# Packet analysis using Wireshark

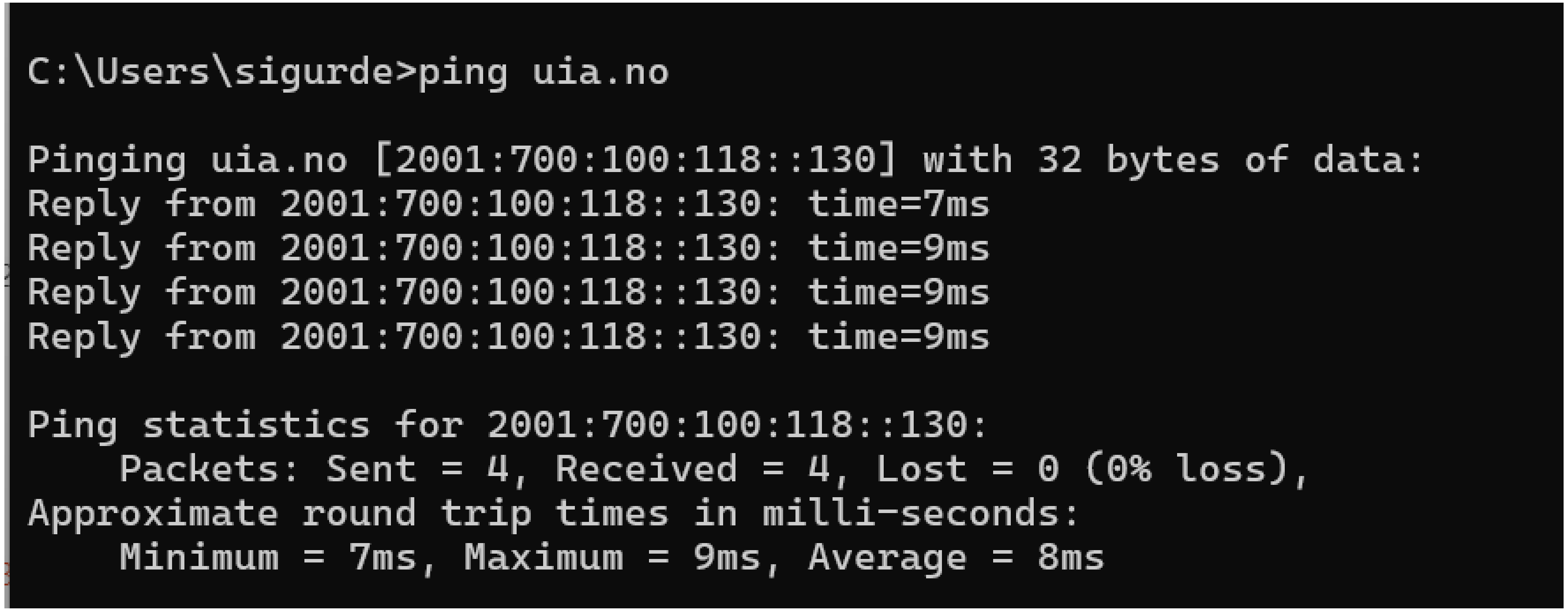
Sigurd Eskeland

# ping command

- *ping* sends four **ICMP** Echo-requests (encapsulated in an IP datagram) to the destination address
- If the specified address is a URL, *ping* will need to do a DNS lookup to get the IP address
  - If the DNS entry does not exist in the local DNS cache, then the host will send a DNS request to the local DNS server (hosted by the IPS)

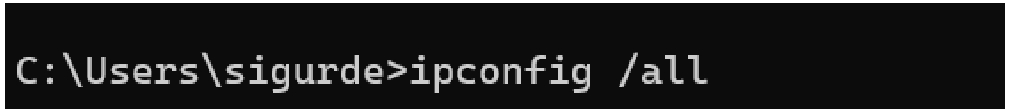
  - The command *nslookup* checks the local DNS cache first.
  - If no proper entry, then the host will send a DNS request to the local DNS server and et mappings from domain names (URL) to IP addresses

