# Course: Use Wireshark to Examine Network Traffic-C1-2026

# Cyber Shujaa Program

## Week 1 Assignment 2
## Use Wireshark to Examine Network Traffic

**Student Name:** Salim Katana Karuku

**Student ID:** CS-CNS11-26048

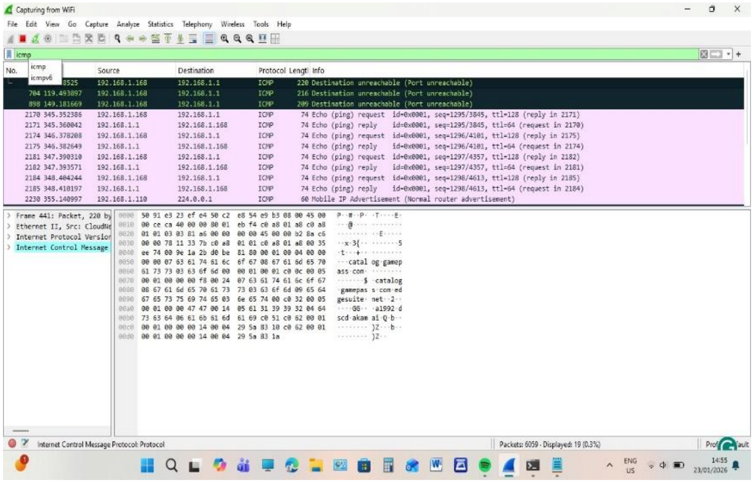
## Table of Contents

## Objectives

The objectives of the assignment were:

1. To troubleshoot network issues
2. To analysing protocol behaviour
3. To enhance network security by detecting threats
4. To optimizing application performance and educational purposes to learn network internals like TCP/IP

# Part 1: Capture and Analyze Local ICMP Data in Wireshark



```
No.    Time              Source           Destination     Protocol Length Info
        8525            192.168.1.168    192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
   704 119.493897       192.168.1.168    192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
   898 149.181669       192.168.1.168    192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
  2170 345.352386       192.168.1.168    192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
  2171 345.360042       192.168.1.1      192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
  2174 346.378208       192.168.1.168    192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
  2175 346.382649       192.168.1.1      192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
  2181 347.390310       192.168.1.168    192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
  2182 347.393571       192.168.1.1      192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
  2184 348.404244       192.168.1.168    192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
  2185 348.410197       192.168.1.1      192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
  2230 355.140997       192.168.1.110    224.0.0.1       ICMP      60 Mobile IP Advertisement (Normal router advertisement)
```

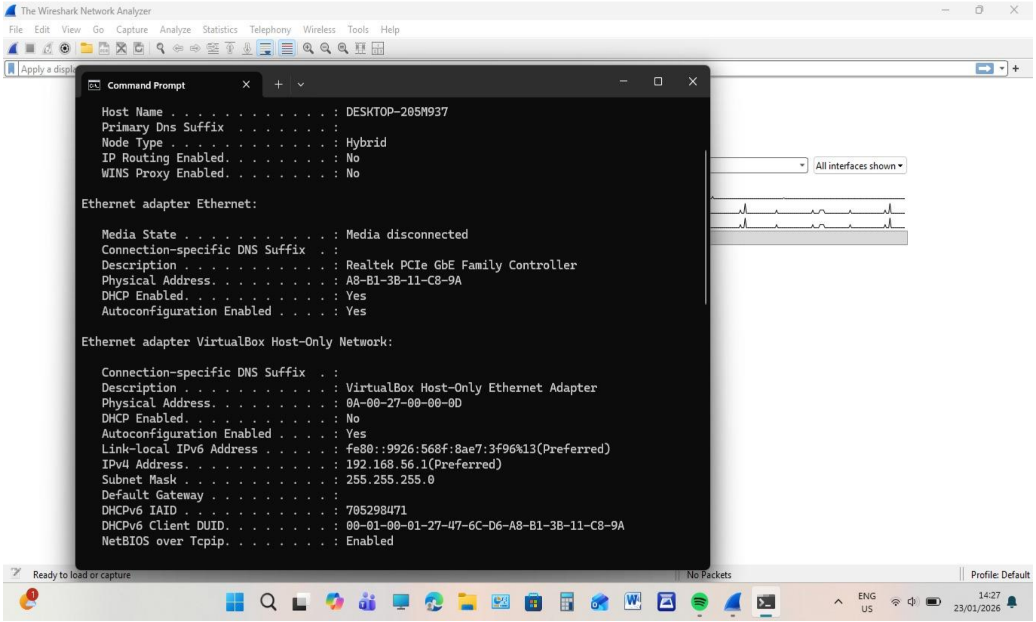
```
> Frame 441: Packet, 220 by
> Ethernet II, Src: CloudNe
> Internet Protocol Versior
> Internet Control Message

0000  50 91 e3 23 ef e4 50 c2  e8 54 e9 b3 08 00 45 00   P··#··P· ·T····E·
0010  00 ce ca 40 00 00 80 01  eb f4 c0 a8 01 a8 c0 a8   ···@···· ········
0020  01 01 03 03 81 a6 00 00  00 00 45 00 00 b2 8a c6   ········ ··E·····
0030  00 00 78 11 33 7b c0 a8  01 01 c0 a8 01 a8 00 35   ··x·3{·· ·······5
0040  ee 74 00 9e 1a 2b d0 be  81 80 00 01 00 04 00 00   ·t···+·· ········
0050  00 00 07 63 61 74 61 6c  6f 67 08 67 61 6d 65 70   ···catal og·gamep
0060  61 73 73 03 63 6f 6d 00  00 01 00 01 c0 0c 00 05   ass·com· ········
0070  00 01 00 00 00 f8 00 24  07 63 61 74 61 6c 6f 67   ·······$ ·catalog
0080  08 67 61 6d 65 70 61 73  73 03 63 6f 6d 09 65 64   ·gamepas s·com·ed
0090  67 65 73 75 69 74 65 03  6e 65 74 00 c0 32 00 05   gesuite· net··2··
00a0  00 01 00 00 47 47 00 14  05 61 31 39 39 32 04 64   ····GG·· ·a1992·d
00b0  73 63 64 06 61 6b 61 6d  61 69 c0 51 c0 62 00 01   scd·akam ai·Q·b··
00c0  00 01 00 00 00 14 00 04  29 5a 83 10 c0 62 00 01   ········ )Z···b··
00d0  00 01 00 00 00 14 00 04  29 5a 83 1a               ········ )Z··
```

Internet Control Message Protocol: Protocol

Packets: 6059 · Displayed: 10 (0.3%)

Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6
Profile: Default
ENG
US
14:55
23/01/2026

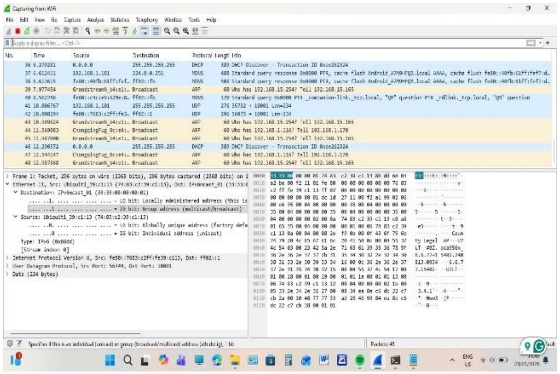
Step 1: Retrieving PC interface addresses



```
   Host Name . . . . . . . . . . . . : DESKTOP-205M937
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : A8-B1-3B-11-C8-9A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9926:568f:8ae7:3f96%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 705298471
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-47-6C-D6-A8-B1-3B-11-C8-9A
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Here I configure the IP address and its MAC address

Step 1: (b) PC IP addresses that were provided with team member



```
No.  Time        Source                Destination       Protocol Length Info
  36 6.279281    0.0.0.0               255.255.255.255   DHCP     383 DHCP Discover - Transaction ID 0xee262324
  37 6.612411    192.168.1.181         224.0.0.251       MDNS     408 Standard query response 0x0000 PTR, cache flush Android_A7M9HFQ3.local AAAA, cache flush fe80::40fb:61ff:fef7:d…
  38 6.613615    fe80::40fb:61ff:fef…  ff02::fb          MDNS     508 Standard query response 0x0000 PTR, cache flush Android_A7M9HFQ3.local AAAA, cache flush fe80::40fb:61ff:fef7:d…
  39 7.977454    GrandstreamN_b4:e1:…  Broadcast         ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
  40 8.502248    fe80::c9c:e9:629e:8…  ff02::fb          MDNS     120 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question
  41 10.006767   192.168.1.181         255.255.255.255   UDP      276 35782 → 10001 Len=234
  42 10.008294   fe80::7683:c2ff:fe3…  ff02::1           UDP      296 56035 → 10001 Len=234
  43 10.989824   GrandstreamN_b4:e1:…  Broadcast         ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
  44 11.569083   ChongqingFug_0c:e4:…  Broadcast         ARP       60 Who has 192.168.1.116? Tell 192.168.1.170
  45 11.987000   GrandstreamN_b4:e1:…  Broadcast         ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
  46 12.290372   0.0.0.0               255.255.255.255   DHCP     383 DHCP Discover - Transaction ID 0xee262324
  47 12.344147   ChongqingFug_0c:e4:…  Broadcast         ARP       60 Who has 192.168.1.116? Tell 192.168.1.170
  48 12.987868   GrandstreamN_b4:e1:…  Broadcast         ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
```

