Διαχείριση Δικτύων Βασισμένων στο Λογισμικό
3^{o} εργαστήριο: “ICMP-Ethernet/ARP”

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:	Νικόλας Μαυρόπουλος
Α.Μ.:	it21865

ICMP lab

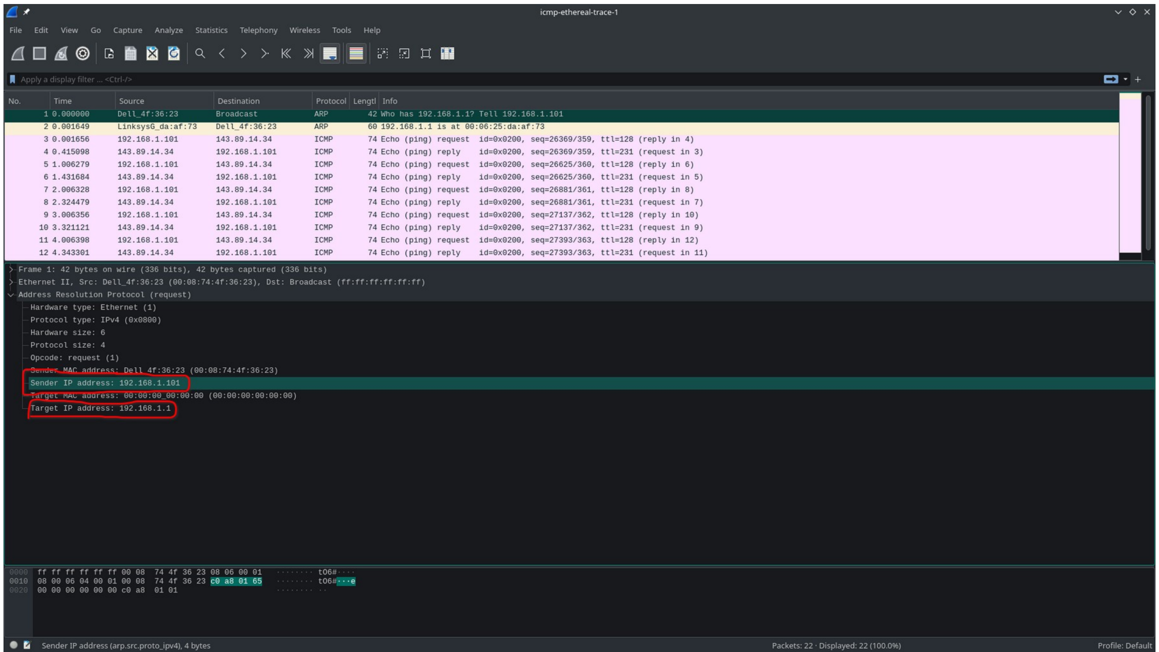
Please provide screenshots to justify your answers to the following questions (the minimum number of screenshots needed – and “to the point” data from these screenshots):

1. What is the IP address of your host? What is the IP address of the destination host?
   My host: 192.168.1.101 Destination host: 192.168.1.1

2. Why is it that an ICMP packet does not have source and destination port numbers?
   It is using network layer so source and destination port numbers are not needed.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have?
   Type: 8   Code: 0, The ICMP has also checksum, identifier and sequence number fields

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have?
   Type: 0   Code:0, This ICMP has checksum, identifier and sequence number fields



```
No.  Time      Source             Destination     Protocol Lengtl Info
   1 0.000000  Dell_4f:36:23      Broadcast       ARP        42 Who has 192.168.1.1? Tell 192.168.1.101
   2 0.001649  LinksysG_da:af:73  Dell_4f:36:23   ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 0.001656  192.168.1.101      143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=26369/359, ttl=128 (reply in 4)
   4 0.415098  143.89.14.34       192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=26369/359, ttl=231 (request in 3)
   5 1.006279  192.168.1.101      143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=26625/360, ttl=128 (reply in 6)
   6 1.431684  143.89.14.34       192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=26625/360, ttl=231 (request in 5)
   7 2.006328  192.168.1.101      143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=26881/361, ttl=128 (reply in 8)
   8 2.324479  143.89.14.34       192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=26881/361, ttl=231 (request in 7)
   9 3.006356  192.168.1.101      143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=27137/362, ttl=128 (reply in 10)
  10 3.321121  143.89.14.34       192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=27137/362, ttl=231 (request in 9)
  11 4.006398  192.168.1.101      143.89.14.34    ICMP       74 Echo (ping) request  id=0x0200, seq=27393/363, ttl=128 (reply in 12)
  12 4.343301  143.89.14.34       192.168.1.101   ICMP       74 Echo (ping) reply    id=0x0200, seq=27393/363, ttl=231 (request in 11)
```