# ping output example

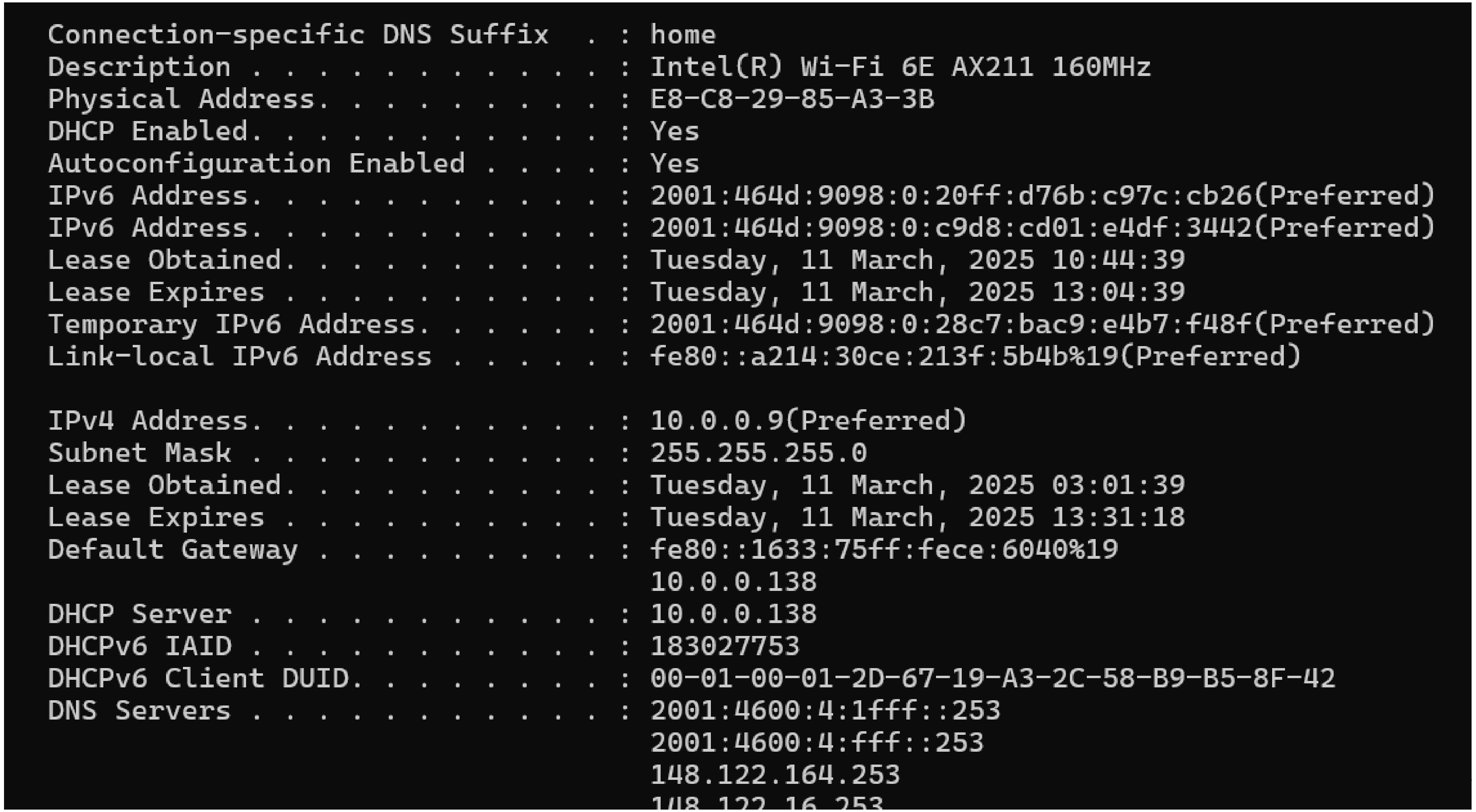


```
C:\Users\sigurde>ping uia.no

Pinging uia.no [2001:700:100:118::130] with 32 bytes of data:
Reply from 2001:700:100:118::130: time=7ms
Reply from 2001:700:100:118::130: time=9ms
Reply from 2001:700:100:118::130: time=9ms
Reply from 2001:700:100:118::130: time=9ms

Ping statistics for 2001:700:100:118::130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 9ms, Average = 8ms
```

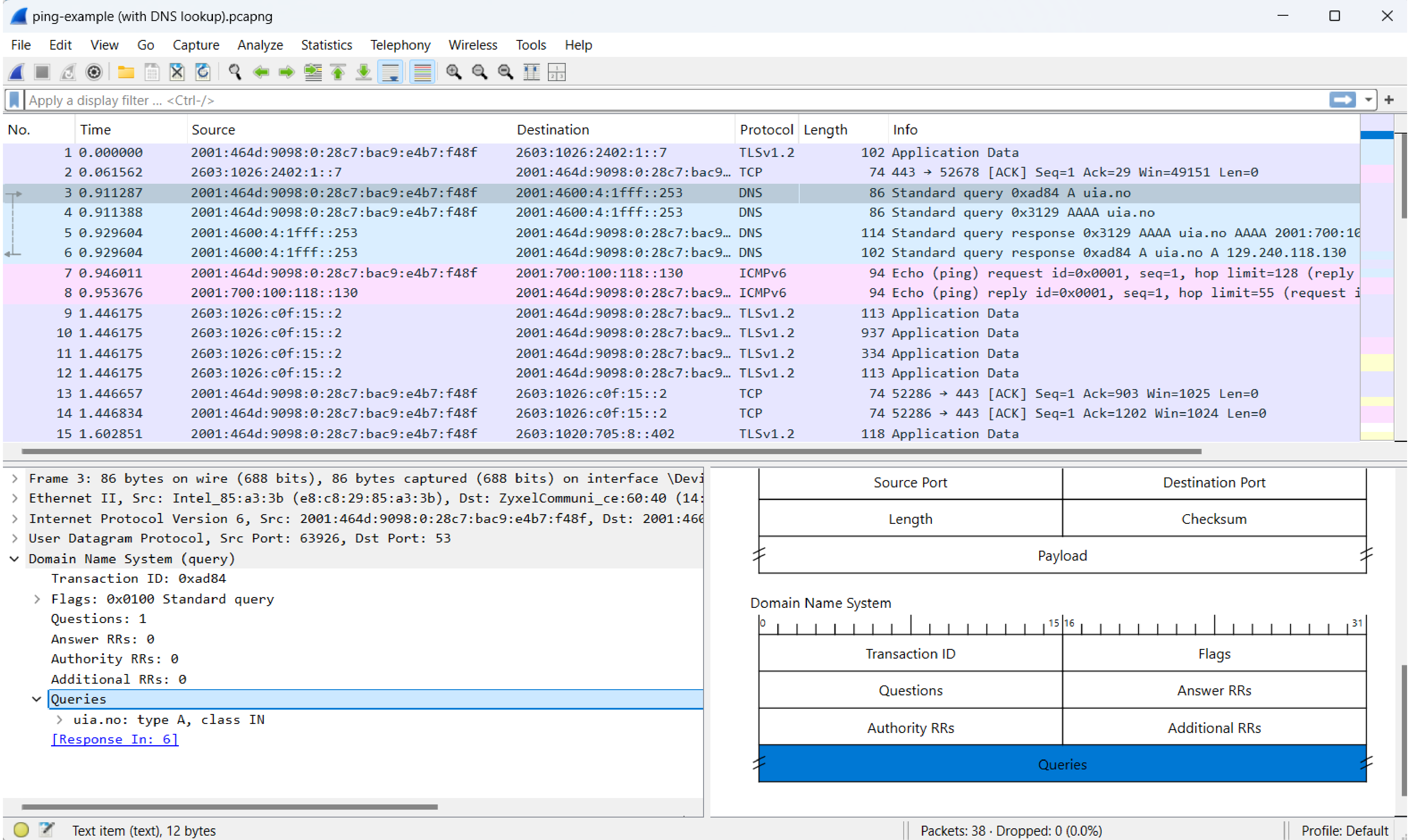
# Checking DNS server IP addresses



```
C:\Users\sigurde>ipconfig /all
```



```
   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
   Physical Address. . . . . . . . . : E8-C8-29-85-A3-3B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:464d:9098:0:20ff:d76b:c97c:cb26(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001:464d:9098:0:c9d8:cd01:e4df:3442(Preferred)
   Lease Obtained. . . . . . . . . . : Tuesday, 11 March, 2025 10:44:39
   Lease Expires . . . . . . . . . . : Tuesday, 11 March, 2025 13:04:39
   Temporary IPv6 Address. . . . . . : 2001:464d:9098:0:28c7:bac9:e4b7:f48f(Preferred)
   Link-local IPv6 Address . . . . . : fe80::a214:30ce:213f:5b4b%19(Preferred)

   IPv4 Address. . . . . . . . . . . : 10.0.0.9(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, 11 March, 2025 03:01:39
   Lease Expires . . . . . . . . . . : Tuesday, 11 March, 2025 13:31:18
   Default Gateway . . . . . . . . . : fe80::1633:75ff:fece:6040%19
                                       10.0.0.138
   DHCP Server . . . . . . . . . . . : 10.0.0.138
   DHCPv6 IAID . . . . . . . . . . . : 183027753
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-19-A3-2C-58-B9-B5-8F-42
   DNS Servers . . . . . . . . . . . : 2001:4600:4:1fff::253
                                       2001:4600:4:fff::253
                                       148.122.164.253
                                       148.122.16.253
```