```
> Frame 1: Packet, 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on i
v Ethernet II, Src: Ubiquiti_39:c1:13 (74:83:c2:39:c1:13), Dst: IPv6mcast_01 (33:33:0
  v Destination: IPv6mcast_01 (33:33:00:00:00:01)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: Ubiquiti_39:c1:13 (74:83:c2:39:c1:13)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: fe80::7683:c2ff:fe39:c113, Dst: ff02::1
> User Datagram Protocol, Src Port: 56349, Dst Port: 10001
> Data (234 bytes)
```

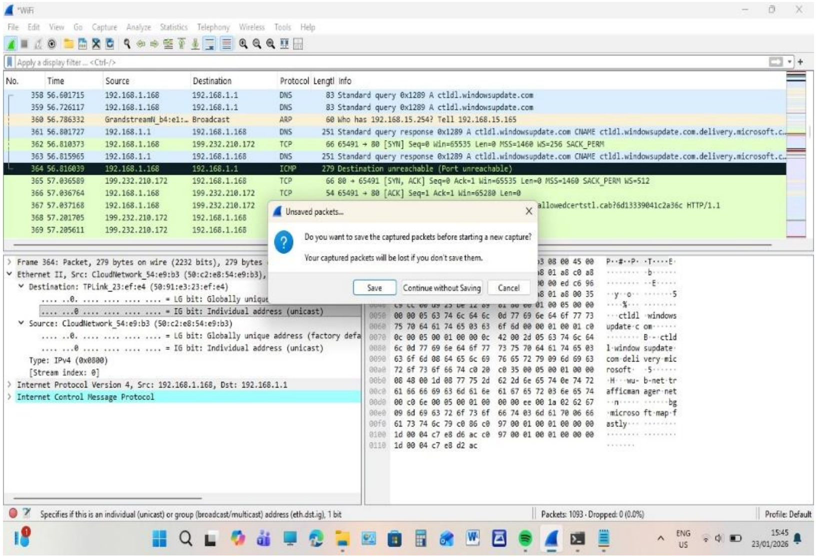
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit

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

PC IP address: 192.168.1.168

Step 2: Start Wireshark and begin Capturing data

(a)



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source              Destination       Protocol Lengtl Info
 358 56.601715   192.168.1.168       192.168.1.1       DNS       83 Standard query 0x1289 A ctldl.windowsupdate.com
 359 56.726117   192.168.1.168       192.168.1.1       DNS       83 Standard query 0x1289 A ctldl.windowsupdate.com
 360 56.786332   GrandstreamN_b4:e1:… Broadcast        ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
 361 56.801727   192.168.1.1         192.168.1.168     DNS      251 Standard query response 0x1289 A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.c…
 362 56.810373   192.168.1.168       199.232.210.172   TCP       66 65491 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 363 56.815965   192.168.1.1         192.168.1.168     DNS      251 Standard query response 0x1289 A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.c…
 364 56.816039   192.168.1.168       192.168.1.1       ICMP     279 Destination unreachable (Port unreachable)
 365 57.036589   199.232.210.172     192.168.1.168     TCP       66 80 → 65491 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
 366 57.036764   192.168.1.168       199.232.210.172   TCP       54 65491 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 367 57.037168   192.168.1.168       199.232.210.172                 allowedcertstl.cab?6d13339041c2a36c HTTP/1.1
 368 57.201705   199.232.210.172     192.168.1.168
 369 57.205611   199.232.210.172     192.168.1.168
```

Unsaved packets...

Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

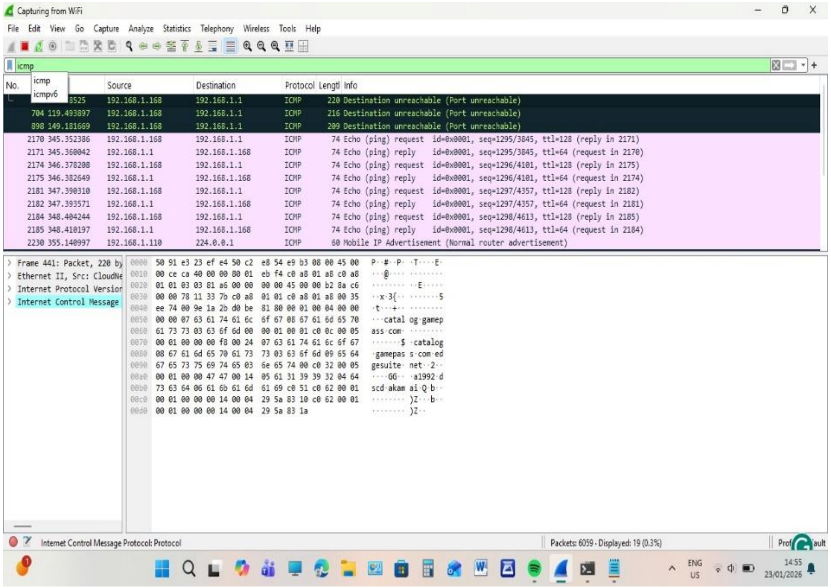
Save | Continue without Saving | Cancel

```
> Frame 364: Packet, 279 bytes on wire (2232 bits), 279 bytes
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3),
  v Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
                                 3 08 00 45 00    P··#··P· ·T····E·
                                 8 01 a8 c0 a8    ········ ·b······
                                 0 00 ed c6 96    ········ ··E·····
                                 8 01 a8 00 35    ··y··o·· ·······5
                                    01 00 05 00 00    ····%··· ········
0050  00 00 05 63 74 6c 64 6c  0d 77 69 6e 64 6f 77 73    ···ctldl ·windows
0060  75 70 64 61 74 65 03 63  6f 6d 00 00 01 00 01 c0    update·c om······
0070  0c 00 05 00 01 00 00 0c  42 00 2d 05 63 74 6c 64    ········ B·-·ctld
0080  6c 0d 77 69 6e 64 6f 77  73 75 70 64 61 74 65 03    l·window supdate·
0090  63 6f 6d 08 64 65 6c 69  76 65 72 79 09 6d 69 63    com·deli very·mic
00a0  72 6f 73 6f 66 74 c0 20  c0 35 00 05 00 01 00 00    rosoft·  ·5······
00b0  08 48 00 1d 08 77 75 2d  62 2d 6e 65 74 0e 74 72    ·H···wu- b-net·tr
00c0  61 66 66 69 63 6d 61 6e  61 67 65 72 03 6e 65 74    afficman ager·net
00d0  00 c0 6e 00 05 00 01 00  00 00 ee 00 1a 02 62 67    ··n····· ······bg
00e0  09 6d 69 63 72 6f 73 6f  66 74 03 6d 61 70 06 66    ·microso ft·map·f
00f0  61 73 74 6c 79 c0 86 c0  97 00 01 00 01 00 00 00    astly··· ········
0100  1d 00 04 c7 e8 d6 ac c0  97 00 01 00 01 00 00 00    ········ ········
0110  1d 00 04 c7 e8 d2 ac                                ·······
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit | Packets: 1093 · Dropped: 0 (0.0%) | Profile: Default

Step 2: (b)



Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmpv6

```
No.   Time        Source          Destination     Protocol Lengtl Info
      …8525       192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
  704 119.493897  192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
  898 149.181669  192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
 2170 345.352386  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
 2171 345.360042  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
 2174 346.378208  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
 2175 346.382649  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
 2181 347.390310  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
 2182 347.393571  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
 2184 348.404244  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
 2185 348.410197  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
 2230 355.140997  192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Advertisement (Normal router advertisement)
```

```
> Frame 441: Packet, 220 by
> Ethernet II, Src: CloudNe
> Internet Protocol Versior
> Internet Control Message
```

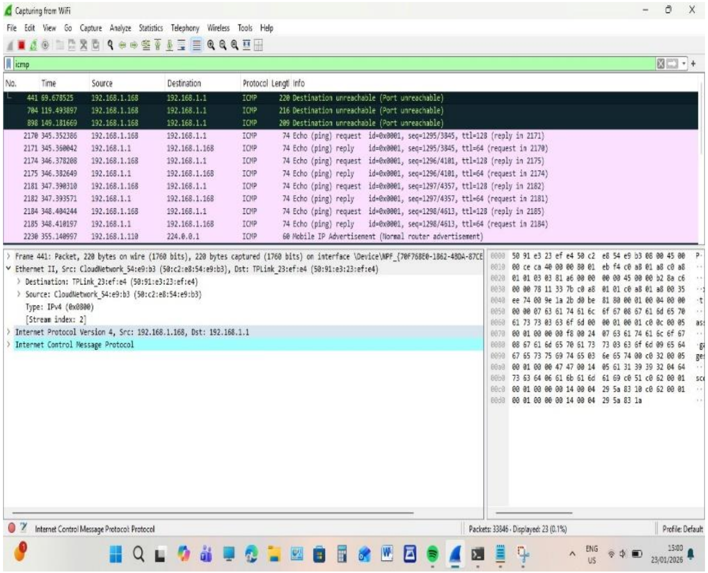
```
0000  50 91 e3 23 ef e4 50 c2  e8 54 e9 b3 08 00 45 00    P··#··P· ·T····E·
0010  00 ce ca 40 00 00 80 01  eb f4 c0 a8 01 a8 c0 a8    ···@···· ········
0020  01 01 03 03 81 a6 00 00  00 00 45 00 00 b2 8a c6    ········ ··E·····
0030  00 00 78 11 33 7b c0 a8  01 01 c0 a8 01 a8 00 35    ··x·3{·· ·······5
0040  ee 74 00 9e 1a 2b d0 be  81 80 00 01 00 04 00 00    ·t···+·· ········
0050  00 00 07 63 61 74 61 6c  6f 67 08 67 61 6d 65 70    ···catal og·gamep
0060  61 73 73 03 63 6f 6d 00  00 01 00 01 c0 0c 00 05    ass·com· ········
0070  00 01 00 00 00 f8 00 24  07 63 61 74 61 6c 6f 67    ·······$ ·catalog
0080  08 67 61 6d 65 70 61 73  73 03 63 6f 6d 09 65 64    ·gamepas s·com·ed
0090  67 65 73 75 69 74 65 03  6e 65 74 00 c0 32 00 05    gesuite· net··2··
00a0  00 01 00 00 47 47 00 14  05 61 31 39 39 32 04 64    ····GG·· ·a1992·d
00b0  73 63 64 06 61 6b 61 6d  61 69 c0 51 c0 62 00 01    scd·akam ai·Q·b··
00c0  00 01 00 00 00 14 00 04  29 5a 83 10 c0 62 00 01    ········ )Z···b··
00d0  00 01 00 00 00 14 00 04  29 5a 83 1a                ········ )Z··
```

Internet Control Message Protocol: Protocol | Packets: 6059 · Displayed: 19 (0.3%) | Prof…ault

Step 2: (c)

- Ping 192.169.1.1

I notice how the data appear at the top window


Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source          Destination     Protocol Lengtl Info
  441 69.678525   192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
  704 119.493897  192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
  898 149.181669  192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
 2170 345.352386  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
 2171 345.360042  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
 2174 346.378208  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
 2175 346.382649  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
 2181 347.390310  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
 2182 347.393571  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
 2184 348.404244  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
 2185 348.410197  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
 2230 355.140997  192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Advertisement (Normal router advertisement)
```

