

```
icmp

Time        Flow                                                            Comment
12.539414   53 Destination unreachable (Port unreachable) 49266             ICMP: Destination unreachable (Port unreachable)
12.539434   53 Destination unreachable (Port unreachable) 49266             ICMP: Destination unreachable (Port unreachable)
19.342858   Echo (ping) request  id=0x0001, seq=3/76...                    ICMP: Echo (ping) request  id=0x0001, seq=3/768,...
19.343106   Echo (ping) reply    id=0x0001, seq=3/768...                   ICMP: Echo (ping) reply    id=0x0001, seq=3/768, ...
20.360158   Echo (ping) request  id=0x0001, seq=4/10...                    ICMP: Echo (ping) request  id=0x0001, seq=4/102...
20.360491   Echo (ping) reply    id=0x0001, seq=4/102...                   ICMP: Echo (ping) reply    id=0x0001, seq=4/1024...
21.375713   Echo (ping) request  id=0x0001, seq=5/12...                    ICMP: Echo (ping) request  id=0x0001, seq=5/128...
21.376053   Echo (ping) reply    id=0x0001, seq=5/128...                   ICMP: Echo (ping) reply    id=0x0001, seq=5/1280...
22.391242   Echo (ping) request  id=0x0001, seq=6/15...                    ICMP: Echo (ping) request  id=0x0001, seq=6/153...
22.391466   Echo (ping) reply    id=0x0001, seq=6/153...                   ICMP: Echo (ping) reply    id=0x0001, seq=6/1536...
78.393543   53 Destination unreachable (Port unreachable) 58101             ICMP: Destination unreachable (Port unreachable)
78.393569   53 Destination unreachable (Port unreachable) 58101             ICMP: Destination unreachable (Port unreachable)
91.568132   50321 Destination unreachable (Port unreachable) 53             ICMP: Destination unreachable (Port unreachable)
142.061258  53 Destination unreachable (Port unreachable) 53494             ICMP: Destination unreachable (Port unreachable)
142.061397  53 Destination unreachable (Port unreachable) 53494             ICMP: Destination unreachable (Port unreachable)
164.689775  Echo (ping) request  id=0x0001, seq=7/17...                    ICMP: Echo (ping) request  id=0x0001, seq=7/179...
164.690239  Echo (ping) reply    id=0x0001, seq=7/179...                   ICMP: Echo (ping) reply    id=0x0001, seq=7/1792...
171.517688  Echo (ping) request  id=0x0001, seq=8/20...                    ICMP: Echo (ping) request  id=0x0001, seq=8/204...
171.518067  Echo (ping) reply    id=0x0001, seq=8/204...                   ICMP: Echo (ping) reply    id=0x0001, seq=8/2048...
209.334501  53 Destination unreachable (Port unreachable) 40504             ICMP: Destination unreachable (Port unreachable)
209.334503  53 Destination unreachable (Port unreachable) 40504             ICMP: Destination unreachable (Port unreachable)

Packet 125: ICMP: Destination unreachable (Port unreachable)
☑ Limit to display filter        Flow type: All Flows        Addresses: Any
                                                              Reset

0030  47 48 49 4a 4b 4c 4d 4e  4f 50 51 52 53 54 55 56   GHIJKLMN OPQRSTUV
0040  57 41 42 43 44 45 46 47  48 49                     WABCDEFG HI

Frame (frame), 74 bytes        Packets: 895 · Displayed: 71 (7.9%)        Profile: Default
```

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...
+

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 09:22:24
Patrick Kierzkowski

Filter: 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
```

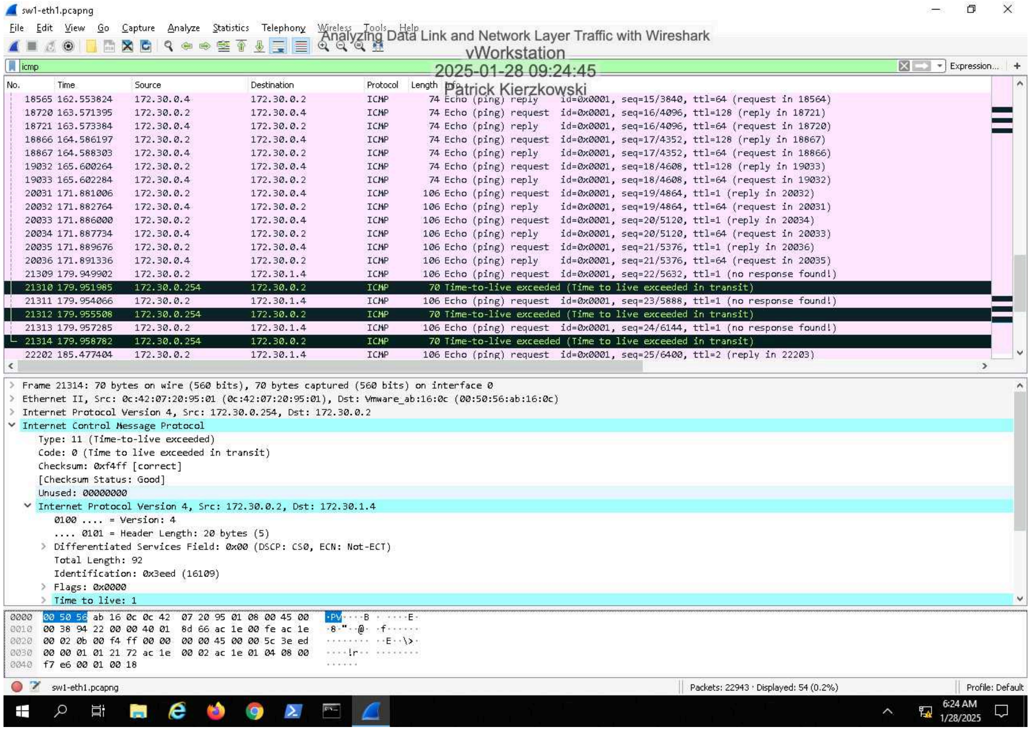
```
> Frame 251: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
> Ethernet II, Src: 0c:42:07:20:95:01 (0c:42:07:20:95:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
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

6:22 AM
1/28/2025

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



sw1-eth1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 09:24:45
Patrick Kierzkowski

Filter: icmp

```
No.     Time        Source        Destination  Protocol  Length Info
  18565 162.553824  172.30.0.4    172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=64 (request in 18564)
  18720 163.571395  172.30.0.2    172.30.0.4   ICMP      74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply in 18721)
  18721 163.573384  172.30.0.4    172.30.0.2   ICMP      74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=64 (request in 18720)
  18866 164.586197  172.30.0.2    172.30.0.4   ICMP      74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=128 (reply in 18867)
  18867 164.588303  172.30.0.4    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)
```