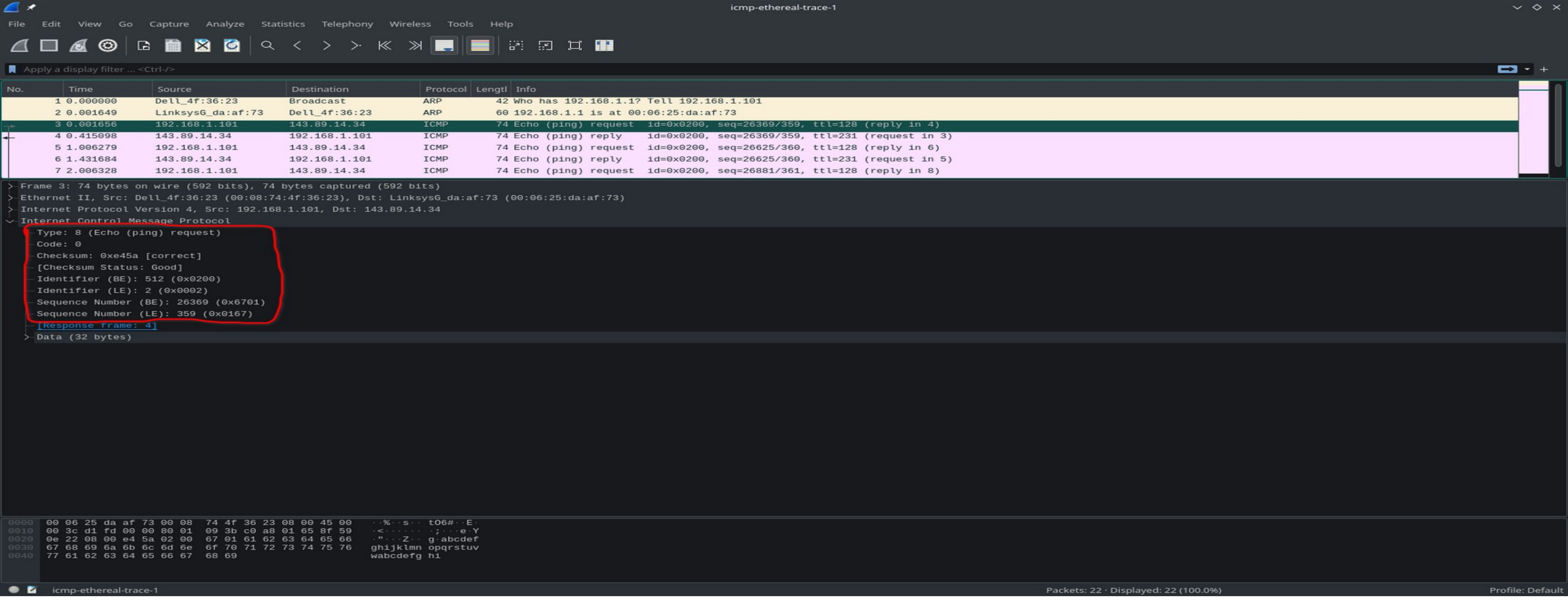
```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    Sender IP address: 192.168.1.101
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 06 00 01   ········ tO6#····
0010  08 00 06 04 00 01 00 08  74 4f 36 23 c0 a8 01 65   ········ tO6#···e
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

Sender IP address (arp.src.proto_ipv4), 4 bytes

Packets: 22 · Displayed: 22 (100.0%)

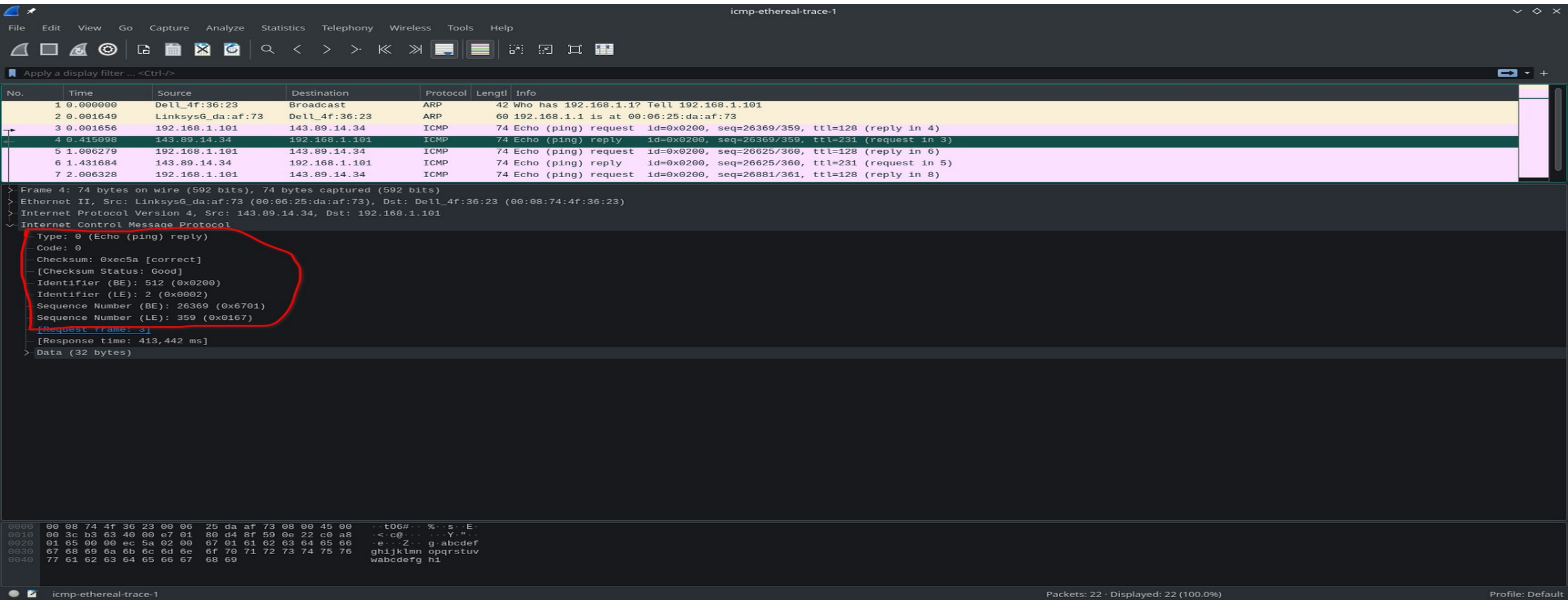
Profile: Default


icmp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packets: 22 · Displayed: 22 (100.0%)
Profile: Default