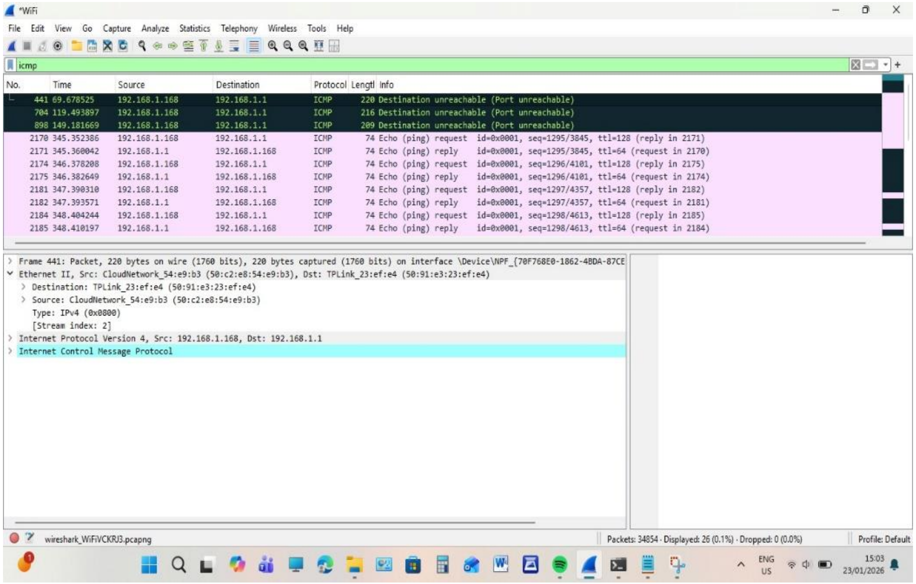
```
> Frame 441: Packet, 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{70F768E0-1862-4BDA-87CE
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
0000  50 91 e3 23 ef e4 50 c2  e8 54 e9 b3 08 00 45 00   P·
0010  00 ce ca 40 00 00 80 01  eb f4 c0 a8 01 a8 c0 a8   ··
0020  01 01 03 03 81 a6 00 00  00 00 45 00 00 b2 8a c6   ··
0030  00 00 78 11 33 7b c0 a8  01 01 c0 a8 01 a8 00 35   ··
0040  ee 74 00 9e 1a 2b d0 be  81 80 00 01 00 04 00 00   ·t
0050  00 00 07 63 61 74 61 6c  6f 67 08 67 61 6d 65 70   ··
0060  61 73 73 03 63 6f 6d 00  00 01 00 01 c0 0c 00 05   as
0070  00 01 00 00 00 f8 00 24  07 63 61 74 61 6c 6f 67   ··
0080  08 67 61 6d 65 70 61 73  73 03 63 6f 6d 09 65 64   ·g
0090  67 65 73 75 69 74 65 03  6e 65 74 00 c0 32 00 05   ge
00a0  00 01 00 00 47 47 00 14  05 61 31 39 39 32 04 64   ··
00b0  73 63 64 06 61 6b 61 6d  61 69 c0 51 c0 62 00 01   sc
00c0  00 01 00 00 00 14 00 04  29 5a 83 10 c0 62 00 01   ··
00d0  00 01 00 00 00 14 00 04  29 5a 83 1a               ··
```

```
Internet Control Message Protocol: Protocol    Packets: 33846 · Displayed: 23 (0.1%)    Profile: Default
```

Step 2: (d) Stop capture data by clicking the Stop Capture

After clicking the stop capture i found the following observation


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

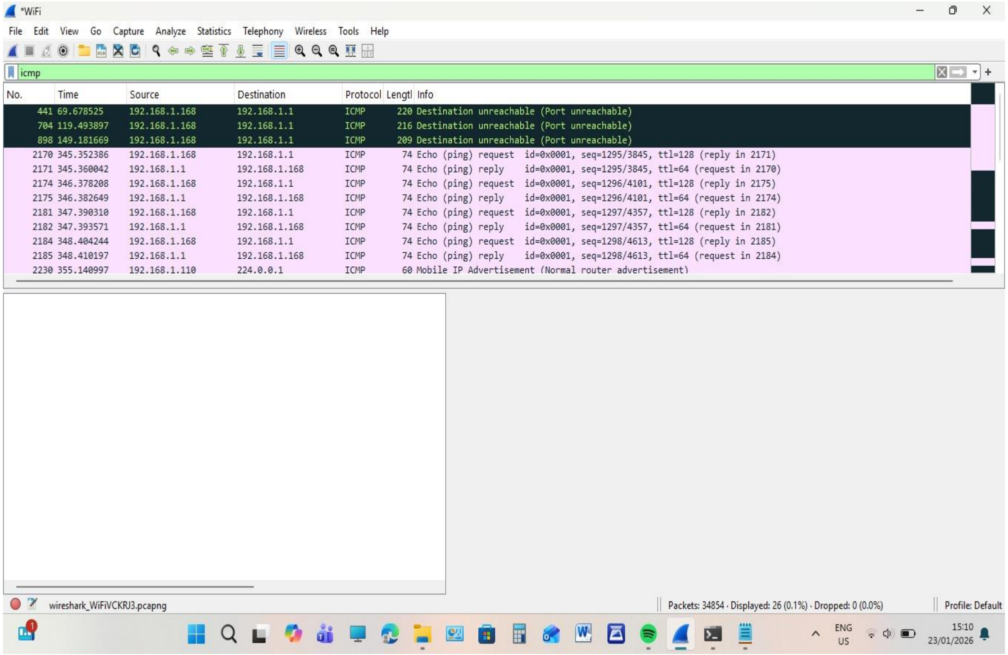
```
No.   Time        Source          Destination     Protocol Lengtl Info
  441 69.678525   192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
  704 119.493897  192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
  898 149.181669  192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
 2170 345.352386  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
 2171 345.360042  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
 2174 346.378208  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
 2175 346.382649  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
 2181 347.390310  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
 2182 347.393571  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
 2184 348.404244  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
 2185 348.410197  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
```

```
> Frame 441: Packet, 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{70F768E0-1862-4BDA-87CE
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
wireshark_WiFiVCKRJ3.pcapng    Packets: 34854 · Displayed: 26 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

## Step 3: Examine the captured data

(a) The source column has my PC IP address 192.168.1.168 while the Destination column has the IP address of the pinged PC 192,168.1.1 as shown below

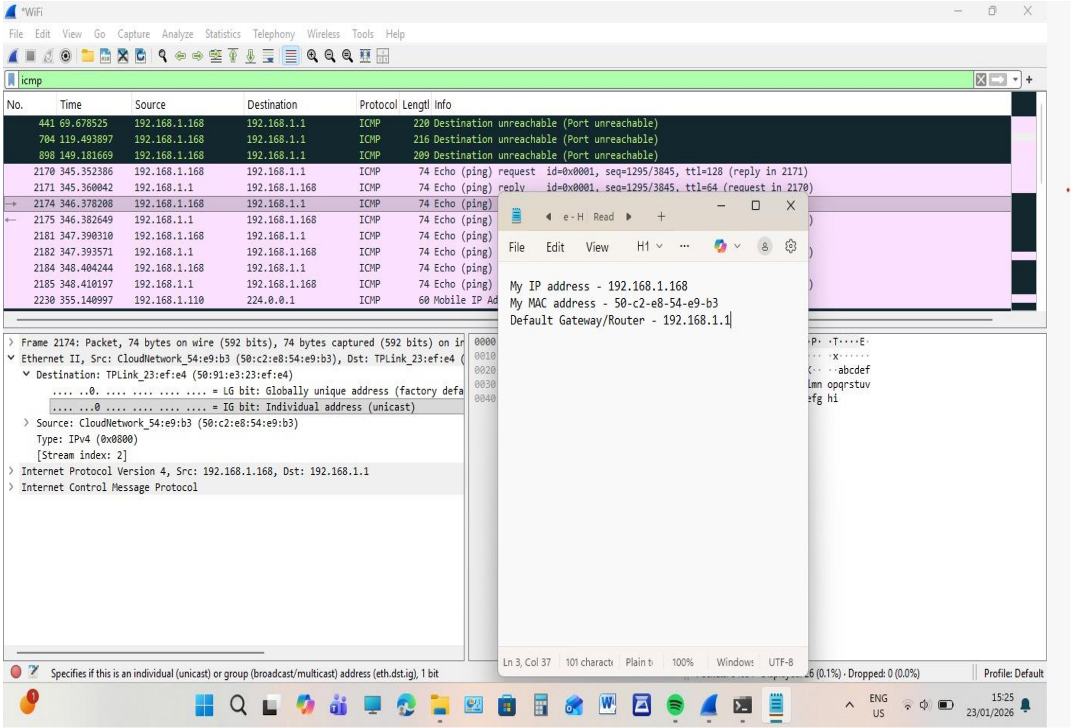


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source          Destination     Protocol Lengtl Info
  441 69.678525   192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
  704 119.493897  192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
  898 149.181669  192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
 2170 345.352386  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
 2171 345.360042  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
 2174 346.378208  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
 2175 346.382649  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
 2181 347.390310  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
 2182 347.393571  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
 2184 348.404244  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
 2185 348.410197  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
 2230 355.140997  192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Advertisement (Normal router advertisement)
```

wireshark_WiFiVCKRJ3.pcapng | Packets: 34854 · Displayed: 26 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