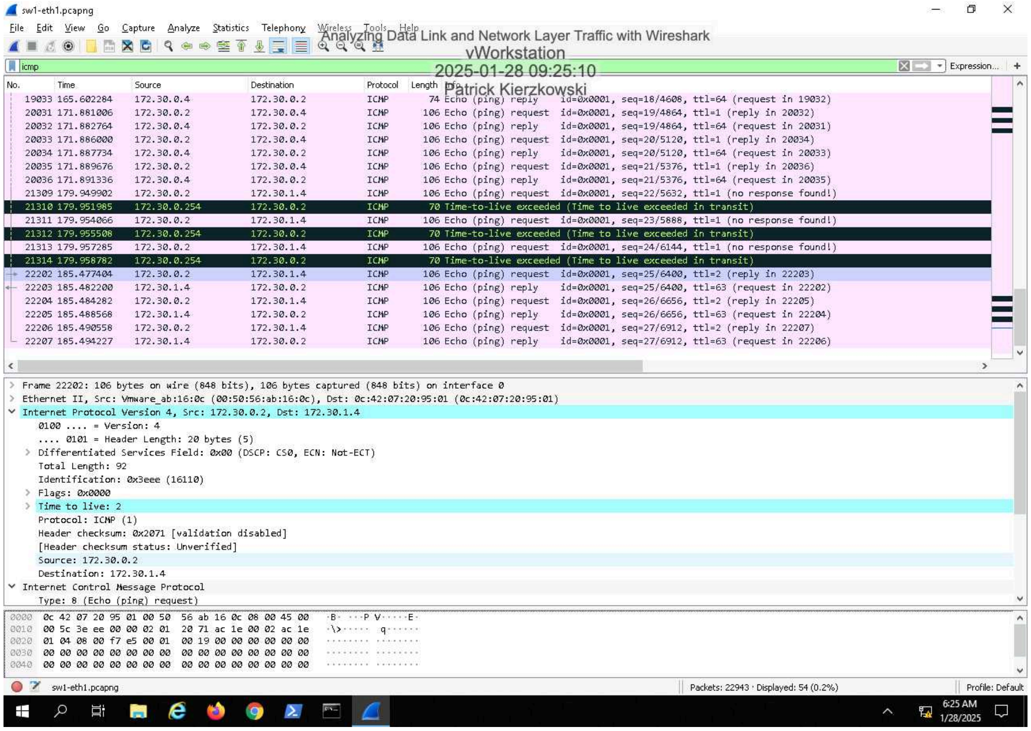
```
> Frame 21314: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: 0c:42:07:20:95:01 (0c:42:07:20:95:01), Dst: Vmware_ab:16:0c (00:50:56:ab:16:0c)
> Internet Protocol Version 4, Src: 172.30.0.254, Dst: 172.30.0.2
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  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: 0x3eed (16109)
    > Flags: 0x0000
    > Time to live: 1
```

```
0000  00 50 56 ab 16 0c 0c 42  07 20 95 01 08 00 45 00   ·PV····B ······E·
0010  00 38 94 22 00 00 40 01  8d 66 ac 1e 00 fe ac 1e   ·8·"··@· ·f······
0020  00 02 0b 00 f4 ff 00 00  00 00 45 00 00 5c 3e ed   ········ ··E··\>·
0030  00 00 01 01 21 72 ac 1e  00 02 ac 1e 01 04 08 00   ····!r·· ········
0040  f7 e6 00 01 00 18                                  ······
```

sw1-eth1.pcapng | Packets: 22943 · Displayed: 54 (0.2%) | Profile: Default

6:24 AM
1/28/2025

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



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 09:25:10
Patrick Kierzkowski

```
No.   Time        Source        Destination  Protocol Length Info
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)
22203 185.482200  172.30.1.4    172.30.0.2   ICMP     106 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=63 (request in 22202)
22204 185.484282  172.30.0.2    172.30.1.4   ICMP     106 Echo (ping) request  id=0x0001, seq=26/6656, ttl=2 (reply in 22205)
22205 185.488568  172.30.1.4    172.30.0.2   ICMP     106 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=63 (request in 22204)
22206 185.490558  172.30.0.2    172.30.1.4   ICMP     106 Echo (ping) request  id=0x0001, seq=27/6912, ttl=2 (reply in 22207)
22207 185.494227  172.30.1.4    172.30.0.2   ICMP     106 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=63 (request in 22206)
```

```
> 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
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

```
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   ·\>·····  q······
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   ········ ········
```

sw1-eth1.pcapng | Packets: 22943 · Displayed: 54 (0.2%) | Profile: Default

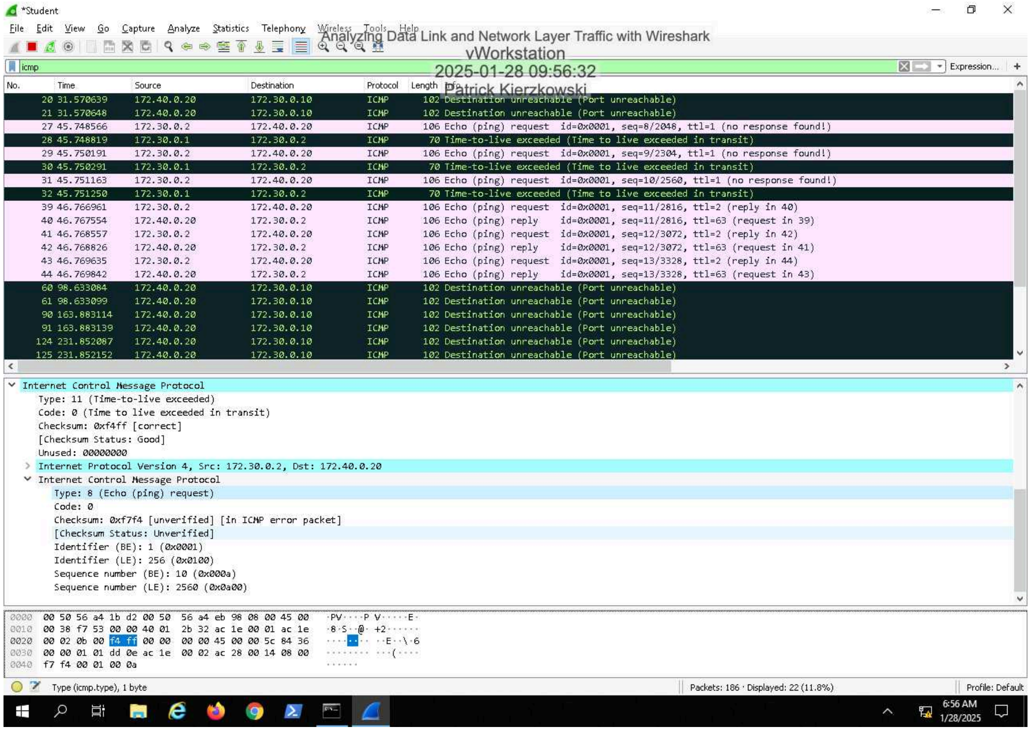
24. **Record** the VLAN ID of the 172.30.0.0/24 network.

VLAN 2

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**.


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

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 09:56:32
Patrick Kierzkowski

icmp