```
No.   Time       Source              Destination        Protocol Lengtl Info
    1 0.000000   Dell_4f:36:23       Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.101
    2 0.001649   LinksysG_da:af:73   Dell_4f:36:23      ARP        60 192.168.1.1 is at 00:06:25:da:af:73
    3 0.001656   192.168.1.101       143.89.14.34       ICMP       74 Echo (ping) request  id=0x0200, seq=26369/359, ttl=128 (reply in 4)
    4 0.415098   143.89.14.34        192.168.1.101      ICMP       74 Echo (ping) reply    id=0x0200, seq=26369/359, ttl=231 (request in 3)
    5 1.006279   192.168.1.101       143.89.14.34       ICMP       74 Echo (ping) request  id=0x0200, seq=26625/360, ttl=128 (reply in 6)
    6 1.431684   143.89.14.34        192.168.1.101      ICMP       74 Echo (ping) reply    id=0x0200, seq=26625/360, ttl=231 (request in 5)
    7 2.006328   192.168.1.101       143.89.14.34       ICMP       74 Echo (ping) request  id=0x0200, seq=26881/361, ttl=128 (reply in 8)
```

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe45a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Response frame: 4]
  > Data (32 bytes)
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  00 3c d1 fd 00 00 80 01  09 3b c0 a8 01 65 8f 59   ·<······ ·;···e·Y
0020  0e 22 08 00 e4 5a 02 00  67 01 61 62 63 64 65 66   ·"···Z·· g·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
```


icmp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packets: 22 · Displayed: 22 (100.0%)
Profile: Default

```
No.   Time       Source              Destination        Protocol Lengtl Info
    1 0.000000   Dell_4f:36:23       Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.101
    2 0.001649   LinksysG_da:af:73   Dell_4f:36:23      ARP        60 192.168.1.1 is at 00:06:25:da:af:73
    3 0.001656   192.168.1.101       143.89.14.34       ICMP       74 Echo (ping) request  id=0x0200, seq=26369/359, ttl=128 (reply in 4)
    4 0.415098   143.89.14.34        192.168.1.101      ICMP       74 Echo (ping) reply    id=0x0200, seq=26369/359, ttl=231 (request in 3)
    5 1.006279   192.168.1.101       143.89.14.34       ICMP       74 Echo (ping) request  id=0x0200, seq=26625/360, ttl=128 (reply in 6)
    6 1.431684   143.89.14.34        192.168.1.101      ICMP       74 Echo (ping) reply    id=0x0200, seq=26625/360, ttl=231 (request in 5)
    7 2.006328   192.168.1.101       143.89.14.34       ICMP       74 Echo (ping) request  id=0x0200, seq=26881/361, ttl=128 (reply in 8)
```

```
> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 143.89.14.34, Dst: 192.168.1.101
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xec5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Request frame: 3]
    [Response time: 413,442 ms]
  > Data (32 bytes)
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  00 3c b3 63 40 00 e7 01  80 d4 8f 59 0e 22 c0 a8   ·<·c@··· ···Y·"··
0020  01 65 00 00 ec 5a 02 00  67 01 61 62 63 64 65 66   ·e···Z·· g·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
```

5. What is the IP address of your host? What is the IP address of the target destination host?
   My host: 192.168.1.101 Destination host: 138.96.146.2

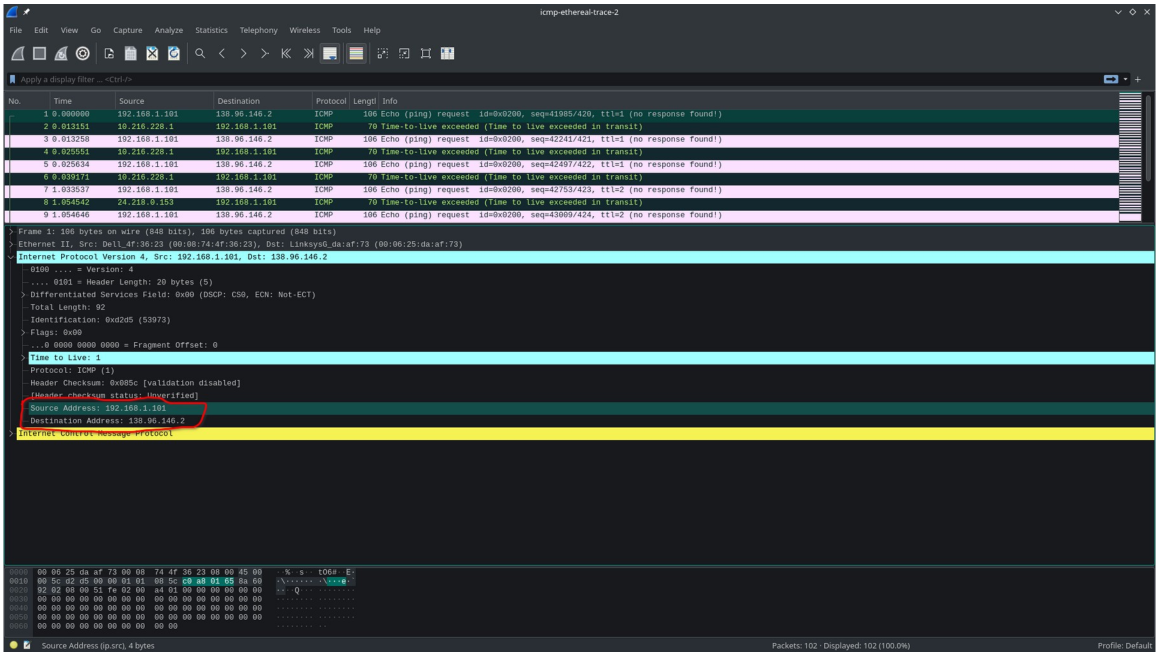
6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be? (Reverse this question if you use LINUX).
   If ICMP sent UDP packets instead then the IP protocol number wouldn't be 01, it would be 0x11

7. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
   It contains the IP header and the first 8 bytes of the original ICMP packet