(b) After watching it carefully I realized that the source MAC address matches my PC interface as shown below



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
e - H
Read
File Edit View H1

```
No.   Time        Source          Destination     Protocol Lengtl Info
  441 69.678525   192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
  704 119.493897  192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
  898 149.181669  192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
 2170 345.352386  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
 2171 345.360042  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
 2174 346.378208  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping)
 2175 346.382649  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping)
 2181 347.390310  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping)
 2182 347.393571  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping)
 2184 348.404244  192.168.1.168   192.168.1.1     ICMP      74 Echo (ping)
 2185 348.410197  192.168.1.1     192.168.1.168   ICMP      74 Echo (ping)
 2230 355.140997  192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Ad
```

```
> Frame 2174: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on ir
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (
  v Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

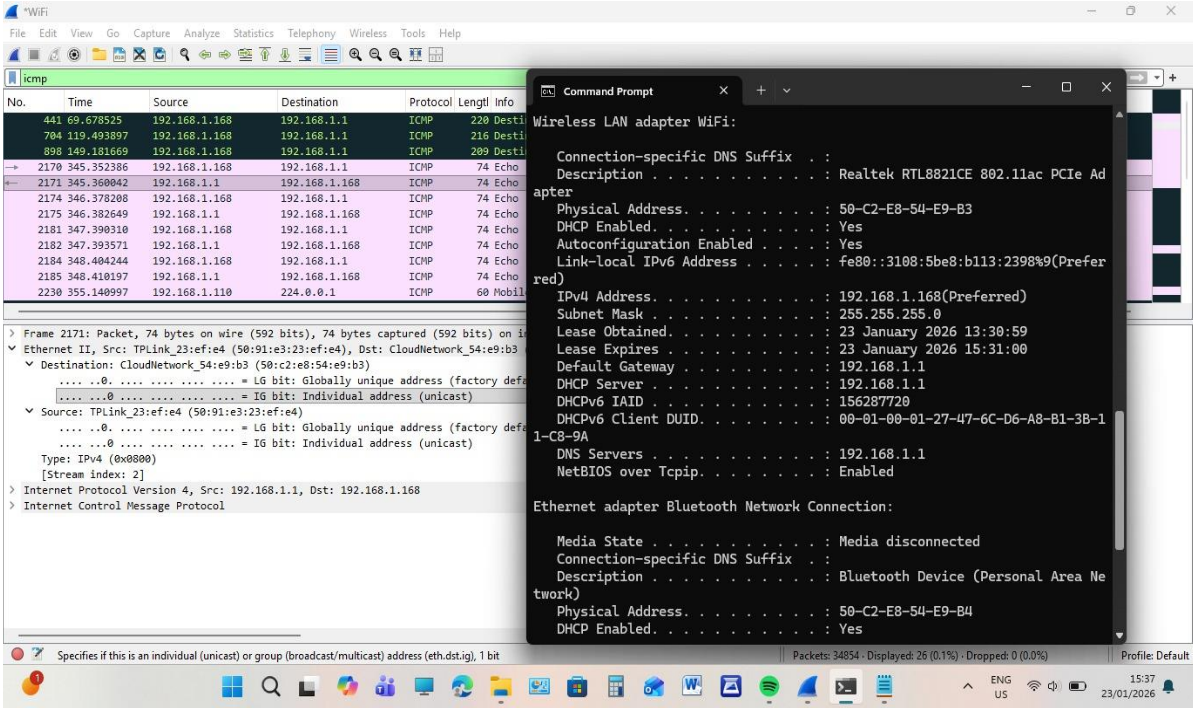
```
0000   ·P· ·T····E·
0010   ··· ·x······
0020   (·· ··abcdef
0030   lmn opqrstuv
0040   efg hi
```

```
My IP address - 192.168.1.168
My MAC address - 50-c2-e8-54-e9-b3
Default Gateway/Router - 192.168.1.1
```

Ln 3, Col 37 | 101 characte | Plain t | 100% | Windows | UTF-8

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit | 26 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

After review it I found out that YES the destination MAC address match my team member in in MAC address as shown below



```
No.   Time          Source          Destination    Protocol Lengtl Info
  441 69.678525     192.168.1.168   192.168.1.1    ICMP     220 Desti
  704 119.493897    192.168.1.168   192.168.1.1    ICMP     216 Desti
  898 149.181669    192.168.1.168   192.168.1.1    ICMP     209 Desti
 2170 345.352386    192.168.1.168   192.168.1.1    ICMP      74 Echo
 2171 345.360042    192.168.1.1     192.168.1.168  ICMP      74 Echo
 2174 346.378208    192.168.1.168   192.168.1.1    ICMP      74 Echo
 2175 346.382649    192.168.1.1     192.168.1.168  ICMP      74 Echo
 2181 347.390310    192.168.1.168   192.168.1.1    ICMP      74 Echo
 2182 347.393571    192.168.1.1     192.168.1.168  ICMP      74 Echo
 2184 348.404244    192.168.1.168   192.168.1.1    ICMP      74 Echo
 2185 348.410197    192.168.1.1     192.168.1.168  ICMP      74 Echo
 2230 355.140997    192.168.1.110   224.0.0.1      ICMP      60 Mobil
```

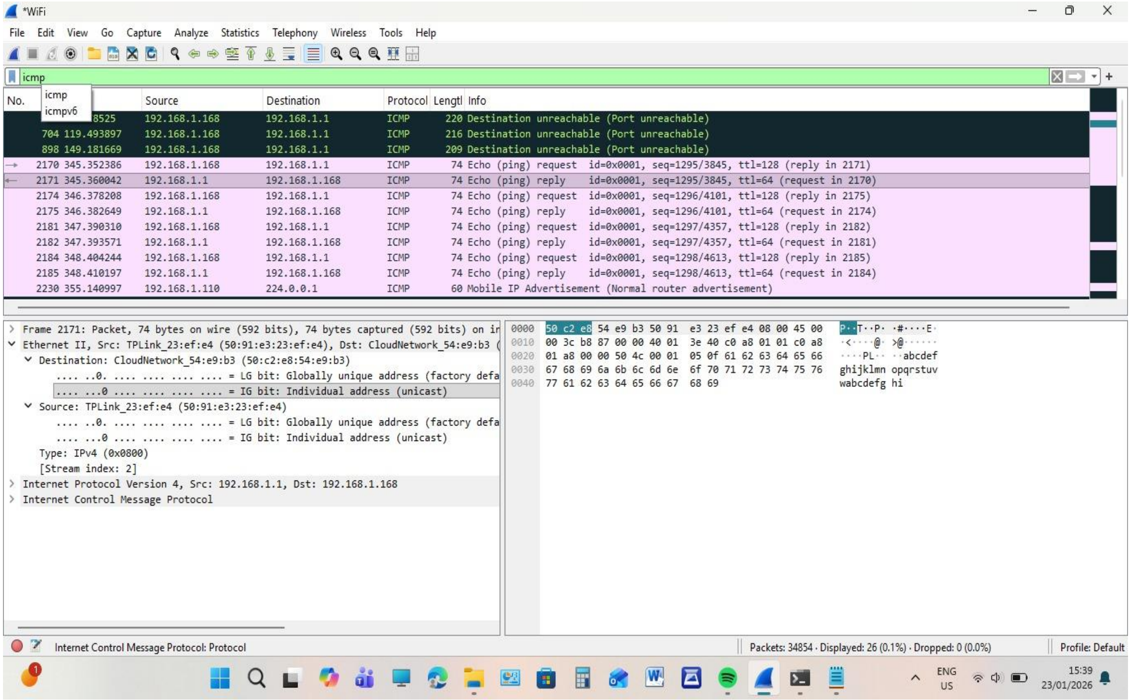
```
> Frame 2171: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
v Ethernet II, Src: TPLink_23:ef:e4 (50:91:e3:23:ef:e4), Dst: CloudNetwork_54:e9:b3
  v Destination: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.168
> Internet Control Message Protocol
```

```
Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8821CE 802.11ac PCIe Ad
apter
   Physical Address. . . . . . . . . : 50-C2-E8-54-E9-B3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::3108:5be8:b113:2398%9(Prefer
red)
   IPv4 Address. . . . . . . . . . . : 192.168.1.168(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 23 January 2026 13:30:59
   Lease Expires . . . . . . . . . . : 23 January 2026 15:31:00
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 156287720
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-47-6C-D6-A8-B1-3B-1
1-C8-9A
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Ne
twork)
   Physical Address. . . . . . . . . : 50-C2-E8-54-E9-B4
   DHCP Enabled. . . . . . . . . . . : Yes
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit | Packets: 34854 · Displayed: 26 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Command Prompt
ENG
US
15:37
23/01/2026

It is obtained through an ARP request when pinging a local IP my computer send a broadcast message asking who has this IP address while the target device replies with its MAC address which is then cached in APR table



```
No.   Time          Source          Destination    Protocol Lengtl Info
     8525           192.168.1.168   192.168.1.1    ICMP     220 Destination unreachable (Port unreachable)
  704 119.493897    192.168.1.168   192.168.1.1    ICMP     216 Destination unreachable (Port unreachable)
  898 149.181669    192.168.1.168   192.168.1.1    ICMP     209 Destination unreachable (Port unreachable)
 2170 345.352386    192.168.1.168   192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
 2171 345.360042    192.168.1.1     192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
 2174 346.378208    192.168.1.168   192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
 2175 346.382649    192.168.1.1     192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
 2181 347.390310    192.168.1.168   192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
 2182 347.393571    192.168.1.1     192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
 2184 348.404244    192.168.1.168   192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
 2185 348.410197    192.168.1.1     192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
 2230 355.140997    192.168.1.110   224.0.0.1      ICMP      60 Mobile IP Advertisement (Normal router advertisement)
```

```
> Frame 2171: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
v Ethernet II, Src: TPLink_23:ef:e4 (50:91:e3:23:ef:e4), Dst: CloudNetwork_54:e9:b3 (
  v Destination: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.168
> Internet Control Message Protocol
```

```
0000  50 c2 e8 54 e9 b3 50 91  e3 23 ef e4 08 00 45 00   P··T··P· ·#····E·
0010  00 3c b8 87 00 00 40 01  3e 40 c0 a8 01 01 c0 a8   ·<····@· >@······
0020  01 a8 00 00 50 4c 00 01  05 0f 61 62 63 64 65 66   ····PL·· ··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
```

