Leonardo Aviles
Data Com. and Security
Paul Smith
February 26,2017

Lab 3

Capturing and analyzing Ethernet frames

1. What is the 48-bit Ethernet address of your computer?

54:ab:3a:9b:4e:5f

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

Ec:08:6b:3a:8e:6a, this is not the ethernet address of the site but the router or device that connects the server.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The value for the frame type field is 0x0800 and corresponds with IPv4

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

The ascii G appears 54 bytes from the very start of the ethernet frame.

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?

54:ab:3a:9b:4e:5f this is the address of the router used at the location I am at.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

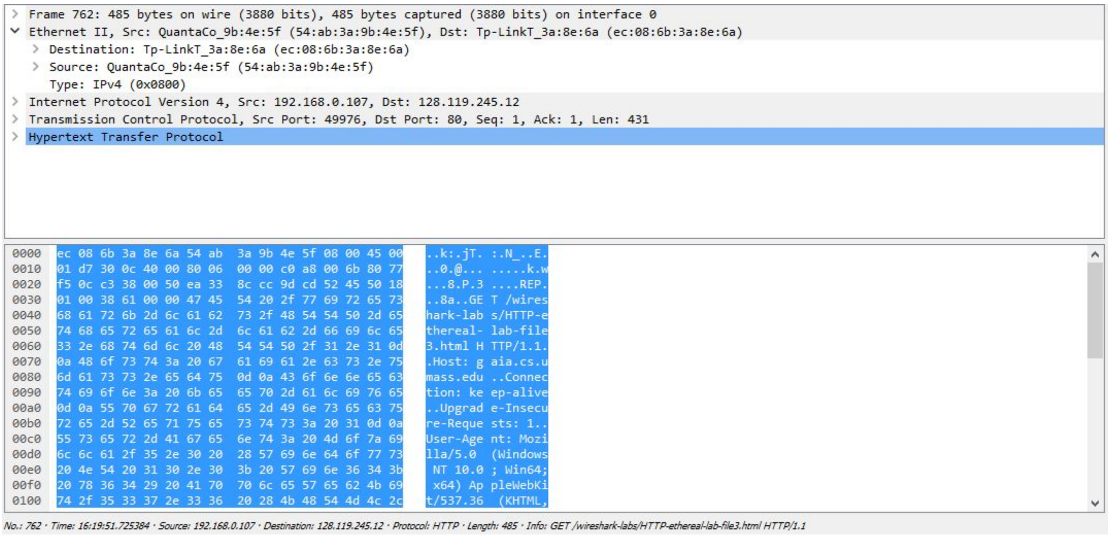
Ec:08:6b:3a:8e:6a, this is not the ethernet address of the site but the router or device that connects the server.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

0x0800 IPv4

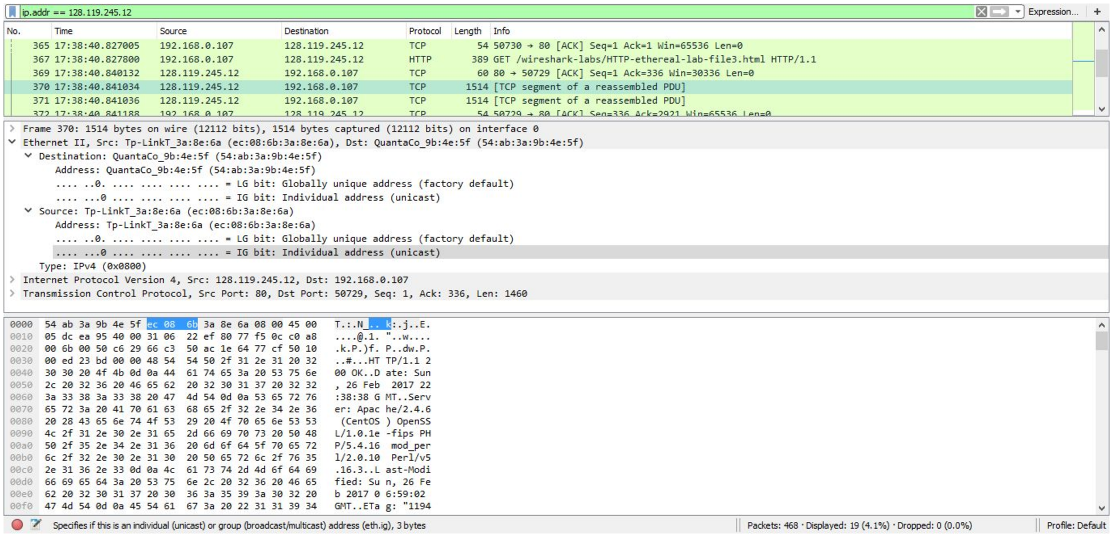
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