ping-example (with DNS lookup).pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

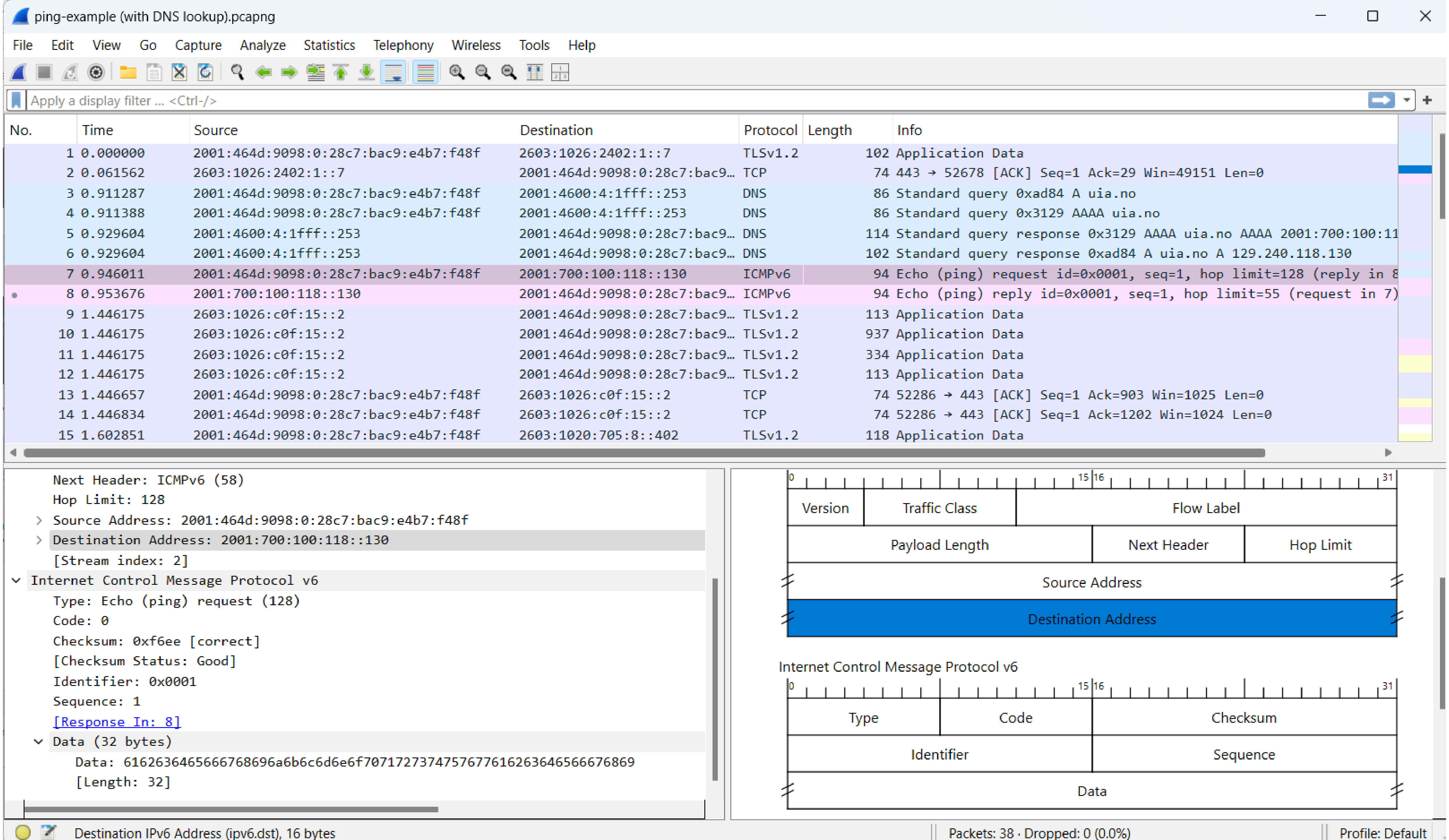
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1026:2402:1::7 | TLSv1.2 | 102 | Application Data |
| 2 | 0.061562 | 2603:1026:2402:1::7 | 2001:464d:9098:0:28c7:bac9… | TCP | 74 | 443 → 52678 [ACK] Seq=1 Ack=29 Win=49151 Len=0 |
| 3 | 0.911287 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2001:4600:4:1fff::253 | DNS | 86 | Standard query 0xad84 A uia.no |
| 4 | 0.911388 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2001:4600:4:1fff::253 | DNS | 86 | Standard query 0x3129 AAAA uia.no |
| 5 | 0.929604 | 2001:4600:4:1fff::253 | 2001:464d:9098:0:28c7:bac9… | DNS | 114 | Standard query response 0x3129 AAAA uia.no AAAA 2001:700:10 |
| 6 | 0.929604 | 2001:4600:4:1fff::253 | 2001:464d:9098:0:28c7:bac9… | DNS | 102 | Standard query response 0xad84 A uia.no A 129.240.118.130 |
| 7 | 0.946011 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2001:700:100:118::130 | ICMPv6 | 94 | Echo (ping) request id=0x0001, seq=1, hop limit=128 (reply |
| 8 | 0.953676 | 2001:700:100:118::130 | 2001:464d:9098:0:28c7:bac9… | ICMPv6 | 94 | Echo (ping) reply id=0x0001, seq=1, hop limit=55 (request i |
| 9 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 113 | Application Data |
| 10 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 937 | Application Data |
| 11 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 334 | Application Data |
| 12 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 113 | Application Data |
| 13 | 1.446657 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1026:c0f:15::2 | TCP | 74 | 52286 → 443 [ACK] Seq=1 Ack=903 Win=1025 Len=0 |
| 14 | 1.446834 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1026:c0f:15::2 | TCP | 74 | 52286 → 443 [ACK] Seq=1 Ack=1202 Win=1024 Len=0 |
| 15 | 1.602851 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1020:705:8::402 | TLSv1.2 | 118 | Application Data |

```
> Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Devi
> Ethernet II, Src: Intel_85:a3:3b (e8:c8:29:85:a3:3b), Dst: ZyxelCommuni_ce:60:40 (14:
> Internet Protocol Version 6, Src: 2001:464d:9098:0:28c7:bac9:e4b7:f48f, Dst: 2001:460
> User Datagram Protocol, Src Port: 63926, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xad84
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > uia.no: type A, class IN
    [Response In: 6]
```