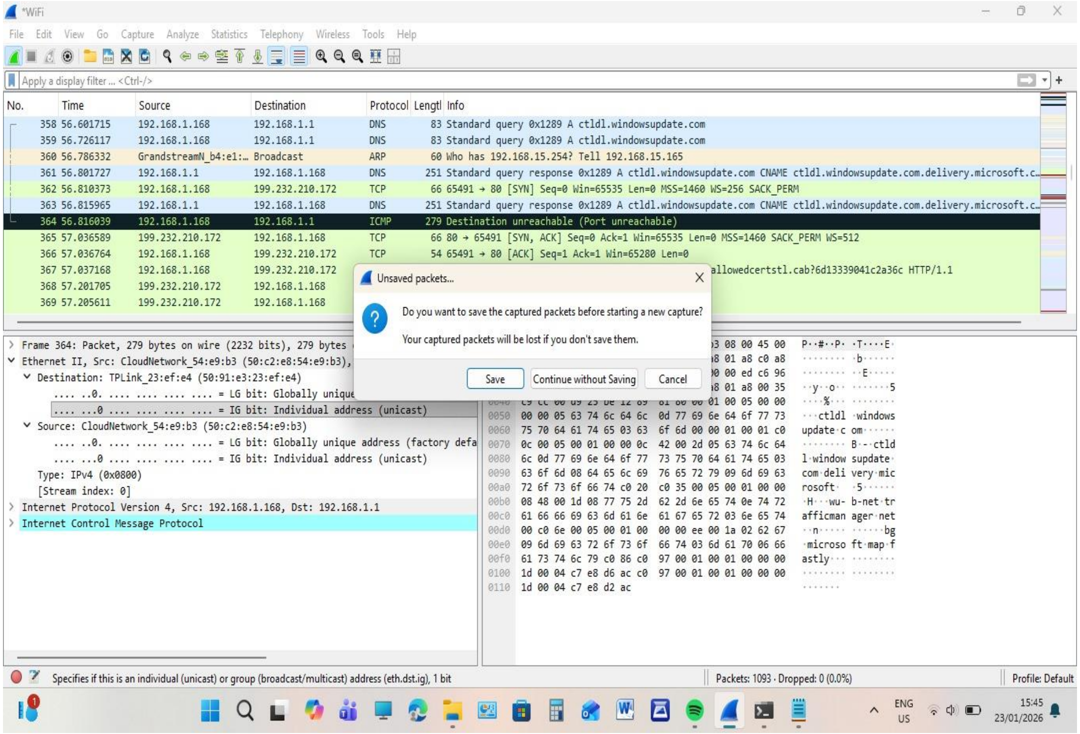
Internet Control Message Protocol: Protocol | Packets: 34854 · Displayed: 26 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6
ENG
US
15:39
23/01/2026

## Part 2: Capture and Analyze Remote ICMP Data in Wireshark

### Step 1: Start capturing data on the interface

(a)


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Unsaved packets...
Save
Continue without Saving
Cancel
ENG
US
15:45
23/01/2026

```
No.  Time       Source                Destination      Protocol Lengtl Info
 358 56.601715  192.168.1.168         192.168.1.1      DNS       83 Standard query 0x1289 A ctldl.windowsupdate.com
 359 56.726117  192.168.1.168         192.168.1.1      DNS       83 Standard query 0x1289 A ctldl.windowsupdate.com
 360 56.786332  GrandstreamN_b4:e1:…  Broadcast        ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
 361 56.801727  192.168.1.1           192.168.1.168    DNS      251 Standard query response 0x1289 A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.c…
 362 56.810373  192.168.1.168         199.232.210.172  TCP       66 65491 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 363 56.815965  192.168.1.1           192.168.1.168    DNS      251 Standard query response 0x1289 A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.c…
 364 56.816039  192.168.1.168         192.168.1.1      ICMP     279 Destination unreachable (Port unreachable)
 365 57.036589  199.232.210.172       192.168.1.168    TCP       66 80 → 65491 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
 366 57.036764  192.168.1.168         199.232.210.172  TCP       54 65491 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 367 57.037168  192.168.1.168         199.232.210.172                allowedcertstl.cab?6d13339041c2a36c HTTP/1.1
 368 57.201705  199.232.210.172       192.168.1.168
 369 57.205611  199.232.210.172       192.168.1.168
```

Do you want to save the captured packets before starting a new capture?

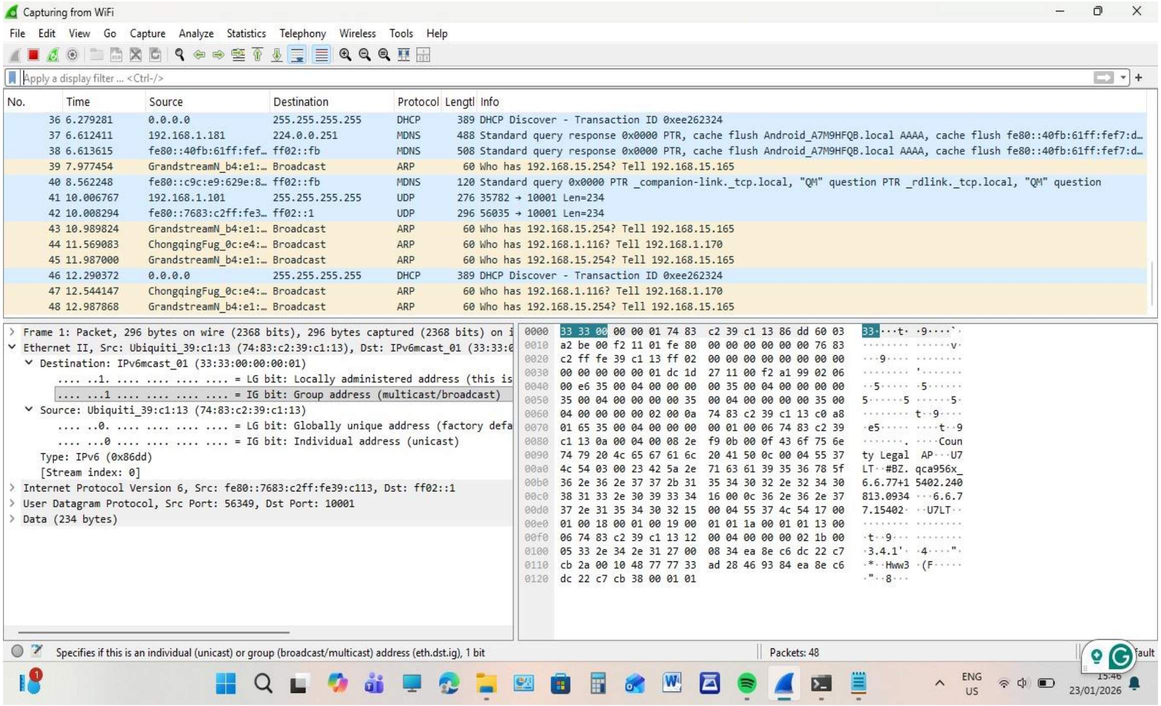
Your captured packets will be lost if you don't save them.

```
> Frame 364: Packet, 279 bytes on wire (2232 bits), 279 bytes
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3),
  v Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
      3 08 00 45 00   P··#··P· ·T····E·
      8 01 a8 c0 a8   ········ ·b······
      0 00 ed c6 96   ········ ··E·····
      8 01 a8 00 35   ··y··o·· ·······5
      01 00 05 00 00  ····%··· ········
0050  00 00 05 63 74 6c 64 6c  0d 77 69 6e 64 6f 77 73   ···ctldl ·windows
0060  75 70 64 61 74 65 03 63  6f 6d 00 00 01 00 01 c0   update·c om······
0070  0c 00 05 00 01 00 00 0c  42 00 2d 05 63 74 6c 64   ········ B·-·ctld
0080  6c 0d 77 69 6e 64 6f 77  73 75 70 64 61 74 65 03   l·window supdate·
0090  63 6f 6d 08 64 65 6c 69  76 65 72 79 09 6d 69 63   com·deli very·mic
00a0  72 6f 73 6f 66 74 c0 20  c0 35 00 05 00 01 00 00   rosoft·  ·5······
00b0  08 48 00 1d 08 77 75 2d  62 2d 6e 65 74 0e 74 72   ·H···wu- b-net·tr
00c0  61 66 66 69 63 6d 61 6e  61 67 65 72 03 6e 65 74   afficman ager·net
00d0  00 c0 6e 00 05 00 01 00  00 00 ee 00 1a 02 62 67   ··n····· ······bg
00e0  09 6d 69 63 72 6f 73 6f  66 74 03 6d 61 70 06 66   ·microso ft·map·f
00f0  61 73 74 6c 79 c0 86 c0  97 00 01 00 01 00 00 00   astly··· ········
0100  1d 00 04 c7 e8 d6 ac c0  97 00 01 00 01 00 00 00   ········ ········
0110  1d 00 04 c7 e8 d2 ac                               ·······
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit | Packets: 1093 · Dropped: 0 (0.0%) | Profile: Default

(b) Then I continue without saving as shown below

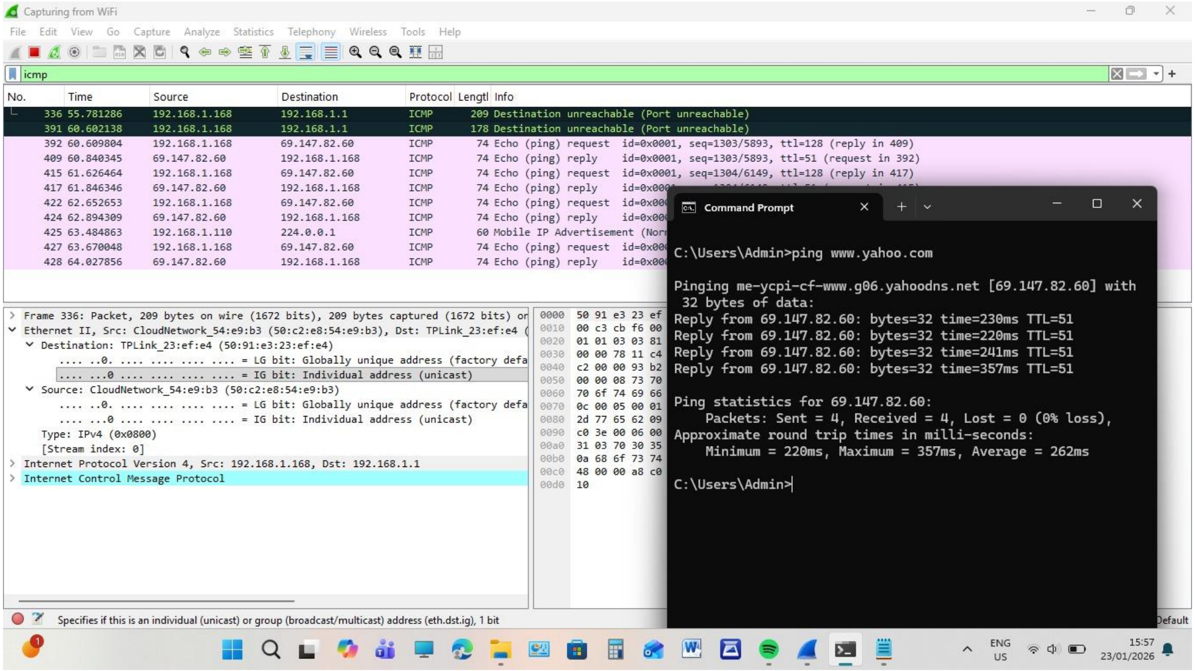

Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ENG
US
15:46
23/01/2026