53 bytes from the start



```
> Frame 762: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface 0
v Ethernet II, Src: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f), Dst: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a)
  > Destination: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a)
  > Source: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49976, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
> Hypertext Transfer Protocol

0000  ec 08 6b 3a 8e 6a 54 ab  3a 9b 4e 5f 08 00 45 00   ..k:.jT. :.N_..E.
0010  01 d7 30 0c 40 00 80 06  00 00 c0 a8 00 6b 80 77   ..0.@... .....k.w
0020  f5 0c c3 38 00 50 ea 33  8c cc 9d cd 52 45 50 18   ...8.P.3 ....REP.
0030  01 00 38 61 00 00 47 45  54 20 2f 77 69 72 65 73   ..8a..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1.
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   .Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ..Connec
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ..Upgrad e-Insecu
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1..
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00d0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00e0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.0 ; Win64;
00f0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) Ap pleWebKi
0100  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c   t/537.36  (KHTML,

No.: 762 · Time: 16:19:51.725384 · Source: 192.168.0.107 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 485 · Info: GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
```

Figure 1: Shows the packet information in the get packet.



```
No.  Time             Source          Destination     Protocol Length Info
 365 17:38:40.827005  192.168.0.107   128.119.245.12  TCP        54 50730 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 367 17:38:40.827800  192.168.0.107   128.119.245.12  HTTP      389 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
 369 17:38:40.840132  128.119.245.12  192.168.0.107   TCP        60 80 → 50729 [ACK] Seq=1 Ack=336 Win=30336 Len=0
 370 17:38:40.841034  128.119.245.12  192.168.0.107   TCP      1514 [TCP segment of a reassembled PDU]
 371 17:38:40.841036  128.119.245.12  192.168.0.107   TCP      1514 [TCP segment of a reassembled PDU]
 372 17:38:40.841188  192.168.0.107   128.119.245.12  TCP        54 50729 → 80 [ACK] Seq=336 Ack=2921 Win=65536 Len=0

> Frame 370: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
v Ethernet II, Src: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a), Dst: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
  v Destination: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
      Address: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a)
      Address: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a)
      .... ..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: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 50729, Seq: 1, Ack: 336, Len: 1460

0000  54 ab 3a 9b 4e 5f ec 08  6b 3a 8e 6a 08 00 45 00   T.:.N_.. k:.j..E.
0010  05 dc ea 95 40 00 31 06  22 ef 80 77 f5 0c c0 a8   ....@.1. "..w....
0020  00 6b 00 50 c6 29 66 c3  50 ac 1e 64 77 cf 50 10   .k.P.)f. P..dw.P.
0030  00 ed 23 bd 00 00 48 54  54 50 2f 31 2e 31 20 32   ..#...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK..D ate: Sun
0050  2c 20 32 36 20 46 65 62  20 32 30 31 37 20 32 32   , 26 Feb  2017 22
0060  3a 33 38 3a 33 38 20 47  4d 54 0d 0a 53 65 72 76   :38:38 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 31 65  2d 66 69 70 73 20 50 48   L/1.0.1e -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3..L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 36 20 46 65   fied: Su n, 26 Fe
00e0  62 20 32 30 31 37 20 30  36 3a 35 39 3a 30 32 20   b 2017 0 6:59:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 31 39 34   GMT..ETa g: "1194

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.ig), 3 bytes | Packets: 468 · Displayed: 19 (4.1%) · Dropped: 0 (0.0%) | Profile: Default
```

Figure 2: Shows the OK packet information

ARP Caching

Write down the content of your computer's ARP cache. What is the meaning of each column value?