```
No.   Time        Source       Destination  Protocol Length Info
   20 31.570639   172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   21 31.570648   172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   27 45.748566   172.30.0.2   172.40.0.20  ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=1 (no response found!)
   28 45.748819   172.30.0.1   172.30.0.2   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   29 45.750191   172.30.0.2   172.40.0.20  ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=1 (no response found!)
   30 45.750291   172.30.0.1   172.30.0.2   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   31 45.751163   172.30.0.2   172.40.0.20  ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=1 (no response found!)
   32 45.751250   172.30.0.1   172.30.0.2   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   39 46.766961   172.30.0.2   172.40.0.20  ICMP     106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=2 (reply in 40)
   40 46.767554   172.40.0.20  172.30.0.2   ICMP     106 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=63 (request in 39)
   41 46.768557   172.30.0.2   172.40.0.20  ICMP     106 Echo (ping) request  id=0x0001, seq=12/3072, ttl=2 (reply in 42)
   42 46.768826   172.40.0.20  172.30.0.2   ICMP     106 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=63 (request in 41)
   43 46.769635   172.30.0.2   172.40.0.20  ICMP     106 Echo (ping) request  id=0x0001, seq=13/3328, ttl=2 (reply in 44)
   44 46.769842   172.40.0.20  172.30.0.2   ICMP     106 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=63 (request in 43)
   60 98.633084   172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   61 98.633099   172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   90 163.883114  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
   91 163.883139  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
  124 231.852087  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
  125 231.852152  172.40.0.20  172.30.0.10  ICMP     102 Destination unreachable (Port unreachable)
```

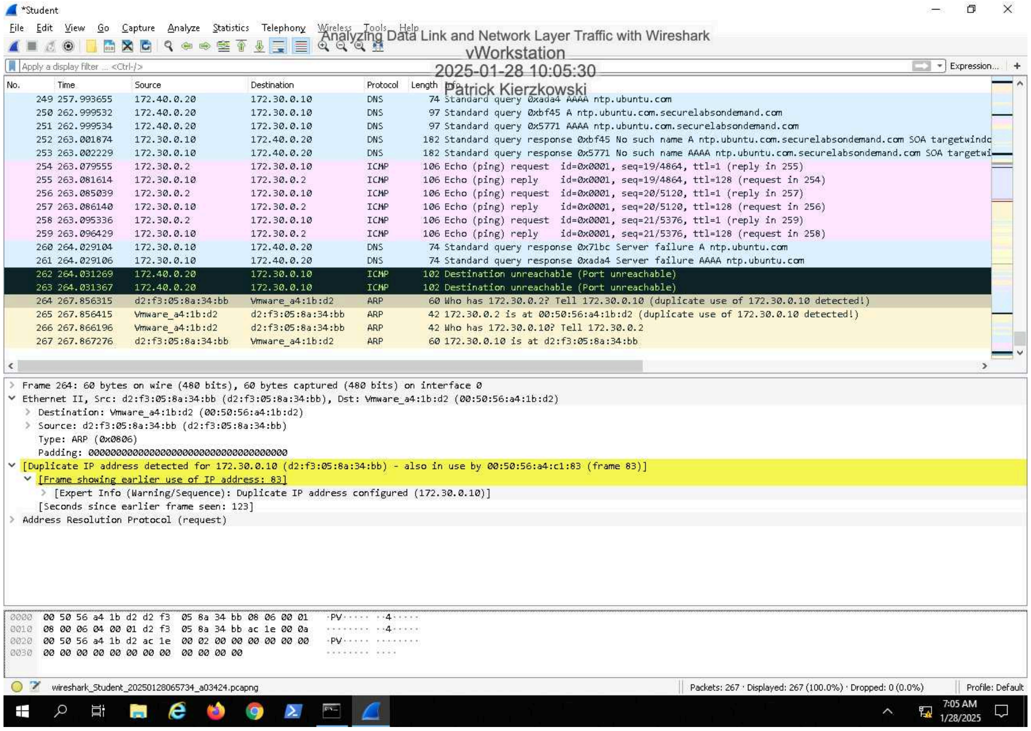
```
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.20
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7f4 [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence number (BE): 10 (0x000a)
      Sequence number (LE): 2560 (0x0a00)
```