Text item (text), 12 bytes

Packets: 38 · Dropped: 0 (0.0%)

Profile: Default


ping-example (with DNS lookup).pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1026:2402:1::7 | TLSv1.2 | 102 | Application Data |
| 2 | 0.061562 | 2603:1026:2402:1::7 | 2001:464d:9098:0:28c7:bac9… | TCP | 74 | 443 → 52678 [ACK] Seq=1 Ack=29 Win=49151 Len=0 |
| 3 | 0.911287 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2001:4600:4:1fff::253 | DNS | 86 | Standard query 0xad84 A uia.no |
| 4 | 0.911388 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2001:4600:4:1fff::253 | DNS | 86 | Standard query 0x3129 AAAA uia.no |
| 5 | 0.929604 | 2001:4600:4:1fff::253 | 2001:464d:9098:0:28c7:bac9… | DNS | 114 | Standard query response 0x3129 AAAA uia.no AAAA 2001:700:100:11 |
| 6 | 0.929604 | 2001:4600:4:1fff::253 | 2001:464d:9098:0:28c7:bac9… | DNS | 102 | Standard query response 0xad84 A uia.no A 129.240.118.130 |
| 7 | 0.946011 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2001:700:100:118::130 | ICMPv6 | 94 | Echo (ping) request id=0x0001, seq=1, hop limit=128 (reply in 8 |
| 8 | 0.953676 | 2001:700:100:118::130 | 2001:464d:9098:0:28c7:bac9… | ICMPv6 | 94 | Echo (ping) reply id=0x0001, seq=1, hop limit=55 (request in 7) |
| 9 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 113 | Application Data |
| 10 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 937 | Application Data |
| 11 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 334 | Application Data |
| 12 | 1.446175 | 2603:1026:c0f:15::2 | 2001:464d:9098:0:28c7:bac9… | TLSv1.2 | 113 | Application Data |