```
No.  Time       Source                Destination      Protocol Lengtl Info
  36 6.279281   0.0.0.0               255.255.255.255  DHCP     389 DHCP Discover - Transaction ID 0xee262324
  37 6.612411   192.168.1.181         224.0.0.251      MDNS     488 Standard query response 0x0000 PTR, cache flush Android_A7M9HFQB.local AAAA, cache flush fe80::40fb:61ff:fef7:d…
  38 6.613615   fe80::40fb:61ff:fef…  ff02::fb         MDNS     508 Standard query response 0x0000 PTR, cache flush Android_A7M9HFQB.local AAAA, cache flush fe80::40fb:61ff:fef7:d…
  39 7.977454   GrandstreamN_b4:e1:…  Broadcast        ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
  40 8.562248   fe80::c9c:e9:629e:8…  ff02::fb         MDNS     120 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question
  41 10.006767  192.168.1.101         255.255.255.255  UDP      276 35782 → 10001 Len=234
  42 10.008294  fe80::7683:c2ff:fe3…  ff02::1          UDP      296 56035 → 10001 Len=234
  43 10.989824  GrandstreamN_b4:e1:…  Broadcast        ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
  44 11.569083  ChongqingFug_0c:e4:…  Broadcast        ARP       60 Who has 192.168.1.116? Tell 192.168.1.170
  45 11.987000  GrandstreamN_b4:e1:…  Broadcast        ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
  46 12.290372  0.0.0.0               255.255.255.255  DHCP     389 DHCP Discover - Transaction ID 0xee262324
  47 12.544147  ChongqingFug_0c:e4:…  Broadcast        ARP       60 Who has 192.168.1.116? Tell 192.168.1.170
  48 12.987868  GrandstreamN_b4:e1:…  Broadcast        ARP       60 Who has 192.168.15.254? Tell 192.168.15.165
```

```
> Frame 1: Packet, 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on i
v Ethernet II, Src: Ubiquiti_39:c1:13 (74:83:c2:39:c1:13), Dst: IPv6mcast_01 (33:33:0
  v Destination: IPv6mcast_01 (33:33:00:00:00:01)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: Ubiquiti_39:c1:13 (74:83:c2:39:c1:13)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: fe80::7683:c2ff:fe39:c113, Dst: ff02::1
> User Datagram Protocol, Src Port: 56349, Dst Port: 10001
> Data (234 bytes)
```

```
0000  33 33 00 00 00 01 74 83  c2 39 c1 13 86 dd 60 03   33····t· ·9····`·
0010  a2 be 00 f2 11 01 fe 80  00 00 00 00 00 00 76 83   ········ ······v·
0020  c2 ff fe 39 c1 13 ff 02  00 00 00 00 00 00 00 00   ···9···· ········
0030  00 00 00 00 00 01 dc 1d  27 11 00 f2 a1 99 02 06   ········ '·······
0040  00 e6 35 00 04 00 00 00  00 35 00 04 00 00 00 00   ··5····· ·5······
0050  35 00 04 00 00 00 00 35  00 04 00 00 00 00 35 00   5······5 ······5·
0060  04 00 00 00 00 02 00 0a  74 83 c2 39 c1 13 c0 a8   ········ t··9····
0070  01 65 35 00 04 00 00 00  00 01 00 06 74 83 c2 39   ·e5····· ····t··9
0080  c1 13 0a 00 04 00 08 2e  f9 0b 00 0f 43 6f 75 6e   ·······. ····Coun
0090  74 79 20 4c 65 67 61 6c  20 41 50 0c 00 04 55 37   ty Legal  AP···U7
00a0  4c 54 03 00 23 42 5a 2e  71 63 61 39 35 36 78 5f   LT··#BZ. qca956x_
00b0  36 2e 36 2e 37 37 2b 31  35 34 30 32 2e 32 34 30   6.6.77+1 5402.240
00c0  38 31 33 2e 30 39 33 34  16 00 0c 36 2e 36 2e 37   813.0934 ···6.6.7
00d0  37 2e 31 35 34 30 32 15  00 04 55 37 4c 54 17 00   7.15402· ··U7LT··
00e0  01 00 18 00 01 00 19 00  01 01 1a 00 01 01 13 00   ········ ········
00f0  06 74 83 c2 39 c1 13 12  00 04 00 00 00 02 1b 00   ·t··9··· ········
0100  05 33 2e 34 2e 31 27 00  08 34 ea 8e c6 dc 22 c7   ·3.4.1'· ·4····"·
0110  cb 2a 00 10 48 77 77 33  ad 28 46 93 84 ea 8e c6   ·*··Hww3 ·(F·····
0120  dc 22 c7 cb 38 00 01 01                            ·"··8···
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit | Packets: 48 | fault (c): (1) www.yahoo.com



Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source          Destination     Protocol Lengtl Info
  336 55.781286   192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
  391 60.602138   192.168.1.168   192.168.1.1     ICMP     178 Destination unreachable (Port unreachable)
  392 60.609804   192.168.1.168   69.147.82.60    ICMP      74 Echo (ping) request  id=0x0001, seq=1303/5893, ttl=128 (reply in 409)
  409 60.840345   69.147.82.60    192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1303/5893, ttl=51 (request in 392)
  415 61.626464   192.168.1.168   69.147.82.60    ICMP      74 Echo (ping) request  id=0x0001, seq=1304/6149, ttl=128 (reply in 417)
  417 61.846346   69.147.82.60    192.168.1.168   ICMP      74 Echo (ping) reply    id=0x000
  422 62.652653   192.168.1.168   69.147.82.60    ICMP      74 Echo (ping) request  id=0x000
  424 62.894309   69.147.82.60    192.168.1.168   ICMP      74 Echo (ping) reply    id=0x000
  425 63.484863   192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Advertisement (Nor
  427 63.670048   192.168.1.168   69.147.82.60    ICMP      74 Echo (ping) request  id=0x000
  428 64.027856   69.147.82.60    192.168.1.168   ICMP      74 Echo (ping) reply    id=0x000
```

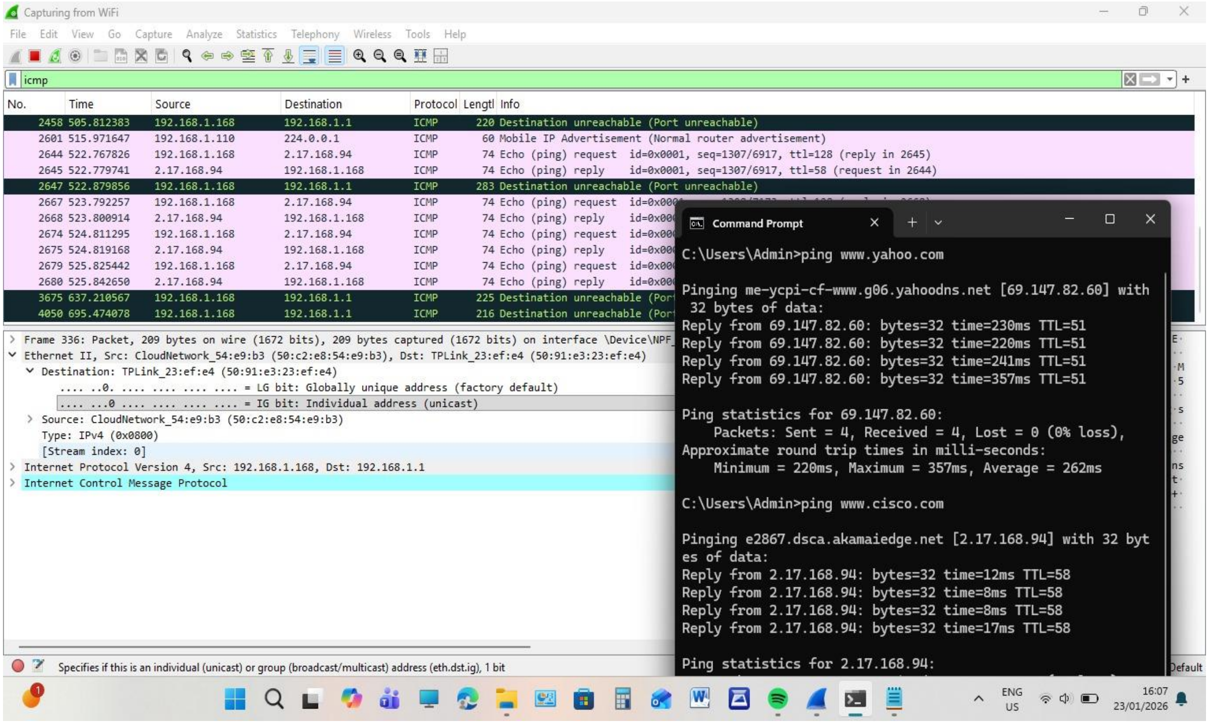
```
> Frame 336: Packet, 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) or
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (
  v Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
0000  50 91 e3 23 ef
0010  00 c3 cb f6 00
0020  01 01 03 03 81
0030  00 00 78 11 c4
0040  c2 00 00 93 b2
0050  00 00 08 73 70
0060  70 6f 74 69 66
0070  0c 00 05 00 01
0080  2d 77 65 62 09
0090  c0 3e 00 06 00
00a0  31 03 70 30 35
00b0  0a 68 6f 73 74
00c0  48 00 00 a8 c0
00d0  10
```