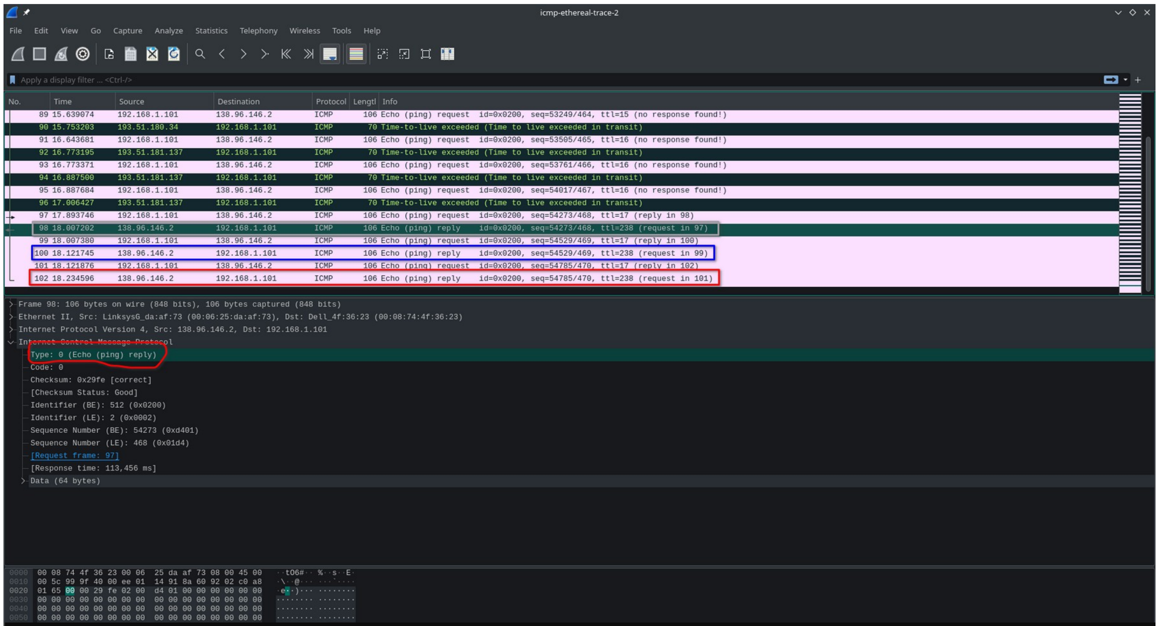
8. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

They all have Type: 0. They are different because they made its destination to the host before TTL expired.

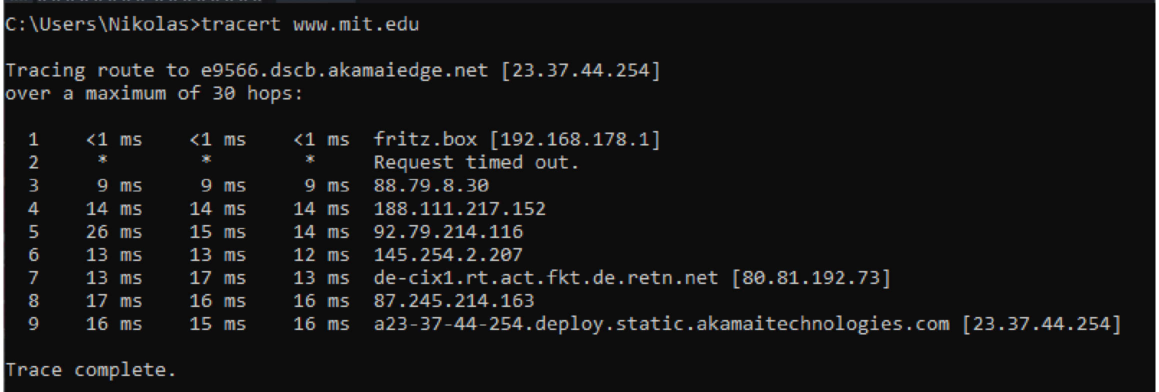
9. Perform traceroute for www.mit.edu. Within the tracert measurements, is there a link whose delay is significantly longer than others?
There is a link between steps 4 and 5 that has a longer delay, than all the other links


icmp-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination    Protocol Lengtl Info
   1 0.000000   192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=41985/420, ttl=1 (no response found!)
   2 0.013151   10.216.228.1    192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   3 0.013258   192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=42241/421, ttl=1 (no response found!)
   4 0.025551   10.216.228.1    192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   5 0.025634   192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=42497/422, ttl=1 (no response found!)
   6 0.039171   10.216.228.1    192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   7 1.033537   192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=42753/423, ttl=2 (no response found!)
   8 1.054542   24.218.0.153    192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   9 1.054646   192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=43009/424, ttl=2 (no response found!)

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xd2d5 (53973)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x085c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.101
    Destination Address: 138.96.146.2
> Internet Control Message Protocol

0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  00 5c d2 d5 00 00 01 01  08 5c c0 a8 01 65 8a 60   ·\······ ·\···e·`
0020  92 02 08 00 51 fe 02 00  a4 01 00 00 00 00 00 00   ····Q··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··

Source Address (ip.src), 4 bytes          Packets: 102 · Displayed: 102 (100.0%)          Profile: Default
```


icmp-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination    Protocol Lengtl Info
  89 15.639074  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=53249/464, ttl=15 (no response found!)
  90 15.753203  193.51.180.34   192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  91 16.643681  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=53505/465, ttl=16 (no response found!)
  92 16.773195  193.51.181.137  192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  93 16.773371  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=53761/466, ttl=16 (no response found!)
  94 16.887500  193.51.181.137  192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  95 16.887684  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54017/467, ttl=16 (no response found!)
  96 17.006427  193.51.181.137  192.168.1.101  ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  97 17.893746  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54273/468, ttl=17 (reply in 98)
  98 18.007202  138.96.146.2    192.168.1.101  ICMP     106 Echo (ping) reply    id=0x0200, seq=54273/468, ttl=238 (request in 97)
  99 18.007380  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54529/469, ttl=17 (reply in 100)
 100 18.121745  138.96.146.2    192.168.1.101  ICMP     106 Echo (ping) reply    id=0x0200, seq=54529/469, ttl=238 (request in 99)
 101 18.121876  192.168.1.101   138.96.146.2   ICMP     106 Echo (ping) request  id=0x0200, seq=54785/470, ttl=17 (reply in 102)
 102 18.234596  138.96.146.2    192.168.1.101  ICMP     106 Echo (ping) reply    id=0x0200, seq=54785/470, ttl=238 (request in 101)

> Frame 98: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 138.96.146.2, Dst: 192.168.1.101
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x29fe [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 54273 (0xd401)
    Sequence Number (LE): 468 (0x01d4)
    [Request frame: 97]
    [Response time: 113,456 ms]
  > Data (64 bytes)

0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  00 5c 99 9f 40 00 ee 01  14 91 8a 60 92 02 c0 a8   ·\··@··· ···`····
0020  01 65 00 00 29 fe 02 00  d4 01 00 00 00 00 00 00   ·e··)··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```