```
0000  00 50 56 a4 1b d2 00 50  56 a4 eb 98 08 00 45 00   ·PV····P V·····E·
0010  00 38 f7 53 00 00 40 01  2b 32 ac 1e 00 01 ac 1e   ·8·S··@· +2······
0020  00 02 0b 00 f4 ff 00 00  00 00 45 00 00 5c 84 36   ········ ··E··\·6
0030  00 00 01 01 dd 0e ac 1e  00 02 ac 28 00 14 08 00   ········ ···(····
0040  f7 f4 00 01 00 0a                                  ······
```

Type (icmp.type), 1 byte | Packets: 186 · Displayed: 22 (11.8%) | Profile: Default

6:56 AM
1/28/2025

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


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
7:05 AM
1/28/2025

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 10:05:30
Patrick Kierzkowski

Apply a display filter ... <Ctrl-/>

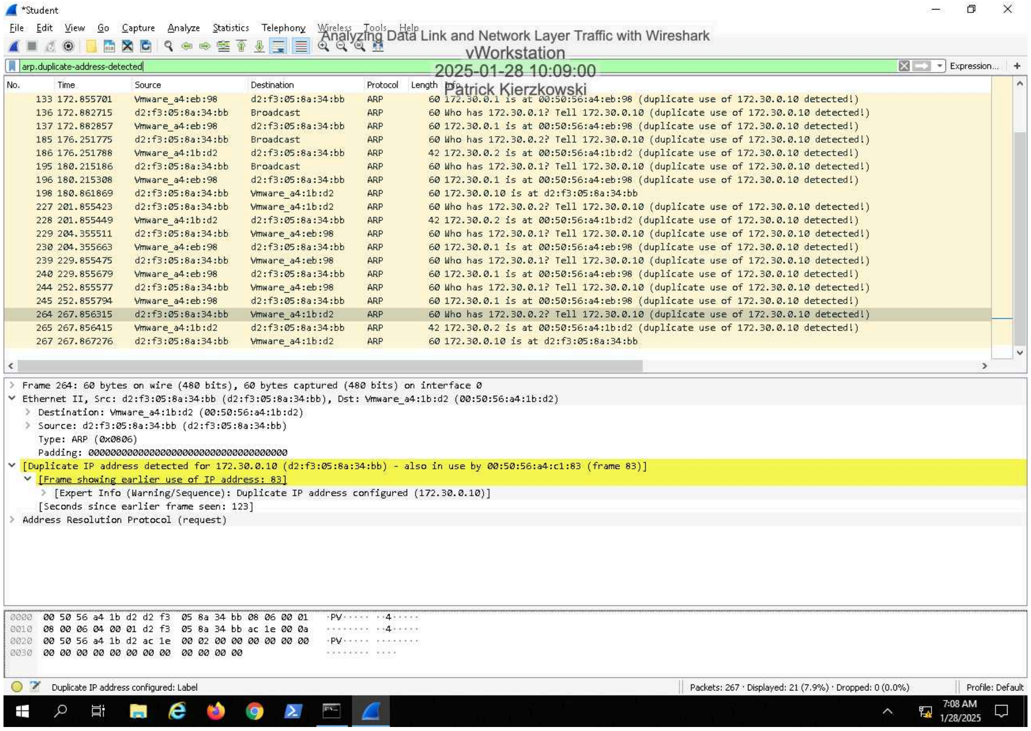
```
No.   Time          Source              Destination         Protocol  Length  Info
  249 257.993655    172.40.0.20         172.30.0.10         DNS        74 Standard query 0xada4 AAAA ntp.ubuntu.com
  250 262.999532    172.40.0.20         172.30.0.10         DNS        97 Standard query 0xbf45 A ntp.ubuntu.com.securelabsondemand.com
  251 262.999534    172.40.0.20         172.30.0.10         DNS        97 Standard query 0x5771 AAAA ntp.ubuntu.com.securelabsondemand.com
  252 263.001874    172.30.0.10         172.40.0.20         DNS       182 Standard query response 0xbf45 No such name A ntp.ubuntu.com.securelabsondemand.com SOA targetwindc
  253 263.002229    172.30.0.10         172.40.0.20         DNS       182 Standard query response 0x5771 No such name AAAA ntp.ubuntu.com.securelabsondemand.com SOA targetwi
  254 263.079555    172.30.0.2          172.30.0.10         ICMP      106 Echo (ping) request  id=0x0001, seq=19/4864, ttl=1 (reply in 255)
  255 263.081614    172.30.0.10         172.30.0.2          ICMP      106 Echo (ping) reply    id=0x0001, seq=19/4864, ttl=128 (request in 254)
  256 263.085039    172.30.0.2          172.30.0.10         ICMP      106 Echo (ping) request  id=0x0001, seq=20/5120, ttl=1 (reply in 257)
  257 263.086140    172.30.0.10         172.30.0.2          ICMP      106 Echo (ping) reply    id=0x0001, seq=20/5120, ttl=128 (request in 256)
  258 263.095336    172.30.0.2          172.30.0.10         ICMP      106 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1 (reply in 259)
  259 263.096429    172.30.0.10         172.30.0.2          ICMP      106 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=128 (request in 258)
  260 264.029104    172.30.0.10         172.40.0.20         DNS        74 Standard query response 0x71bc Server failure A ntp.ubuntu.com
  261 264.029106    172.30.0.10         172.40.0.20         DNS        74 Standard query response 0xada4 Server failure AAAA ntp.ubuntu.com
  262 264.031269    172.40.0.20         172.30.0.10         ICMP      102 Destination unreachable (Port unreachable)
  263 264.031367    172.40.0.20         172.30.0.10         ICMP      102 Destination unreachable (Port unreachable)
  264 267.856315    d2:f3:05:8a:34:bb   Vmware_a4:1b:d2     ARP        60 Who has 172.30.0.2? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  265 267.856415    Vmware_a4:1b:d2     d2:f3:05:8a:34:bb   ARP        42 172.30.0.2 is at 00:50:56:a4:1b:d2 (duplicate use of 172.30.0.10 detected!)
  266 267.866196    Vmware_a4:1b:d2     d2:f3:05:8a:34:bb   ARP        42 Who has 172.30.0.10? Tell 172.30.0.2
  267 267.867276    d2:f3:05:8a:34:bb   Vmware_a4:1b:d2     ARP        60 172.30.0.10 is at d2:f3:05:8a:34:bb
```

```
> Frame 264: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: d2:f3:05:8a:34:bb (d2:f3:05:8a:34:bb), Dst: Vmware_a4:1b:d2 (00:50:56:a4:1b:d2)
  > Destination: Vmware_a4:1b:d2 (00:50:56:a4:1b:d2)
  > Source: d2:f3:05:8a:34:bb (d2:f3:05:8a:34:bb)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v [Duplicate IP address detected for 172.30.0.10 (d2:f3:05:8a:34:bb) - also in use by 00:50:56:a4:c1:83 (frame 83)]
  v [Frame showing earlier use of IP address: 83]
    > [Expert Info (Warning/Sequence): Duplicate IP address configured (172.30.0.10)]
    [Seconds since earlier frame seen: 123]
> Address Resolution Protocol (request)
```

```
0000  00 50 56 a4 1b d2 d2 f3  05 8a 34 bb 08 06 00 01   ·PV····· ··4·····
0010  08 00 06 04 00 01 d2 f3  05 8a 34 bb ac 1e 00 0a   ········ ··4·····
0020  00 50 56 a4 1b d2 ac 1e  00 02 00 00 00 00 00 00   ·PV····· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

wireshark_Student_20250128065734_a03424.pcapng | Packets: 267 · Displayed: 267 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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...
7:08 AM
1/28/2025

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 10:09:00
Patrick Kierzkowski