```
C:\Users\Admin>ping www.yahoo.com

Pinging me-ycpi-cf-www.g06.yahoodns.net [69.147.82.60] with
 32 bytes of data:
Reply from 69.147.82.60: bytes=32 time=230ms TTL=51
Reply from 69.147.82.60: bytes=32 time=220ms TTL=51
Reply from 69.147.82.60: bytes=32 time=241ms TTL=51
Reply from 69.147.82.60: bytes=32 time=357ms TTL=51

Ping statistics for 69.147.82.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 220ms, Maximum = 357ms, Average = 262ms

C:\Users\Admin>
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit

(2) www.cisco.com



Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

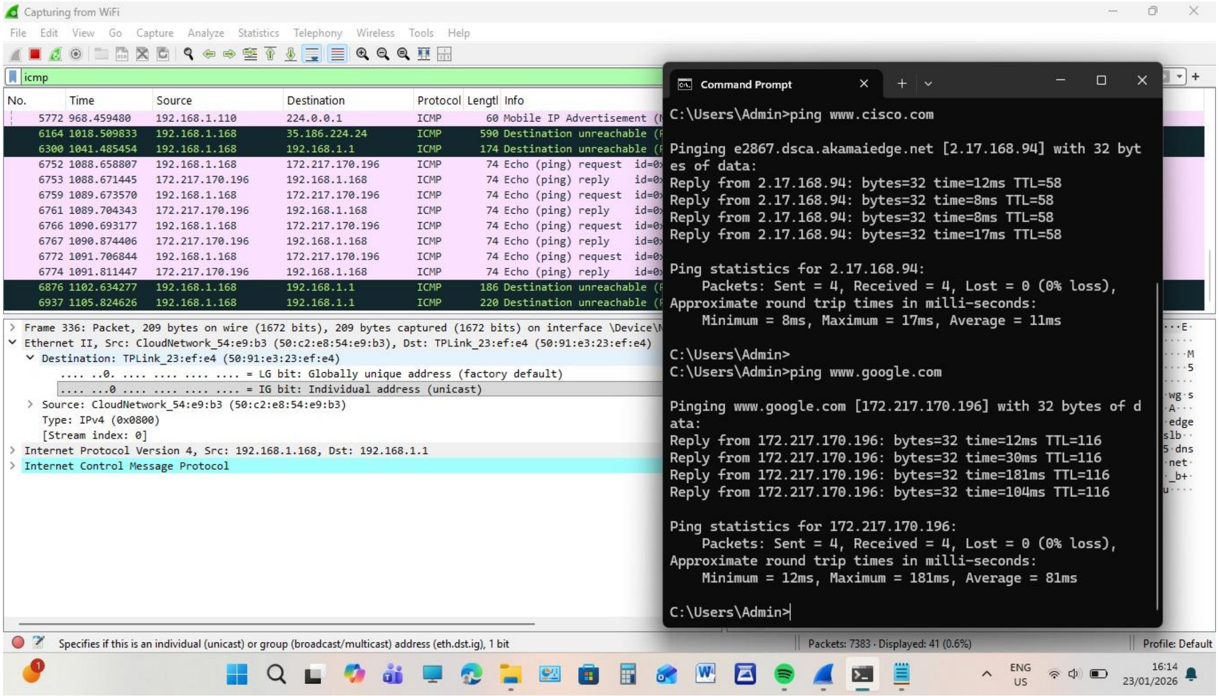
```
No.   Time         Source          Destination     Protocol Lengtl Info
 2458 505.812383   192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
 2601 515.971647   192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Advertisement (Normal router advertisement)
 2644 522.767826   192.168.1.168   2.17.168.94     ICMP      74 Echo (ping) request  id=0x0001, seq=1307/6917, ttl=128 (reply in 2645)
 2645 522.779741   2.17.168.94     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1307/6917, ttl=58 (request in 2644)
 2647 522.879856   192.168.1.168   192.168.1.1     ICMP     283 Destination unreachable (Port unreachable)
 2667 523.792257   192.168.1.168   2.17.168.94     ICMP      74 Echo (ping) request  id=0x000
 2668 523.800914   2.17.168.94     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x000
 2674 524.811295   192.168.1.168   2.17.168.94     ICMP      74 Echo (ping) request  id=0x000
 2675 524.819168   2.17.168.94     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x000
 2679 525.825442   192.168.1.168   2.17.168.94     ICMP      74 Echo (ping) request  id=0x000
 2680 525.842650   2.17.168.94     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x000
 3675 637.210567   192.168.1.168   192.168.1.1     ICMP     225 Destination unreachable (Por
 4050 695.474078   192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Por
```

```
> Frame 336: Packet, 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  v Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
C:\Users\Admin>ping www.yahoo.com

Pinging me-ycpi-cf-www.g06.yahoodns.net [69.147.82.60] with
 32 bytes of data:
Reply from 69.147.82.60: bytes=32 time=230ms TTL=51
Reply from 69.147.82.60: bytes=32 time=220ms TTL=51
Reply from 69.147.82.60: bytes=32 time=241ms TTL=51
Reply from 69.147.82.60: bytes=32 time=357ms TTL=51

Ping statistics for 69.147.82.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 220ms, Maximum = 357ms, Average = 262ms

C:\Users\Admin>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [2.17.168.94] with 32 byt
es of data:
Reply from 2.17.168.94: bytes=32 time=12ms TTL=58
Reply from 2.17.168.94: bytes=32 time=8ms TTL=58
Reply from 2.17.168.94: bytes=32 time=8ms TTL=58
Reply from 2.17.168.94: bytes=32 time=17ms TTL=58

Ping statistics for 2.17.168.94:
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit

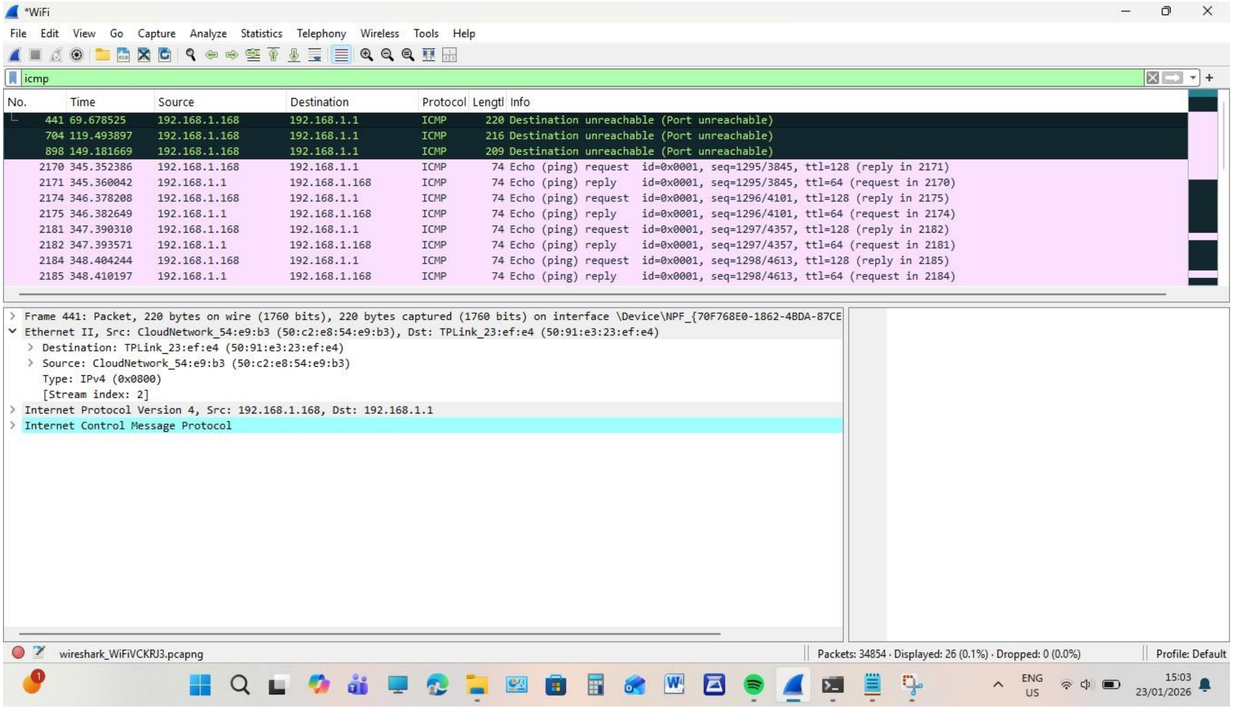
(3) www.google.com