| 13 | 1.446657 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1026:c0f:15::2 | TCP | 74 | 52286 → 443 [ACK] Seq=1 Ack=903 Win=1025 Len=0 |
| 14 | 1.446834 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1026:c0f:15::2 | TCP | 74 | 52286 → 443 [ACK] Seq=1 Ack=1202 Win=1024 Len=0 |
| 15 | 1.602851 | 2001:464d:9098:0:28c7:bac9:e4b7:f48f | 2603:1020:705:8::402 | TLSv1.2 | 118 | Application Data |

```
    Next Header: ICMPv6 (58)
    Hop Limit: 128
  > Source Address: 2001:464d:9098:0:28c7:bac9:e4b7:f48f
  > Destination Address: 2001:700:100:118::130
    [Stream index: 2]
v Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xf6ee [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 1
    [Response In: 8]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

| 0 … 15 | | 16 … 31 | |
|---|---|---|---|
| Version | Traffic Class | Flow Label | |
| Payload Length | | Next Header | Hop Limit |
| Source Address | | | |
| Destination Address | | | |

Internet Control Message Protocol v6

| 0 … 15 | | 16 … 31 |
|---|---|---|
| Type | Code | Checksum |
| Identifier | | Sequence |
| Data | | |

Destination IPv6 Address (ipv6.dst), 16 bytes

Packets: 38 · Dropped: 0 (0.0%)

Profile: Default

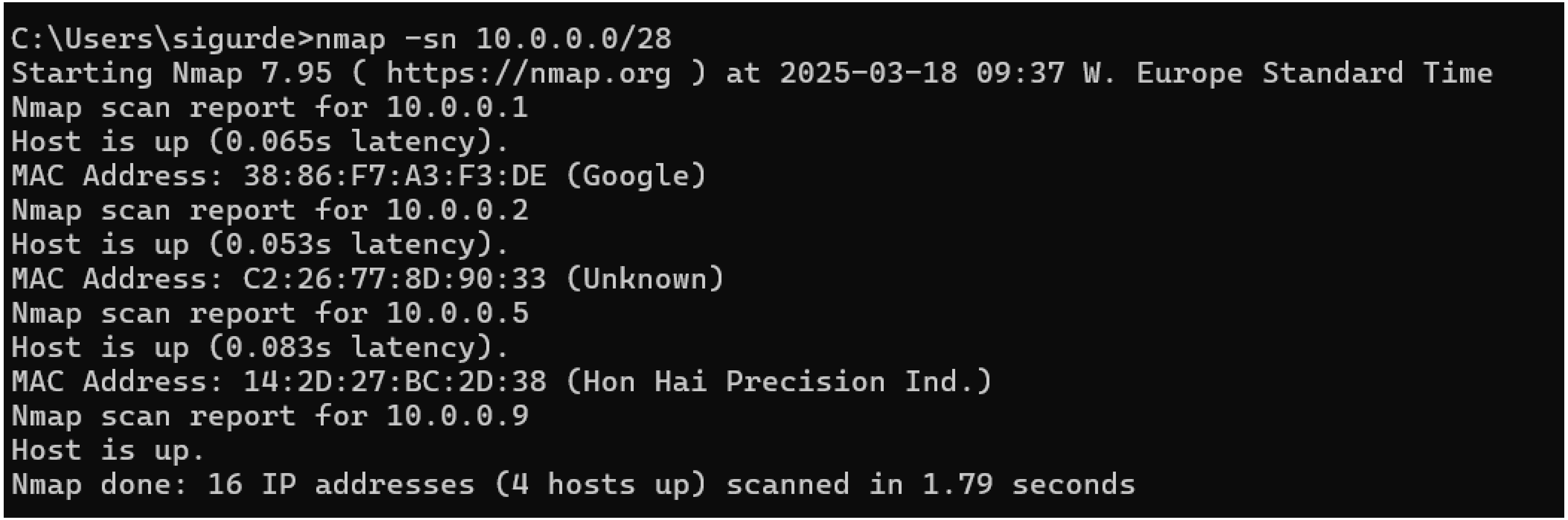
# Show devices connected to the local network

- nmap -sn 192.168.0.0/24
- nmap -sn 10.0.0.0/28

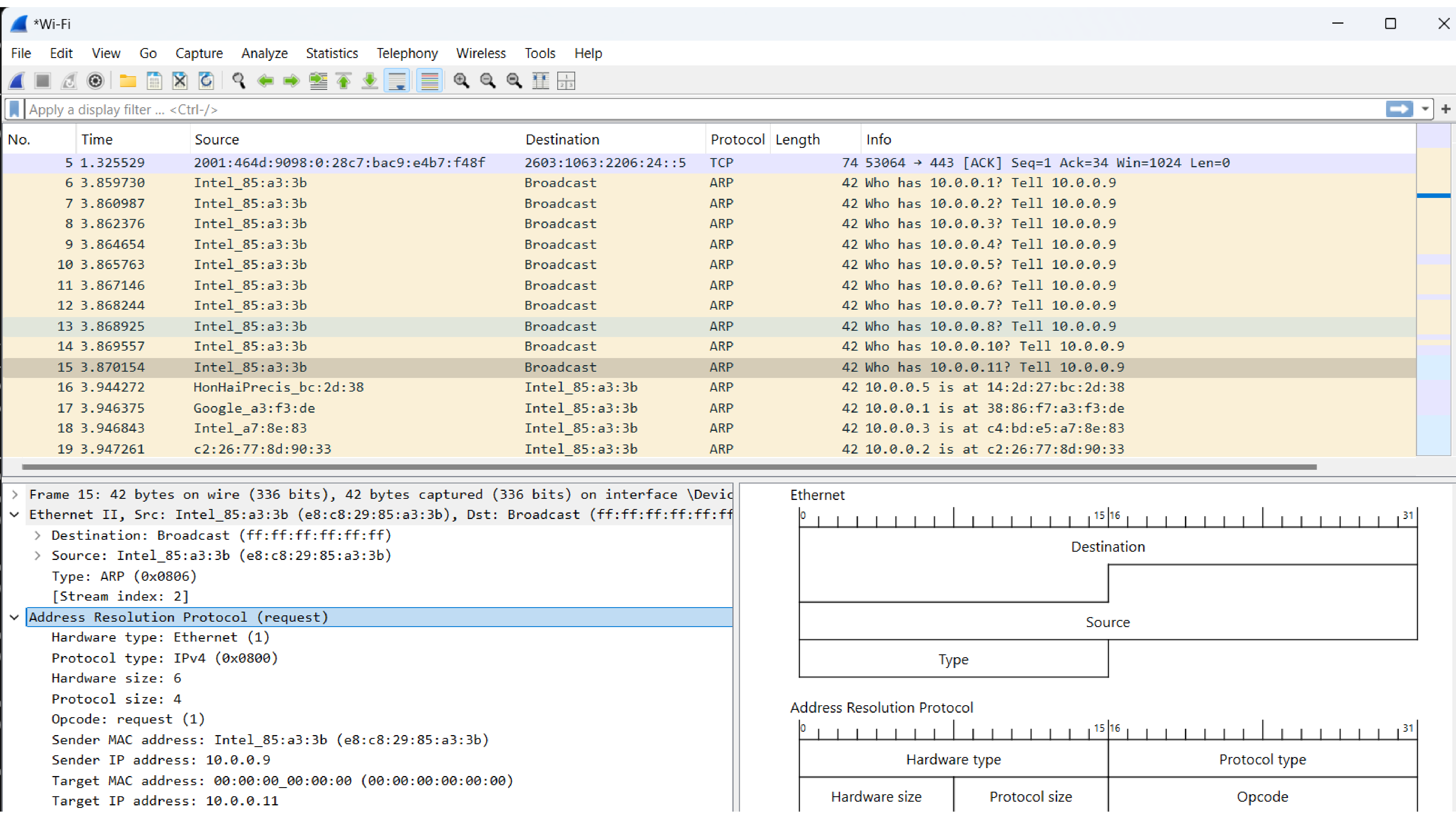
(replacing the subnet with the appropriate one for your LAN)

- nmap broadcast an **ARP request** on the local subset for each IP address in the specified subnet address

# nmap output example

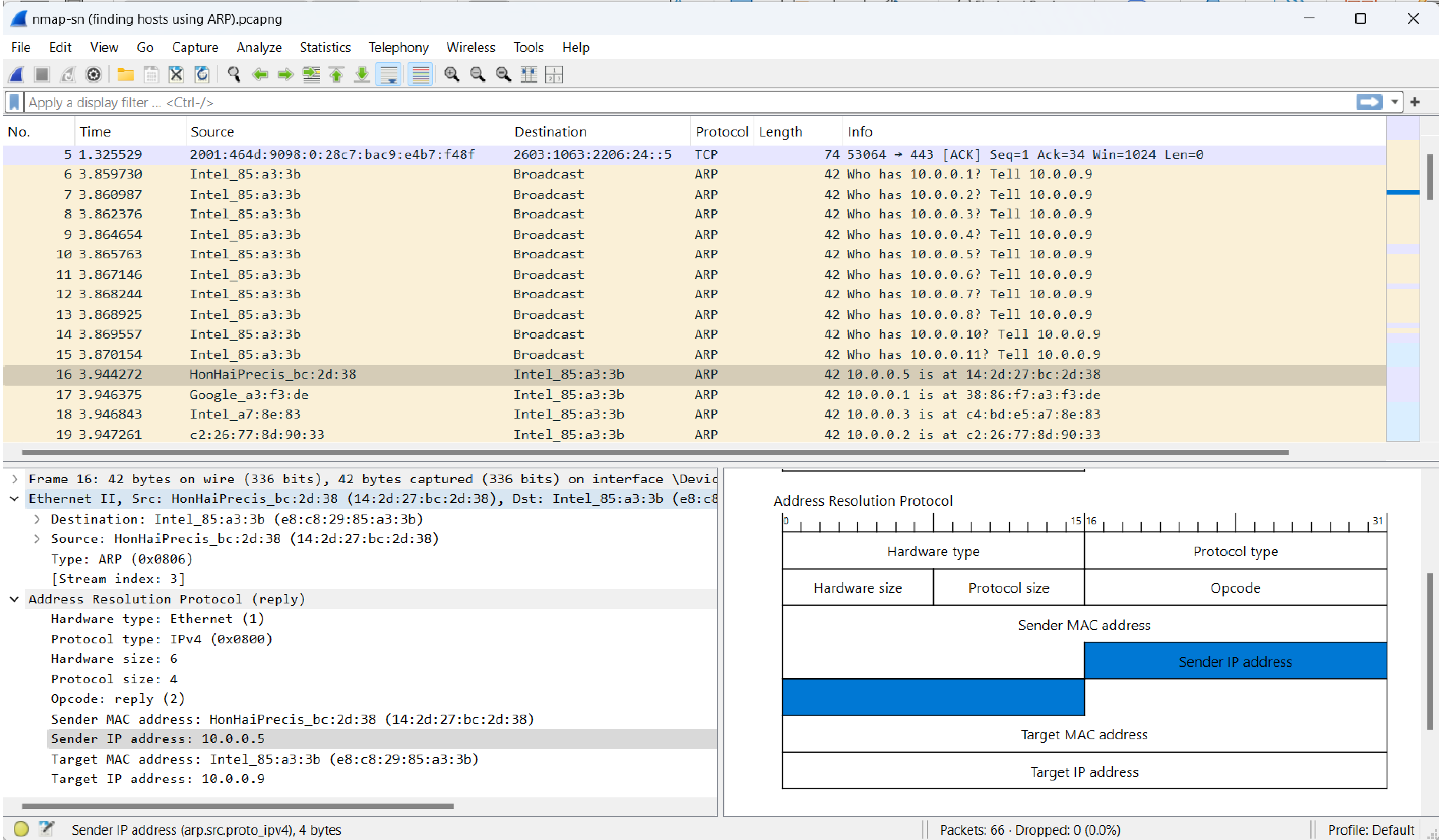