```
C:\Users\Nikolas>tracert www.mit.edu

Tracing route to e9566.dscb.akamaiedge.net [23.37.44.254]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  fritz.box [192.168.178.1]
  2     *        *        *     Request timed out.
  3     9 ms     9 ms     9 ms  88.79.8.30
  4    14 ms    14 ms    14 ms  188.111.217.152
  5    26 ms    15 ms    14 ms  92.79.214.116
  6    13 ms    13 ms    12 ms  145.254.2.207
  7    13 ms    17 ms    13 ms  de-cix1.rt.act.fkt.de.retn.net [80.81.192.73]
  8    17 ms    16 ms    16 ms  87.245.214.163
  9    16 ms    15 ms    16 ms  a23-37-44-254.deploy.static.akamaitechnologies.com [23.37.44.254]

Trace complete.
```

ARP lab

Please respond to the following questions and add respective screenshot(s):

1. What is the 48-bit Ethernet address of your computer?
   It is c8:f7:33:d6:56:1e

2. What is the 48-bit destination address in the Ethernet frame?
   Destination address: f8:aa:3f:44:c1:38

3. Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address?
   It is not the address of gaia.cs.umass.edu It is the address of my router

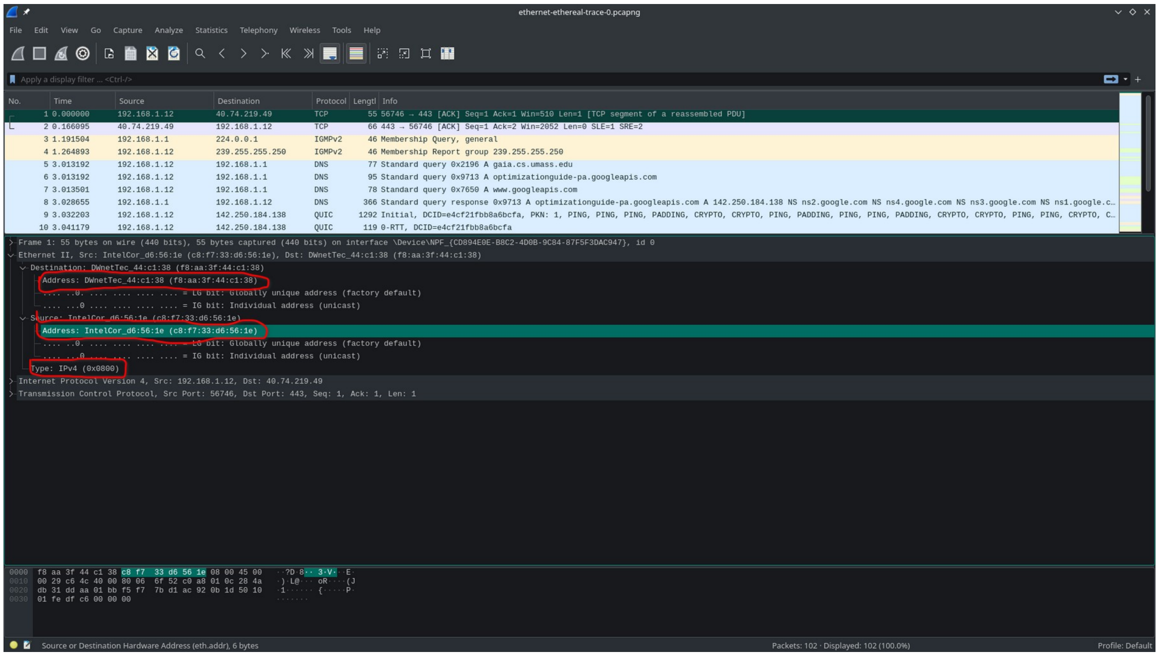
4. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   Frame type field value is 0x0800. It corresponds to IPv4

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu. What device has this as its Ethernet address?
   Source address: f8:aa:3f:44:c1:38 This is the address of my router

6. What is the destination address in the Ethernet frame?
   Destination address: c8:f7:33:d6:56:1e

7. Is this the Ethernet address of your computer?
   Yes, it is the Ethernet address of my computer

8. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   Hexadecimal value: 0x0800. This corresponds to Ipv4


ethernet-ethereal-trace-0.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source          Destination      Protocol Lengtl Info
   1 0.000000  192.168.1.12    40.74.219.49     TCP        55 56746 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
   2 0.166095  40.74.219.49    192.168.1.12     TCP        66 443 → 56746 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
   3 1.191504  192.168.1.1     224.0.0.1        IGMPv2     46 Membership Query, general
   4 1.264893  192.168.1.12    239.255.255.250  IGMPv2     46 Membership Report group 239.255.255.250
   5 3.013192  192.168.1.12    192.168.1.1      DNS        77 Standard query 0x2196 A gaia.cs.umass.edu
   6 3.013192  192.168.1.12    192.168.1.1      DNS        95 Standard query 0x9713 A optimizationguide-pa.googleapis.com
   7 3.013501  192.168.1.12    192.168.1.1      DNS        78 Standard query 0x7650 A www.googleapis.com
   8 3.028655  192.168.1.1     192.168.1.12     DNS       366 Standard query response 0x9713 A optimizationguide-pa.googleapis.com A 142.250.184.138 NS ns2.google.com NS ns4.google.com NS ns3.google.com NS ns1.google.c…
   9 3.032203  192.168.1.12    142.250.184.138  QUIC     1292 Initial, DCID=e4cf21fbb8a6bcfa, PKN: 1, PING, PING, PING, PADDING, CRYPTO, CRYPTO, PING, PADDING, PING, PING, PADDING, CRYPTO, CRYPTO, PING, PING, CRYPTO, C…
  10 3.041179  192.168.1.12    142.250.184.138  QUIC      119 0-RTT, DCID=e4cf21fbb8a6bcfa
```