arp.duplicate-address-detected

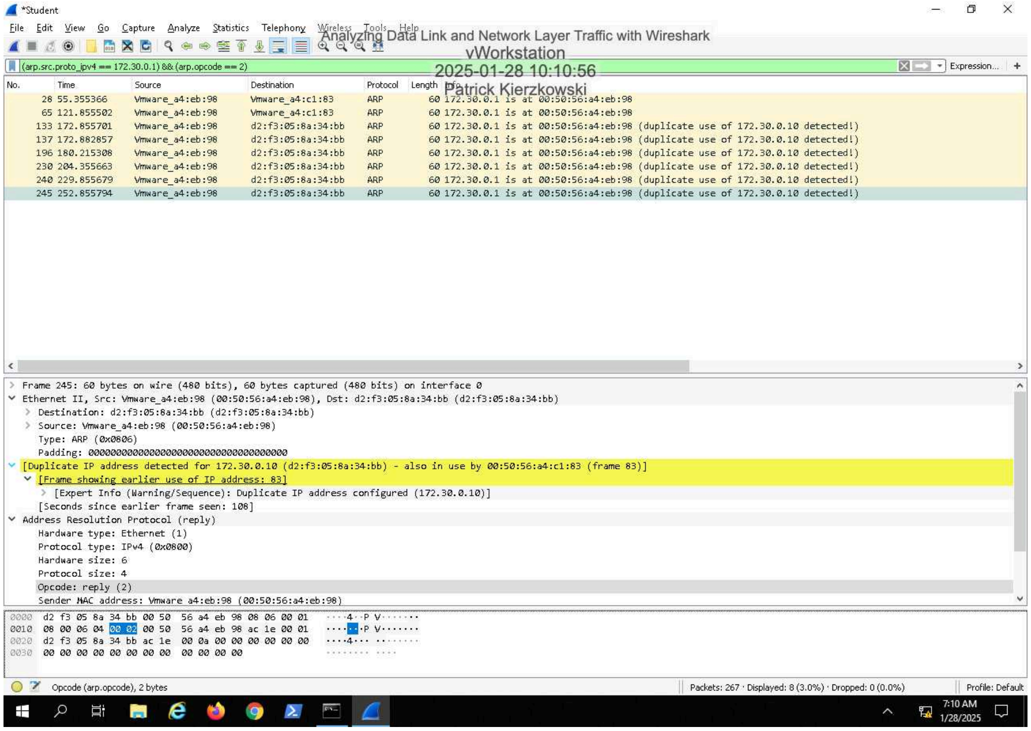
```
No.   Time          Source              Destination         Protocol  Length  Info
  133 172.855701    Vmware_a4:eb:98     d2:f3:05:8a:34:bb   ARP        60 172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
  136 172.882715    d2:f3:05:8a:34:bb   Broadcast           ARP        60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  137 172.882857    Vmware_a4:eb:98     d2:f3:05:8a:34:bb   ARP        60 172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
  185 176.251775    d2:f3:05:8a:34:bb   Broadcast           ARP        60 Who has 172.30.0.2? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  186 176.251788    Vmware_a4:1b:d2     d2:f3:05:8a:34:bb   ARP        42 172.30.0.2 is at 00:50:56:a4:1b:d2 (duplicate use of 172.30.0.10 detected!)
  195 180.215186    d2:f3:05:8a:34:bb   Broadcast           ARP        60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  196 180.215308    Vmware_a4:eb:98     d2:f3:05:8a:34:bb   ARP        60 172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
  198 180.861869    d2:f3:05:8a:34:bb   Vmware_a4:1b:d2     ARP        60 172.30.0.10 is at d2:f3:05:8a:34:bb
  227 201.855423    d2:f3:05:8a:34:bb   Vmware_a4:1b:d2     ARP        60 Who has 172.30.0.2? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  228 201.855449    Vmware_a4:1b:d2     d2:f3:05:8a:34:bb   ARP        42 172.30.0.2 is at 00:50:56:a4:1b:d2 (duplicate use of 172.30.0.10 detected!)
  229 204.355511    d2:f3:05:8a:34:bb   Vmware_a4:eb:98     ARP        60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  230 204.355663    Vmware_a4:eb:98     d2:f3:05:8a:34:bb   ARP        60 172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
  239 229.855475    d2:f3:05:8a:34:bb   Vmware_a4:eb:98     ARP        60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  240 229.855679    Vmware_a4:eb:98     d2:f3:05:8a:34:bb   ARP        60 172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
  244 252.855577    d2:f3:05:8a:34:bb   Vmware_a4:eb:98     ARP        60 Who has 172.30.0.1? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  245 252.855794    Vmware_a4:eb:98     d2:f3:05:8a:34:bb   ARP        60 172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
  264 267.856315    d2:f3:05:8a:34:bb   Vmware_a4:1b:d2     ARP        60 Who has 172.30.0.2? Tell 172.30.0.10 (duplicate use of 172.30.0.10 detected!)
  265 267.856415    Vmware_a4:1b:d2     d2:f3:05:8a:34:bb   ARP        42 172.30.0.2 is at 00:50:56:a4:1b:d2 (duplicate use of 172.30.0.10 detected!)
  267 267.867276    d2:f3:05:8a:34:bb   Vmware_a4:1b:d2     ARP        60 172.30.0.10 is at d2:f3:05:8a:34:bb
```

```
> Frame 264: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: d2:f3:05:8a:34:bb (d2:f3:05:8a:34:bb), Dst: Vmware_a4:1b:d2 (00:50:56:a4:1b:d2)
  > Destination: Vmware_a4:1b:d2 (00:50:56:a4:1b:d2)
  > Source: d2:f3:05:8a:34:bb (d2:f3:05:8a:34:bb)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v [Duplicate IP address detected for 172.30.0.10 (d2:f3:05:8a:34:bb) - also in use by 00:50:56:a4:c1:83 (frame 83)]
  v [Frame showing earlier use of IP address: 83]
    > [Expert Info (Warning/Sequence): Duplicate IP address configured (172.30.0.10)]
    [Seconds since earlier frame seen: 123]
> Address Resolution Protocol (request)
```

```
0000  00 50 56 a4 1b d2 d2 f3  05 8a 34 bb 08 06 00 01   ·PV····· ··4·····
0010  08 00 06 04 00 01 d2 f3  05 8a 34 bb ac 1e 00 0a   ········ ··4·····
0020  00 50 56 a4 1b d2 ac 1e  00 02 00 00 00 00 00 00   ·PV····· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Duplicate IP address configured: Label | Packets: 267 · Displayed: 21 (7.9%) · 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
Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-28 10:10:56
Patrick Kierzkowski
Expression...

(arp.src.proto_ipv4 == 172.30.0.1) && (arp.opcode == 2)

No.	Time	Source	Destination	Protocol	Length	Info
28	55.355366	Vmware_a4:eb:98	Vmware_a4:c1:83	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98
65	121.855502	Vmware_a4:eb:98	Vmware_a4:c1:83	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98
133	172.855701	Vmware_a4:eb:98	d2:f3:05:8a:34:bb	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
137	172.882857	Vmware_a4:eb:98	d2:f3:05:8a:34:bb	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
196	180.215308	Vmware_a4:eb:98	d2:f3:05:8a:34:bb	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
230	204.355663	Vmware_a4:eb:98	d2:f3:05:8a:34:bb	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
240	229.855679	Vmware_a4:eb:98	d2:f3:05:8a:34:bb	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)
245	252.855794	Vmware_a4:eb:98	d2:f3:05:8a:34:bb	ARP	60	172.30.0.1 is at 00:50:56:a4:eb:98 (duplicate use of 172.30.0.10 detected!)

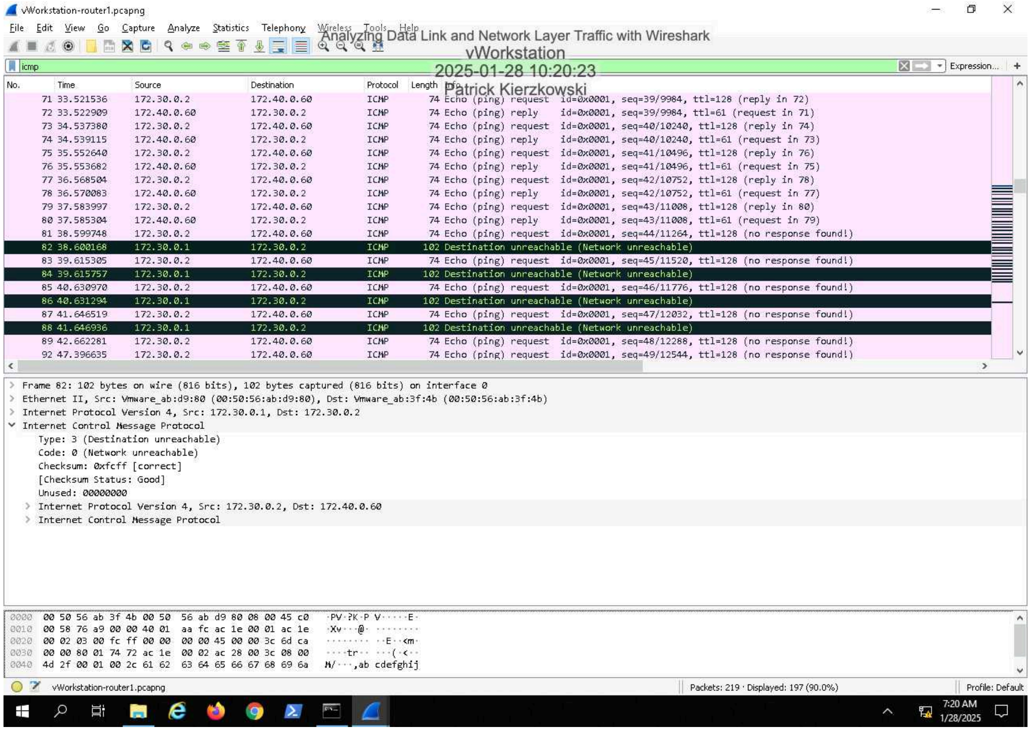
```
> Frame 245: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: Vmware_a4:eb:98 (00:50:56:a4:eb:98), Dst: d2:f3:05:8a:34:bb (d2:f3:05:8a:34:bb)
  > Destination: d2:f3:05:8a:34:bb (d2:f3:05:8a:34:bb)
  > Source: Vmware_a4:eb:98 (00:50:56:a4:eb:98)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v [Duplicate IP address detected for 172.30.0.10 (d2:f3:05:8a:34:bb) - also in use by 00:50:56:a4:c1:83 (frame 83)]
  v [Frame showing earlier use of IP address: 83]
    > [Expert Info (Warning/Sequence): Duplicate IP address configured (172.30.0.10)]
    [Seconds since earlier frame seen: 108]
v 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_a4:eb:98 (00:50:56:a4:eb:98)
```