```
C:\Users\sigurde>nmap -sn 10.0.0.0/28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 09:37 W. Europe Standard Time
Nmap scan report for 10.0.0.1
Host is up (0.065s latency).
MAC Address: 38:86:F7:A3:F3:DE (Google)
Nmap scan report for 10.0.0.2
Host is up (0.053s latency).
MAC Address: C2:26:77:8D:90:33 (Unknown)
Nmap scan report for 10.0.0.5
Host is up (0.083s latency).
MAC Address: 14:2D:27:BC:2D:38 (Hon Hai Precision Ind.)
Nmap scan report for 10.0.0.9
Host is up.
Nmap done: 16 IP addresses (4 hosts up) scanned in 1.79 seconds
```



```
No.   Time      Source                                Destination              Protocol  Length  Info
    5 1.325529  2001:464d:9098:0:28c7:bac9:e4b7:f48f  2603:1063:2206:24::5     TCP           74  53064 → 443 [ACK] Seq=1 Ack=34 Win=1024 Len=0
    6 3.859730  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.1? Tell 10.0.0.9
    7 3.860987  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.2? Tell 10.0.0.9
    8 3.862376  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.3? Tell 10.0.0.9
    9 3.864654  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.4? Tell 10.0.0.9
   10 3.865763  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.5? Tell 10.0.0.9
   11 3.867146  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.6? Tell 10.0.0.9
   12 3.868244  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.7? Tell 10.0.0.9
   13 3.868925  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.8? Tell 10.0.0.9
   14 3.869557  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.10? Tell 10.0.0.9
   15 3.870154  Intel_85:a3:3b                        Broadcast                ARP           42  Who has 10.0.0.11? Tell 10.0.0.9
   16 3.944272  HonHaiPrecis_bc:2d:38                 Intel_85:a3:3b           ARP           42  10.0.0.5 is at 14:2d:27:bc:2d:38
   17 3.946375  Google_a3:f3:de                       Intel_85:a3:3b           ARP           42  10.0.0.1 is at 38:86:f7:a3:f3:de
   18 3.946843  Intel_a7:8e:83                        Intel_85:a3:3b           ARP           42  10.0.0.3 is at c4:bd:e5:a7:8e:83
   19 3.947261  c2:26:77:8d:90:33                     Intel_85:a3:3b           ARP           42  10.0.0.2 is at c2:26:77:8d:90:33
```