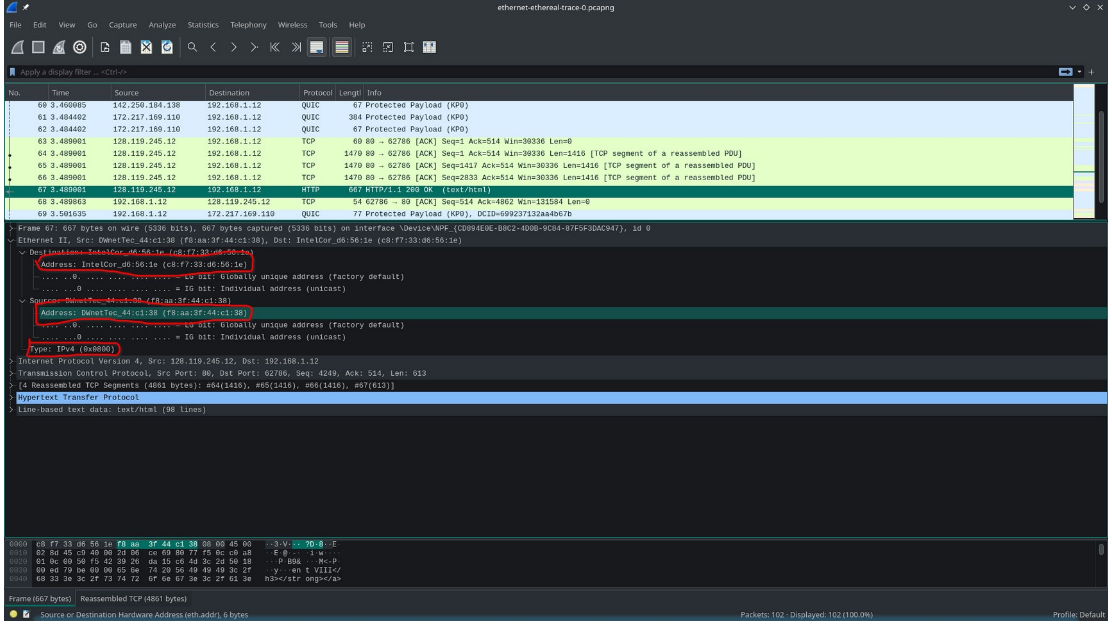
```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{CD894E0E-B8C2-4D0B-9C84-87F5F3DAC947}, id 0
v Ethernet II, Src: IntelCor_d6:56:1e (c8:f7:33:d6:56:1e), Dst: DWnetTec_44:c1:38 (f8:aa:3f:44:c1:38)
  v Destination: DWnetTec_44:c1:38 (f8:aa:3f:44:c1:38)
      Address: DWnetTec_44:c1:38 (f8:aa:3f:44:c1:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_d6:56:1e (c8:f7:33:d6:56:1e)
      Address: IntelCor_d6:56:1e (c8:f7:33:d6:56:1e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 40.74.219.49
> Transmission Control Protocol, Src Port: 56746, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  f8 aa 3f 44 c1 38 c8 f7  33 d6 56 1e 08 00 45 00   ··?D·8·· 3·V···E·
0010  00 29 c6 4c 40 00 80 06  6f 52 c0 a8 01 0c 28 4a   ·)·L@··· oR····(J
0020  db 31 dd aa 01 bb f5 f7  7b d1 ac 92 0b 1d 50 10   ·1······ {·····P·
0030  01 fe df c6 00 00 00                               ·······
```

Source or Destination Hardware Address (eth.addr), 6 bytes

Packets: 102 · Displayed: 102 (100.0%)

Profile: Default


ethernet-ethereal-trace-0.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Frame (667 bytes)
Reassembled TCP (4861 bytes)
Source or Destination Hardware Address (eth.addr), 6 bytes
Packets: 102 · Displayed: 102 (100.0%)
Profile: Default

```
No.   Time      Source           Destination      Protocol Lengtl Info
   60 3.460085  142.250.184.138  192.168.1.12     QUIC       67 Protected Payload (KP0)
   61 3.484402  172.217.169.110  192.168.1.12     QUIC      384 Protected Payload (KP0)
   62 3.484402  172.217.169.110  192.168.1.12     QUIC       67 Protected Payload (KP0)
   63 3.489001  128.119.245.12   192.168.1.12     TCP        60 80 → 62786 [ACK] Seq=1 Ack=514 Win=30336 Len=0
   64 3.489001  128.119.245.12   192.168.1.12     TCP      1470 80 → 62786 [ACK] Seq=1 Ack=514 Win=30336 Len=1416 [TCP segment of a reassembled PDU]
   65 3.489001  128.119.245.12   192.168.1.12     TCP      1470 80 → 62786 [ACK] Seq=1417 Ack=514 Win=30336 Len=1416 [TCP segment of a reassembled PDU]
   66 3.489001  128.119.245.12   192.168.1.12     TCP      1470 80 → 62786 [ACK] Seq=2833 Ack=514 Win=30336 Len=1416 [TCP segment of a reassembled PDU]
   67 3.489001  128.119.245.12   192.168.1.12     HTTP      667 HTTP/1.1 200 OK  (text/html)
   68 3.489863  192.168.1.12     128.119.245.12   TCP        54 62786 → 80 [ACK] Seq=514 Ack=4862 Win=131584 Len=0
   69 3.501635  192.168.1.12     172.217.169.110  QUIC       77 Protected Payload (KP0), DCID=699237132aa4b67b

> Frame 67: 667 bytes on wire (5336 bits), 667 bytes captured (5336 bits) on interface \Device\NPF_{CD894E0E-B8C2-4D0B-9C84-87F5F3DAC947}, id 0
v Ethernet II, Src: DWnetTec_44:c1:38 (f8:aa:3f:44:c1:38), Dst: IntelCor_d6:56:1e (c8:f7:33:d6:56:1e)
  v Destination: IntelCor_d6:56:1e (c8:f7:33:d6:56:1e)
      Address: IntelCor_d6:56:1e (c8:f7:33:d6:56:1e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: DWnetTec_44:c1:38 (f8:aa:3f:44:c1:38)
      Address: DWnetTec_44:c1:38 (f8:aa:3f:44:c1:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 80, Dst Port: 62786, Seq: 4249, Ack: 514, Len: 613
> [4 Reassembled TCP Segments (4861 bytes): #64(1416), #65(1416), #66(1416), #67(613)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)

0000  c8 f7 33 d6 56 1e f8 aa  3f 44 c1 38 08 00 45 00   ··3·V··· ?D·8··E·
0010  02 8d 45 c9 40 00 2d 06  ce 69 80 77 f5 0c c0 a8   ··E·@·-· ·i·w····
0020  01 0c 00 50 f5 42 39 26  da 15 c6 4d 3c 2d 50 18   ···P·B9& ···M<-P·
0030  00 ed 79 be 00 00 65 6e  74 20 56 49 49 49 3c 2f   ··y···en t VIII</
0040  68 33 3e 3c 2f 73 74 72  6f 6e 67 3e 3c 2f 61 3e   h3></str ong></a>
```