```
0000  d2 f3 05 8a 34 bb 00 50  56 a4 eb 98 08 06 00 01   ····4··P V·······
0010  08 00 06 04 00 02 00 50  56 a4 eb 98 ac 1e 00 01   ········P V·······
0020  d2 f3 05 8a 34 bb ac 1e  00 0a 00 00 00 00 00 00   ····4··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Opcode (arp.opcode), 2 bytes | Packets: 267 · Displayed: 8 (3.0%) · Dropped: 0 (0.0%) | Profile: Default

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
2025-01-28 10:20:23
Patrick Kierzkowski
Expression...

icmp

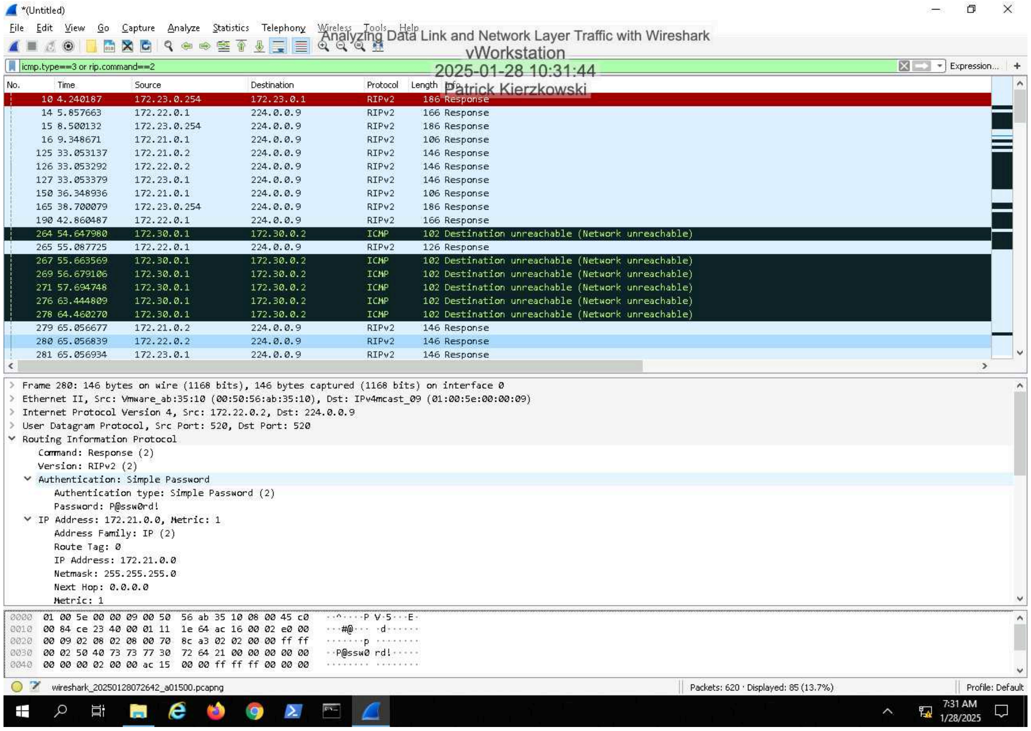
No.	Time	Source	Destination	Protocol	Length	Info
71	33.521536	172.30.0.2	172.40.0.60	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 72)
72	33.522909	172.40.0.60	172.30.0.2	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=61 (request in 71)
73	34.537380	172.30.0.2	172.40.0.60	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 found!)
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 found!)
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 found!)
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 found!)
88	41.646936	172.30.0.1	172.30.0.2	ICMP	102	Destination unreachable (Network unreachable)
89	42.662281	172.30.0.2	172.40.0.60	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (no response found!)
92	47.396635	172.30.0.2	172.40.0.60	ICMP	74	Echo (ping) request id=0x0001, seq=49/12544, ttl=128 (no response found!)

```
> Frame 82: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: Vmware_ab:d9:80 (00:50:56:ab:d9:80), Dst: Vmware_ab:3f:4b (00:50:56:ab:3f:4b)
> Internet Protocol Version 4, Src: 172.30.0.1, Dst: 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
```

```
0000  00 50 56 ab 3f 4b 00 50  56 ab d9 80 08 00 45 c0   ·PV·?K·P V·····E·
0010  00 58 76 a9 00 00 40 01  aa fc ac 1e 00 01 ac 1e   ·Xv···@· ········
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·· ···(·<··
0040  4d 2f 00 01 00 2c 61 62  63 64 65 66 67 68 69 6a   M/···,ab cdefghij
```

vWorkstation-router1.pcapng | 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
2025-01-28 10:31:44
Patrick Kierzkowski
Expression…
7:31 AM
1/28/2025

icmp.type==3 or 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
   264 54.647980  172.30.0.1     172.30.0.2    ICMP      102 Destination unreachable (Network unreachable)
   265 55.087725  172.22.0.1     224.0.0.9     RIPv2     126 Response
   267 55.663569  172.30.0.1     172.30.0.2    ICMP      102 Destination unreachable (Network unreachable)
   269 56.679106  172.30.0.1     172.30.0.2    ICMP      102 Destination unreachable (Network unreachable)
   271 57.694748  172.30.0.1     172.30.0.2    ICMP      102 Destination unreachable (Network unreachable)
   276 63.444809  172.30.0.1     172.30.0.2    ICMP      102 Destination unreachable (Network unreachable)
   278 64.460270  172.30.0.1     172.30.0.2    ICMP      102 Destination unreachable (Network unreachable)
   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
```