```
> Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Devic
v Ethernet II, Src: Intel_85:a3:3b (e8:c8:29:85:a3:3b), Dst: Broadcast (ff:ff:ff:ff:ff:ff
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Intel_85:a3:3b (e8:c8:29:85:a3:3b)
    Type: ARP (0x0806)
    [Stream index: 2]
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Intel_85:a3:3b (e8:c8:29:85:a3:3b)
    Sender IP address: 10.0.0.9
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.0.11
```



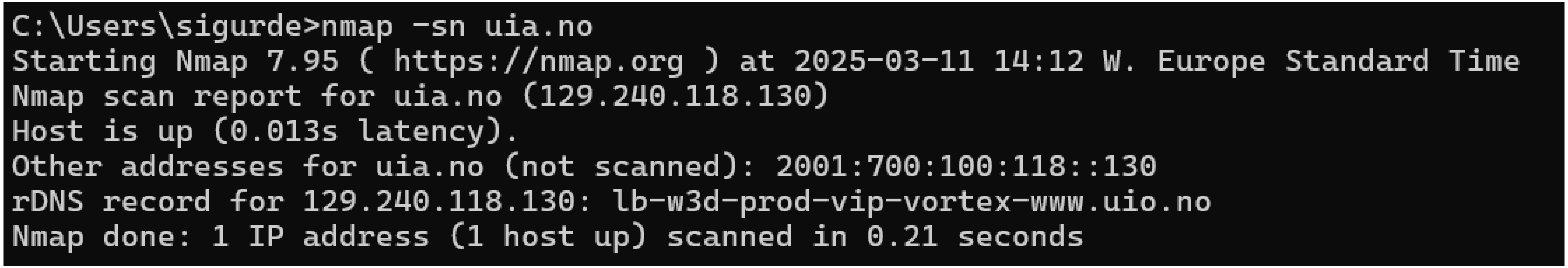
```
No.  Time      Source                                Destination          Protocol Length Info
   5 1.325529  2001:464d:9098:0:28c7:bac9:e4b7:f48f  2603:1063:2206:24::5 TCP          74 53064 → 443 [ACK] Seq=1 Ack=34 Win=1024 Len=0
   6 3.859730  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.1? Tell 10.0.0.9
   7 3.860987  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.2? Tell 10.0.0.9
   8 3.862376  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.3? Tell 10.0.0.9
   9 3.864654  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.4? Tell 10.0.0.9
  10 3.865763  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.5? Tell 10.0.0.9
  11 3.867146  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.6? Tell 10.0.0.9
  12 3.868244  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.7? Tell 10.0.0.9
  13 3.868925  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.8? Tell 10.0.0.9
  14 3.869557  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.10? Tell 10.0.0.9
  15 3.870154  Intel_85:a3:3b                        Broadcast            ARP          42 Who has 10.0.0.11? Tell 10.0.0.9
  16 3.944272  HonHaiPrecis_bc:2d:38                 Intel_85:a3:3b       ARP          42 10.0.0.5 is at 14:2d:27:bc:2d:38
  17 3.946375  Google_a3:f3:de                       Intel_85:a3:3b       ARP          42 10.0.0.1 is at 38:86:f7:a3:f3:de
  18 3.946843  Intel_a7:8e:83                        Intel_85:a3:3b       ARP          42 10.0.0.3 is at c4:bd:e5:a7:8e:83
  19 3.947261  c2:26:77:8d:90:33                     Intel_85:a3:3b       ARP          42 10.0.0.2 is at c2:26:77:8d:90:33
```