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?
   The Internet address column contains the IP address, the Physical address column contains the MAC address and the Type column contains if it is dynamic or static

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
    Source address: 00:d0:59:a9:3d:68   Destination address: ff:ff:ff:ff:ff:ff

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
    Hexadecimal value: 0x0806. This corresponds to ARP

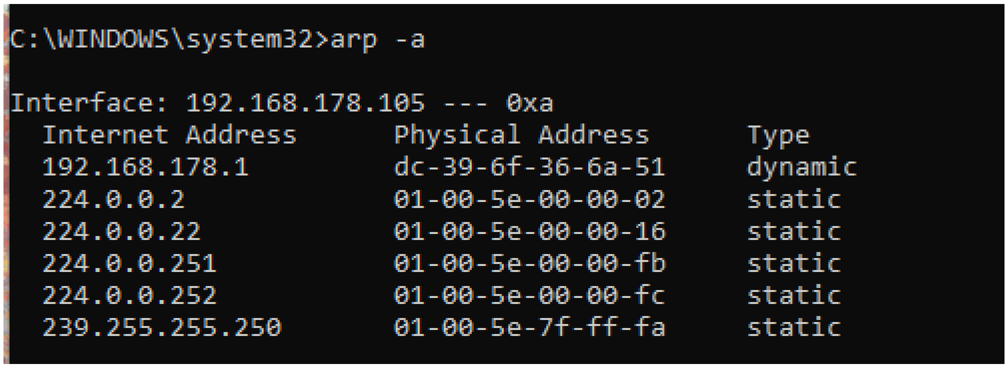
12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
    a) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
       Opcode value: 0x0001
    b) Does the ARP message contain the IP address of the sender?
       Yes
    c) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
       The “question” appears in the Target MAC address field, which is 00:00:00:00:00:00 to question the machine whose corresponding IP address 192.168.1.1 is being queried

13. Now find the ARP reply that was sent in response to the ARP request.
    a) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
       Opcode value: 0x0002
    b) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
       The “answer” appears in the Sender MAC address field

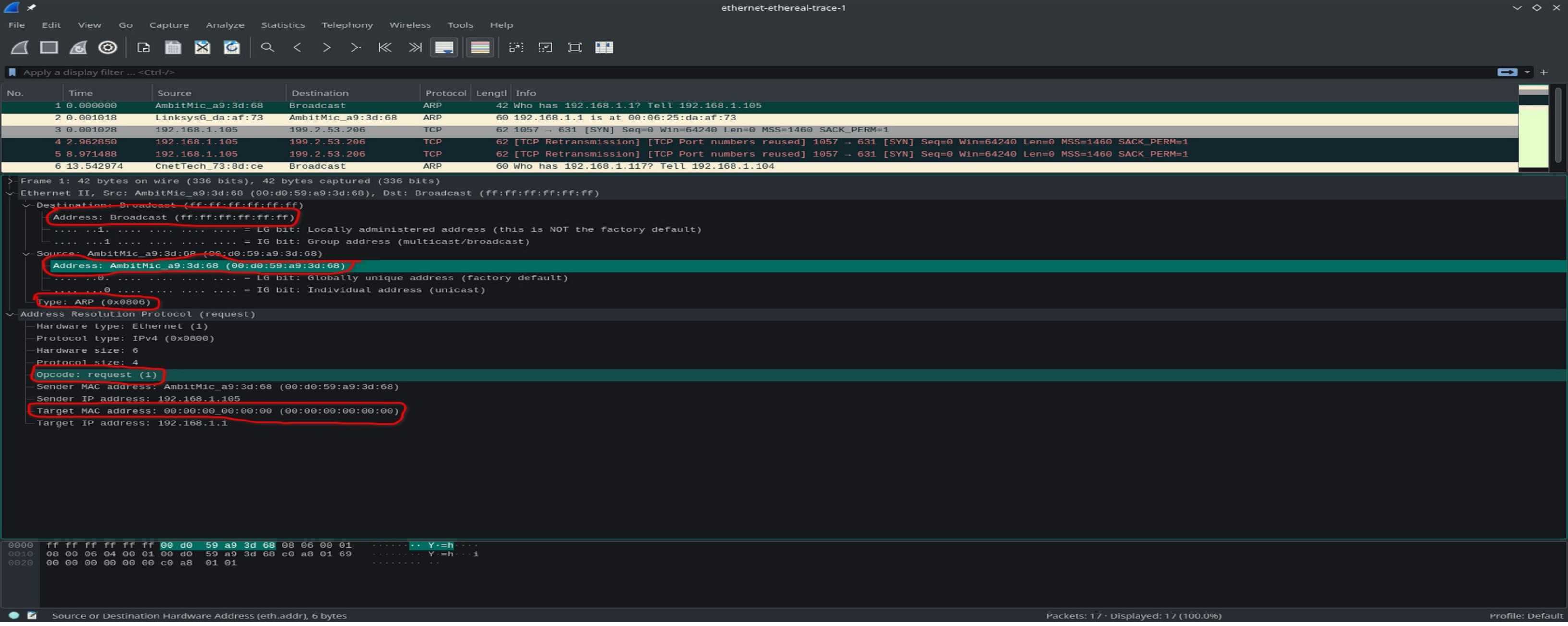
14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
Source address: 00:06:25:da:af:73   Destination address: 00:d0:59:a9:3d:68