```
> 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
```

```
0000  01 00 5e 00 00 09 00 50  56 ab 35 10 08 00 45 c0   ··^····P V·5···E·
0010  00 84 ce 23 40 00 01 11  1e 64 ac 16 00 02 e0 00   ···#@···  ·d······
0020  00 09 02 08 02 08 00 70  8c a3 02 02 00 00 ff ff   ·······p ········
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   ········ ········
```

wireshark_20250128072642_a01500.pcapng | Packets: 620 · Displayed: 85 (13.7%) | Profile: Default

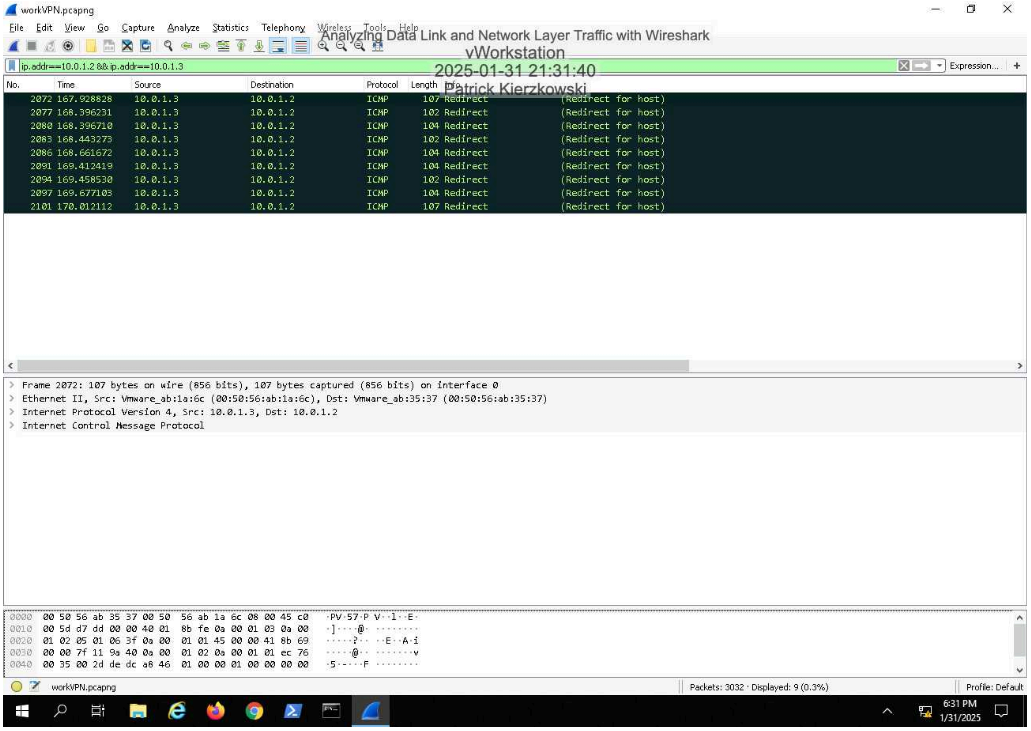
25. **Record** the number of the packet that contains the first corrected RIPv2 simple password**.**

348

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**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-31 21:31:40
Patrick Kierzkowski

ip.addr==10.0.1.2 && ip.addr==10.0.1.3

```
No.    Time        Source      Destination  Protocol  Length  Info
  2072 167.928828  10.0.1.3    10.0.1.2     ICMP      107 Redirect          (Redirect for host)
  2077 168.396231  10.0.1.3    10.0.1.2     ICMP      102 Redirect          (Redirect for host)
  2080 168.396710  10.0.1.3    10.0.1.2     ICMP      104 Redirect          (Redirect for host)
  2083 168.443273  10.0.1.3    10.0.1.2     ICMP      102 Redirect          (Redirect for host)
  2086 168.661672  10.0.1.3    10.0.1.2     ICMP      104 Redirect          (Redirect for host)
  2091 169.412419  10.0.1.3    10.0.1.2     ICMP      104 Redirect          (Redirect for host)
  2094 169.458530  10.0.1.3    10.0.1.2     ICMP      102 Redirect          (Redirect for host)
  2097 169.677103  10.0.1.3    10.0.1.2     ICMP      104 Redirect          (Redirect for host)
  2101 170.012112  10.0.1.3    10.0.1.2     ICMP      107 Redirect          (Redirect for host)
```