```
Capturing from WiFi
icmp
No.  Time         Source           Destination      Protocol Lengtl Info
5772 968.459480   192.168.1.110    224.0.0.1        ICMP      60 Mobile IP Advertisement (
6164 1018.509833  192.168.1.168    35.186.224.24    ICMP     590 Destination unreachable (
6300 1041.485454  192.168.1.168    192.168.1.1      ICMP     174 Destination unreachable (
6752 1088.658807  192.168.1.168    172.217.170.196  ICMP      74 Echo (ping) request  id=0
6753 1088.671445  172.217.170.196  192.168.1.168    ICMP      74 Echo (ping) reply    id=0
6759 1089.673570  192.168.1.168    172.217.170.196  ICMP      74 Echo (ping) request  id=0
6761 1089.704343  172.217.170.196  192.168.1.168    ICMP      74 Echo (ping) reply    id=0
6766 1090.693177  192.168.1.168    172.217.170.196  ICMP      74 Echo (ping) request  id=0
6767 1090.874406  172.217.170.196  192.168.1.168    ICMP      74 Echo (ping) reply    id=0
6772 1091.706844  192.168.1.168    172.217.170.196  ICMP      74 Echo (ping) request  id=0
6774 1091.811447  172.217.170.196  192.168.1.168    ICMP      74 Echo (ping) reply    id=0
6876 1102.634277  192.168.1.168    192.168.1.1      ICMP     186 Destination unreachable (
6937 1105.824626  192.168.1.168    192.168.1.1      ICMP     220 Destination unreachable (

> Frame 336: Packet, 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  v Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit
Packets: 7383 · Displayed: 41 (0.6%)    Profile: Default
```

```
Command Prompt

C:\Users\Admin>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [2.17.168.94] with 32 byt
es of data:
Reply from 2.17.168.94: bytes=32 time=12ms TTL=58
Reply from 2.17.168.94: bytes=32 time=8ms TTL=58
Reply from 2.17.168.94: bytes=32 time=8ms TTL=58
Reply from 2.17.168.94: bytes=32 time=17ms TTL=58

Ping statistics for 2.17.168.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 17ms, Average = 11ms

C:\Users\Admin>
C:\Users\Admin>ping www.google.com

Pinging www.google.com [172.217.170.196] with 32 bytes of d
ata:
Reply from 172.217.170.196: bytes=32 time=12ms TTL=116
Reply from 172.217.170.196: bytes=32 time=30ms TTL=116
Reply from 172.217.170.196: bytes=32 time=181ms TTL=116
Reply from 172.217.170.196: bytes=32 time=104ms TTL=116

Ping statistics for 172.217.170.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 181ms, Average = 81ms

C:\Users\Admin>
```

(d) Stop capturing the data



```
*WiFi
icmp
No.  Time        Source         Destination    Protocol Lengtl Info
 441 69.678525   192.168.1.168  192.168.1.1    ICMP     220 Destination unreachable (Port unreachable)
 704 119.493897  192.168.1.168  192.168.1.1    ICMP     216 Destination unreachable (Port unreachable)
 898 149.181669  192.168.1.168  192.168.1.1    ICMP     209 Destination unreachable (Port unreachable)
2170 345.352386  192.168.1.168  192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
2171 345.360042  192.168.1.1    192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
2174 346.378208  192.168.1.168  192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
2175 346.382649  192.168.1.1    192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
2181 347.390310  192.168.1.168  192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
2182 347.393571  192.168.1.1    192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
2184 348.404244  192.168.1.168  192.168.1.1    ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
2185 348.410197  192.168.1.1    192.168.1.168  ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)

> Frame 441: Packet, 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{70F768E0-1862-4BDA-87CE
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol

wireshark_WiFiVCKRJ3.pcapng
Packets: 34854 · Displayed: 26 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Step 2: Examining and analyzing the data from the remote hosts

IP address for www.yahoo.com

69.147.82.60

MAC address for www.yahoo.com

50-c2-e8-54-e9-b3 (Default Gateway/Router)

IP address for www.cisco.com

2.17.168.94

MAC address for www.cisco.com

50-c2-e8-54-e9-b3 (Default Gateway /Router)

IP address for www.google.com

172.217.170.196

MAC address for www.google.com

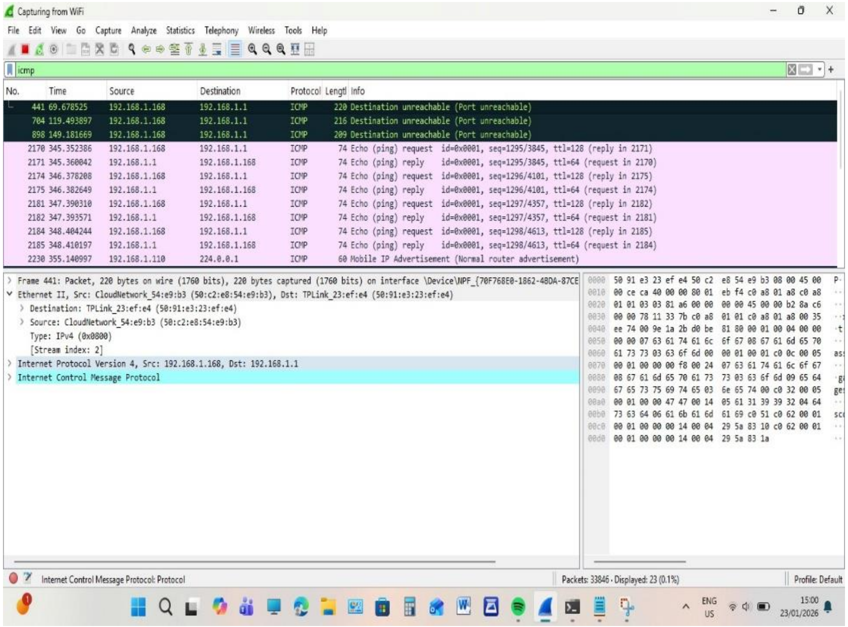
50-c2-e8-54-e9-b3 (Default Gateway /Router)

The significance is that MAC addresses results are the same they are the default gateway

The information differ because when you PING local it returns the MAC address of the PC when you PING remotely it returns MAC address of the default gateway

## Reflection Question

This is because it captures frames on the immediate network segment



Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.   Time         Source          Destination     Protocol Lengtl Info
 441  69.678525    192.168.1.168   192.168.1.1     ICMP     220 Destination unreachable (Port unreachable)
 704  119.493897   192.168.1.168   192.168.1.1     ICMP     216 Destination unreachable (Port unreachable)
 898  149.181669   192.168.1.168   192.168.1.1     ICMP     209 Destination unreachable (Port unreachable)
2170  345.352386   192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1295/3845, ttl=128 (reply in 2171)
2171  345.360042   192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1295/3845, ttl=64 (request in 2170)
2174  346.378208   192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1296/4101, ttl=128 (reply in 2175)
2175  346.382649   192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1296/4101, ttl=64 (request in 2174)
2181  347.390310   192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1297/4357, ttl=128 (reply in 2182)
2182  347.393571   192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1297/4357, ttl=64 (request in 2181)
2184  348.404244   192.168.1.168   192.168.1.1     ICMP      74 Echo (ping) request  id=0x0001, seq=1298/4613, ttl=128 (reply in 2185)
2185  348.410197   192.168.1.1     192.168.1.168   ICMP      74 Echo (ping) reply    id=0x0001, seq=1298/4613, ttl=64 (request in 2184)
2230  355.140997   192.168.1.110   224.0.0.1       ICMP      60 Mobile IP Advertisement (Normal router advertisement)
```

```
> Frame 441: Packet, 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{70F768E0-1862-48DA-87CE
v Ethernet II, Src: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3), Dst: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Destination: TPLink_23:ef:e4 (50:91:e3:23:ef:e4)
  > Source: CloudNetwork_54:e9:b3 (50:c2:e8:54:e9:b3)
    Type: IPv4 (0x0800)
    [Stream index: 2]
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
0000  50 91 e3 23 ef e4 50 c2  e8 54 e9 b3 08 00 45 00   P·
0010  00 ce ca 40 00 00 80 01  eb f4 c0 a8 01 a8 c0 a8   ··
0020  01 01 03 03 81 a6 00 00  00 00 45 00 00 b2 8a c6   ··
0030  00 00 78 11 33 7b c0 a8  01 01 c0 a8 01 a8 00 35   ··
0040  ee 74 00 9e 1a 2b d0 be  81 80 00 01 00 04 00 00   ·t
0050  00 00 07 63 61 74 61 6c  6f 67 08 67 61 6d 65 70   ··
0060  61 73 73 03 63 6f 6d 00  00 01 00 01 c0 0c 00 05   as
0070  00 01 00 00 00 f8 00 24  07 63 61 74 61 6c 6f 67   ··
0080  08 67 61 6d 65 70 61 73  73 03 63 6f 6d 09 65 64   ·g
0090  67 65 73 75 69 74 65 03  6e 65 74 00 c0 32 00 05   ge
00a0  00 01 00 00 47 47 00 14  05 61 31 39 39 32 04 64   ··
00b0  73 63 64 06 61 6b 61 6d  61 69 c0 51 c0 62 00 01   sc
00c0  00 01 00 00 00 14 00 04  29 5a 83 10 c0 62 00 01   ··
00d0  00 01 00 00 00 14 00 04  29 5a 83 1a               ··
```

Internet Control Message Protocol: Protocol

Packets: 33846 · Displayed: 23 (0.1%)

Profile: Default