15. Open the *ethernet-ethereal-trace-1* trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Because this machine is not the router that maintains the ARP table and as a result it does not give the sender an answer.



```
C:\WINDOWS\system32>arp -a

Interface: 192.168.178.105 --- 0xa
  Internet Address      Physical Address      Type
  192.168.178.1         dc-39-6f-36-6a-51     dynamic
  224.0.0.2             01-00-5e-00-00-02     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

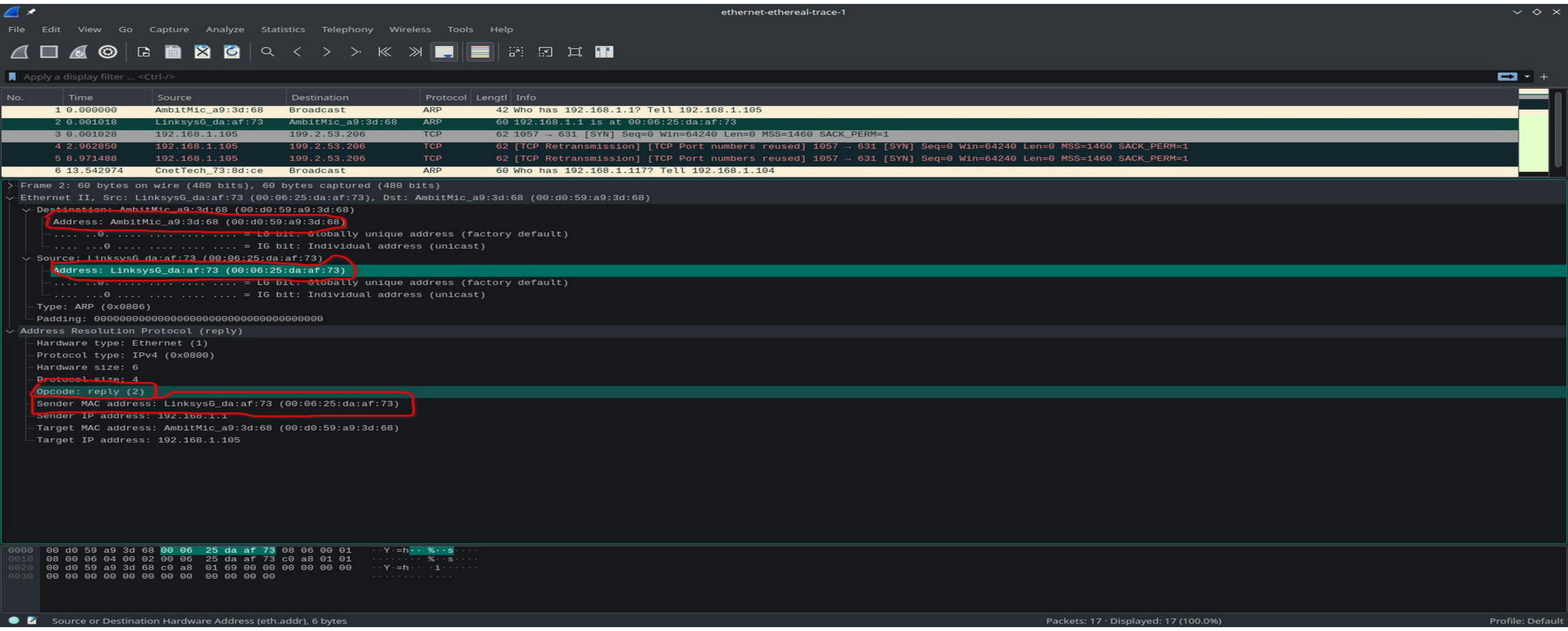


```
No.   Time        Source              Destination         Protocol Lengtl Info
    1 0.000000    AmbitMic_a9:3d:68   Broadcast           ARP          42 Who has 192.168.1.1? Tell 192.168.1.105
    2 0.001018    LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP          60 192.168.1.1 is at 00:06:25:da:af:73
    3 0.001028    192.168.1.105       199.2.53.206        TCP          62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    4 2.962850    192.168.1.105       199.2.53.206        TCP          62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    5 8.971488    192.168.1.105       199.2.53.206        TCP          62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    6 13.542974   CnetTech_73:8d:ce   Broadcast           ARP          60 Who has 192.168.1.117? Tell 192.168.1.104
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
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: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

```
0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

```
Source or Destination Hardware Address (eth.addr), 6 bytes          Packets: 17 · Displayed: 17 (100.0%)          Profile: Default
```



```
No.   Time        Source              Destination         Protocol Lengtl Info
    1 0.000000    AmbitMic_a9:3d:68   Broadcast           ARP          42 Who has 192.168.1.1? Tell 192.168.1.105
    2 0.001018    LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP          60 192.168.1.1 is at 00:06:25:da:af:73
    3 0.001028    192.168.1.105       199.2.53.206        TCP          62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    4 2.962850    192.168.1.105       199.2.53.206        TCP          62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    5 8.971488    192.168.1.105       199.2.53.206        TCP          62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    6 13.542974   CnetTech_73:8d:ce   Broadcast           ARP          60 Who has 192.168.1.117? Tell 192.168.1.104
```

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  v Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
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: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

```
Source or Destination Hardware Address (eth.addr), 6 bytes          Packets: 17 · Displayed: 17 (100.0%)          Profile: Default
```