```
> Frame 16: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Devic
v Ethernet II, Src: HonHaiPrecis_bc:2d:38 (14:2d:27:bc:2d:38), Dst: Intel_85:a3:3b (e8:c8
  > Destination: Intel_85:a3:3b (e8:c8:29:85:a3:3b)
  > Source: HonHaiPrecis_bc:2d:38 (14:2d:27:bc:2d:38)
    Type: ARP (0x0806)
    [Stream index: 3]
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: HonHaiPrecis_bc:2d:38 (14:2d:27:bc:2d:38)
    Sender IP address: 10.0.0.5
    Target MAC address: Intel_85:a3:3b (e8:c8:29:85:a3:3b)
    Target IP address: 10.0.0.9
```

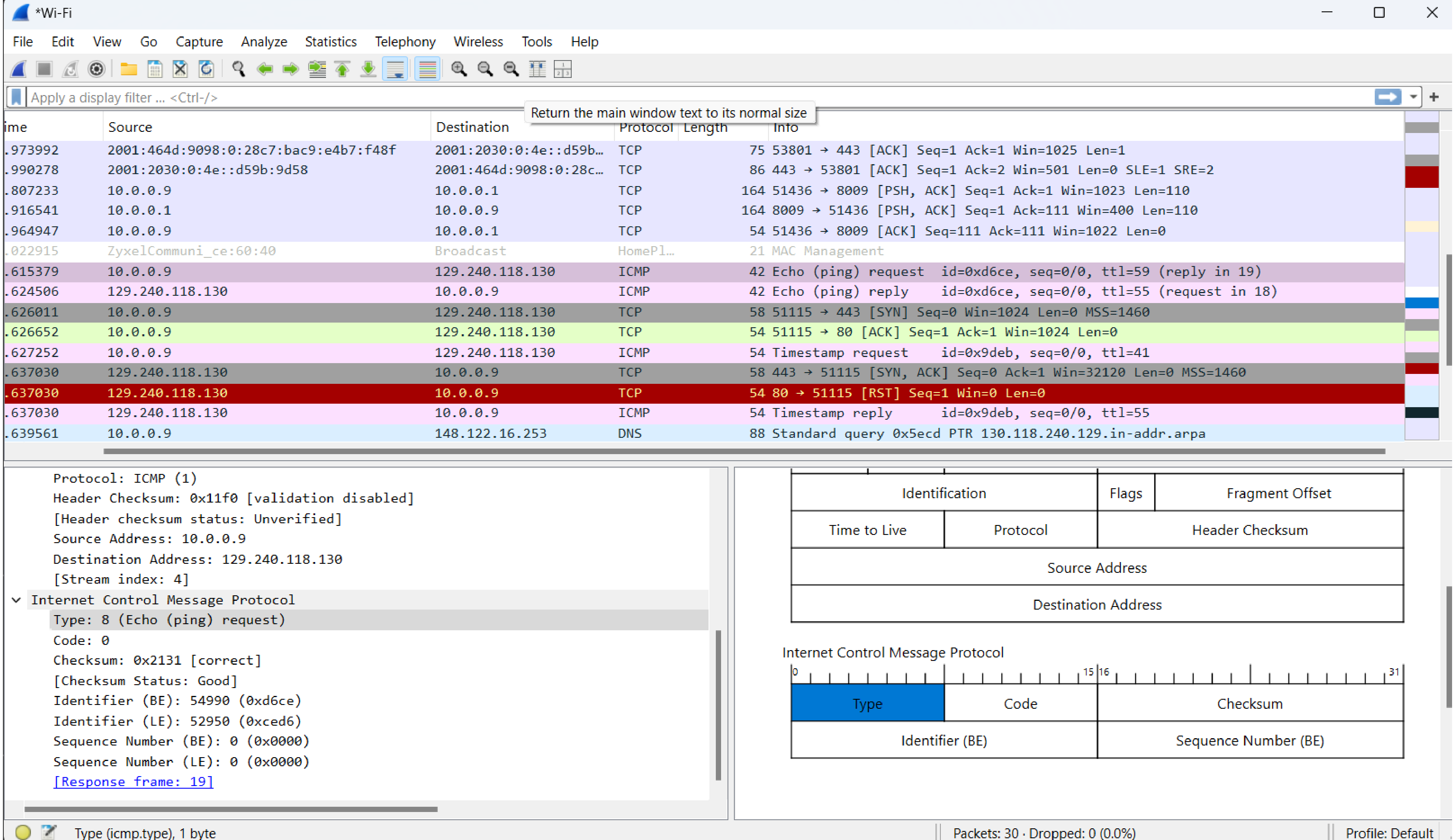
Sender IP address (arp.src.proto_ipv4), 4 bytes | Packets: 66 · Dropped: 0 (0.0%) | Profile: Default

# Another nmap example

- When looking up an *external* server, nmap sends an ICMP request



```
C:\Users\sigurde>nmap -sn uia.no
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-11 14:12 W. Europe Standard Time
Nmap scan report for uia.no (129.240.118.130)
Host is up (0.013s latency).
Other addresses for uia.no (not scanned): 2001:700:100:118::130
rDNS record for 129.240.118.130: lb-w3d-prod-vip-vortex-www.uio.no
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```



Return the main window text to its normal size

```
ime       Source                              Destination              Protocol Length Info
.973992   2001:464d:9098:0:28c7:bac9:e4b7:f48f 2001:2030:0:4e::d59b…   TCP          75 53801 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1
.990278   2001:2030:0:4e::d59b:9d58           2001:464d:9098:0:28c…    TCP          86 443 → 53801 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
.807233   10.0.0.9                            10.0.0.1                 TCP         164 51436 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=1023 Len=110
.916541   10.0.0.1                            10.0.0.9                 TCP         164 8009 → 51436 [PSH, ACK] Seq=1 Ack=111 Win=400 Len=110
.964947   10.0.0.9                            10.0.0.1                 TCP          54 51436 → 8009 [ACK] Seq=111 Ack=111 Win=1022 Len=0
.022915   ZyxelCommuni_ce:60:40               Broadcast                HomePl…      21 MAC Management
.615379   10.0.0.9                            129.240.118.130          ICMP         42 Echo (ping) request  id=0xd6ce, seq=0/0, ttl=59 (reply in 19)
.624506   129.240.118.130                     10.0.0.9                 ICMP         42 Echo (ping) reply    id=0xd6ce, seq=0/0, ttl=55 (request in 18)
.626011   10.0.0.9                            129.240.118.130          TCP          58 51115 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.626652   10.0.0.9                            129.240.118.130          TCP          54 51115 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
.627252   10.0.0.9                            129.240.118.130          ICMP         54 Timestamp request    id=0x9deb, seq=0/0, ttl=41
.637030   129.240.118.130                     10.0.0.9                 TCP          58 443 → 51115 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460
.637030   129.240.118.130                     10.0.0.9                 TCP          54 80 → 51115 [RST] Seq=1 Win=0 Len=0
.637030   129.240.118.130                     10.0.0.9                 ICMP         54 Timestamp reply      id=0x9deb, seq=0/0, ttl=55
.639561   10.0.0.9                            148.122.16.253           DNS          88 Standard query 0x5ecd PTR 130.118.240.129.in-addr.arpa
```

```
    Protocol: ICMP (1)
    Header Checksum: 0x11f0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.0.9
    Destination Address: 129.240.118.130
    [Stream index: 4]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2131 [correct]
    [Checksum Status: Good]
    Identifier (BE): 54990 (0xd6ce)
    Identifier (LE): 52950 (0xced6)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 19]
```

| | | | |
|---|---|---|---|
| Identification | | Flags | Fragment Offset |
| Time to Live | Protocol | Header Checksum | |
| Source Address | | | |
| Destination Address | | | |

Internet Control Message Protocol

| | | |
|---|---|---|
| Type | Code | Checksum |
| Identifier (BE) | | Sequence Number (BE) |

Type (icmp.type), 1 byte

Packets: 30 · Dropped: 0 (0.0%)

Profile: Default