```
> Frame 2072: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
> Ethernet II, Src: Vmware_ab:1a:6c (00:50:56:ab:1a:6c), Dst: Vmware_ab:35:37 (00:50:56:ab:35:37)
> Internet Protocol Version 4, Src: 10.0.1.3, Dst: 10.0.1.2
> Internet Control Message Protocol
```

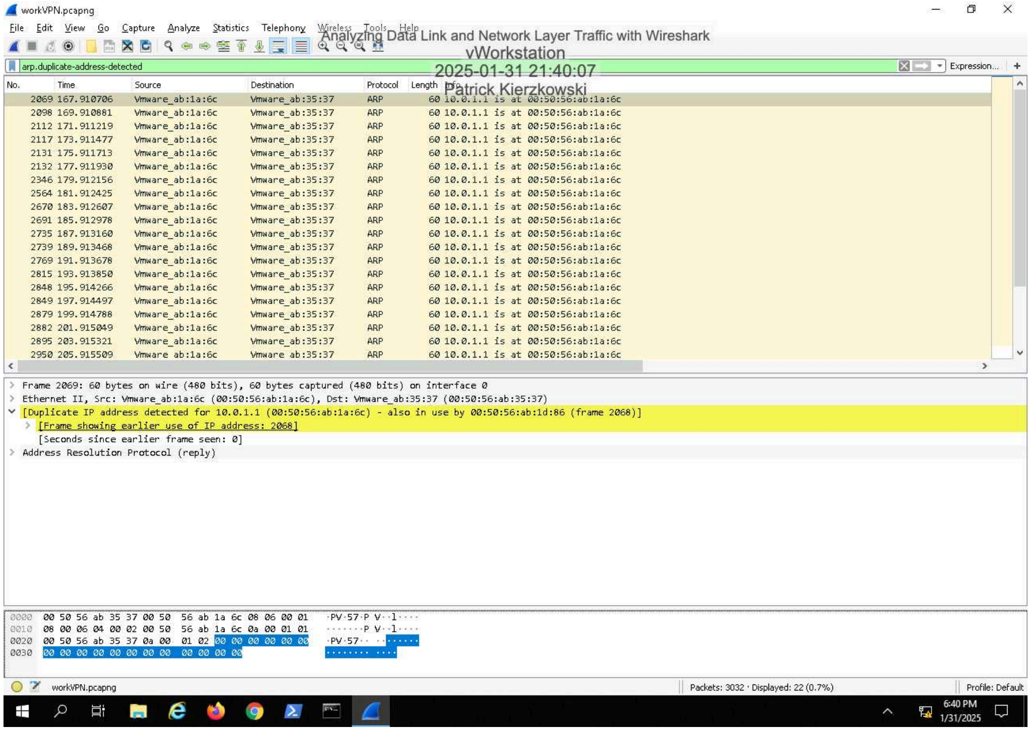
```
0000  00 50 56 ab 35 37 00 50  56 ab 1a 6c 08 00 45 c0   ·PV·57·P V··l··E·
0010  00 5d d7 dd 00 00 40 01  8b fe 0a 00 01 03 0a 00   ·]····@· ········
0020  01 02 05 01 06 3f 0a 00  01 01 45 00 00 41 8b 69   ·····?·· ··E··A·i
0030  00 00 7f 11 9a 40 0a 00  01 02 0a 00 01 01 ec 76   ·····@·· ·······v
0040  00 35 00 2d de dc a8 46  01 00 00 01 00 00 00 00   ·5·-···F ········
```

workVPN.pcapng | Packets: 3032 · Displayed: 9 (0.3%) | Profile: Default

6:31 PM
1/31/2025

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**.



Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-31 21:40:07
Patrick Kierzkowski

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
 2882 201.915049  Vmware_ab:1a:6c    Vmware_ab:35:37    ARP       60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2895 203.915321  Vmware_ab:1a:6c    Vmware_ab:35:37    ARP       60 10.0.1.1 is at 00:50:56:ab:1a:6c
 2950 205.915509  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
> Ethernet II, Src: Vmware_ab:1a:6c (00:50:56:ab:1a:6c), Dst: Vmware_ab:35:37 (00:50:56:ab:35:37)
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)]
  > [Frame showing earlier use of IP address: 2068]
    [Seconds since earlier frame seen: 0]
> Address Resolution Protocol (reply)
```

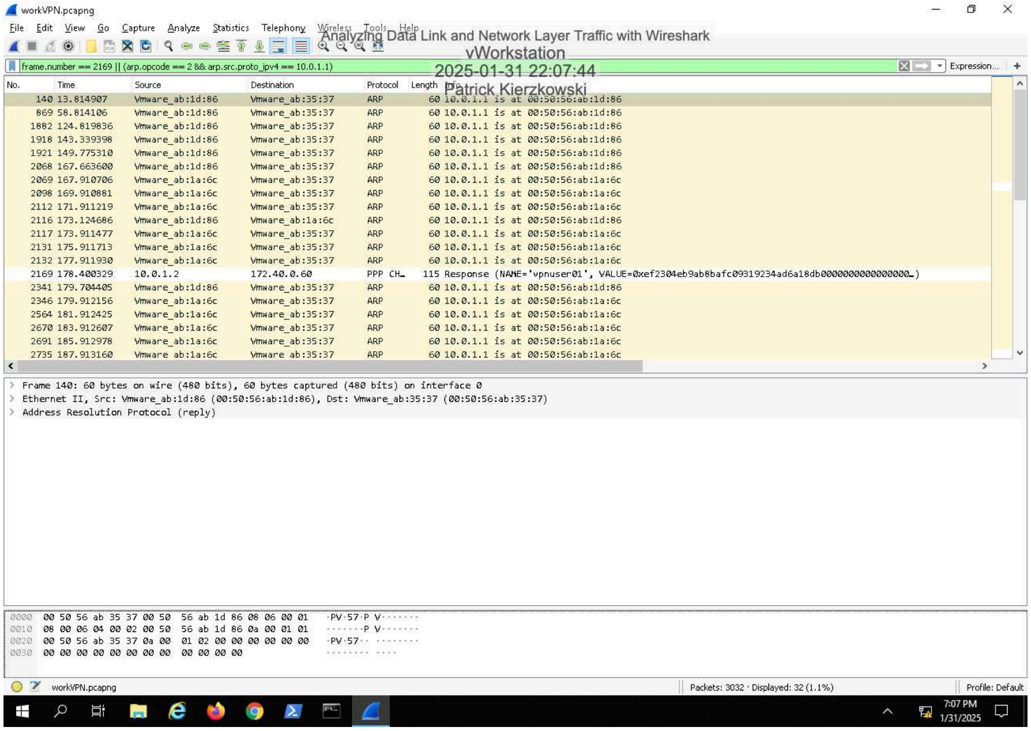
```
0000  00 50 56 ab 35 37 00 50  56 ab 1a 6c 08 06 00 01   ·PV·57·P V··l····
0010  08 00 06 04 00 02 00 50  56 ab 1a 6c 0a 00 01 01   ·······P V··l····
0020  00 50 56 ab 35 37 0a 00  01 02 00 00 00 00 00 00   ·PV·57·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

workVPN.pcapng | Packets: 3032 · Displayed: 22 (0.7%) | Profile: Default

6:40 PM
1/31/2025

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…
+
7:07 PM
1/31/2025

Analyzing Data Link and Network Layer Traffic with Wireshark
vWorkstation
2025-01-31 22:07:44
Patrick Kierzkowski

frame.number == 2169 || (arp.opcode == 2 && arp.src.proto_ipv4 == 10.0.1.1)

No.	Time	Source	Destination	Protocol	Length	Info
140	13.814907	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
869	58.814106	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
1882	124.819836	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
1918	143.339398	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
1921	149.775310	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
2068	167.663600	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
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
2116	173.124686	Vmware_ab:1d:86	Vmware_ab:1a:6c	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
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
2169	178.400329	10.0.1.2	172.40.0.60	PPP CH…	115	Response (NAME='vpnuser01', VALUE=0xef2304eb9ab8bafc09319234ad6a18db0000000000000000…)
2341	179.704405	Vmware_ab:1d:86	Vmware_ab:35:37	ARP	60	10.0.1.1 is at 00:50:56:ab:1d:86
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

```
> Frame 140: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_ab:1d:86 (00:50:56:ab:1d:86), Dst: Vmware_ab:35:37 (00:50:56:ab:35:37)
> Address Resolution Protocol (reply)
```

```
0000  00 50 56 ab 35 37 00 50  56 ab 1d 86 08 06 00 01   ·PV·57·P V·······
0010  08 00 06 04 00 02 00 50  56 ab 1d 86 0a 00 01 01   ·······P V·······
0020  00 50 56 ab 35 37 0a 00  01 02 00 00 00 00 00 00   ·PV·57·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

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