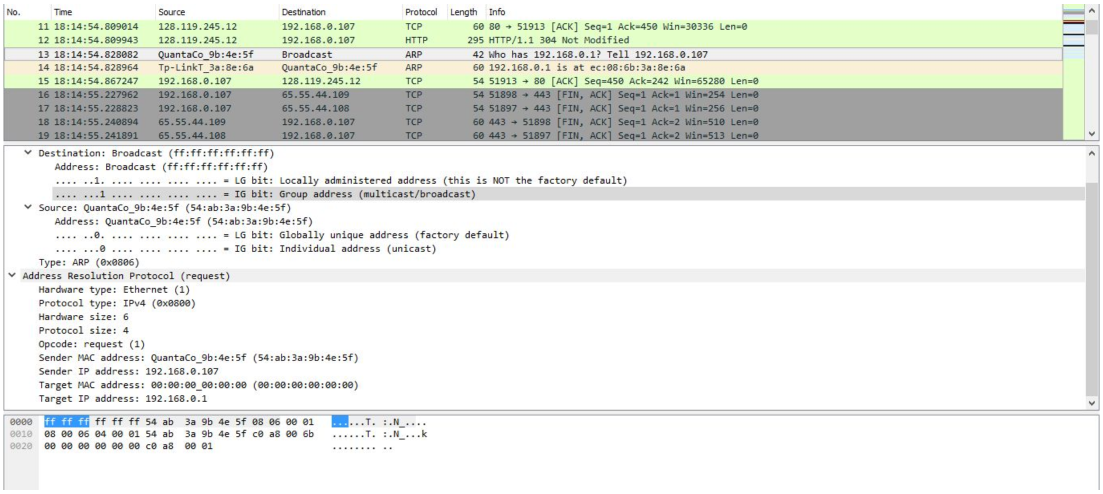
```
C:\Users\avile>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

SRC: 54:AB:3A:9B:4E:5F
DEST: FF:FF:FF:FF:FF:FF

Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

ARP- (Ox0806)



No.	Time	Source	Destination	Protocol	Length	Info
11	18:14:54.809014	128.119.245.12	192.168.0.107	TCP	60	80 → 51913 [ACK] Seq=1 Ack=450 Win=30336 Len=0
12	18:14:54.809943	128.119.245.12	192.168.0.107	HTTP	295	HTTP/1.1 304 Not Modified
13	18:14:54.828082	QuantaCo_9b:4e:5f	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.107
14	18:14:54.828964	Tp-LinkT_3a:8e:6a	QuantaCo_9b:4e:5f	ARP	60	192.168.0.1 is at ec:08:6b:3a:8e:6a
15	18:14:54.867247	192.168.0.107	128.119.245.12	TCP	54	51913 → 80 [ACK] Seq=450 Ack=242 Win=65280 Len=0
16	18:14:55.227962	192.168.0.107	65.55.44.109	TCP	54	51898 → 443 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
17	18:14:55.228823	192.168.0.107	65.55.44.108	TCP	54	51897 → 443 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
18	18:14:55.240894	65.55.44.109	192.168.0.107	TCP	60	443 → 51898 [FIN, ACK] Seq=1 Ack=2 Win=510 Len=0
19	18:14:55.241891	65.55.44.108	192.168.0.107	TCP	60	443 → 51897 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0

```
  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)
  Source: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
    Address: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
  Sender IP address: 192.168.0.107
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.1
```

```
0000  ff ff ff ff ff ff 54 ab  3a 9b 4e 5f 08 06 00 01   ......T. :.N_....
0010  08 00 06 04 00 01 54 ab  3a 9b 4e 5f c0 a8 00 6b   ......T. :.N_...k
0020  00 00 00 00 00 00 c0 a8  00 01                     ........ ..
```

Figure 3: Picture above shows the capture of the new packets and the arp protocols

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)   How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

ARP opcode begins 19 bytes from the beginning of the ethernet frame at byte 20

b)   What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

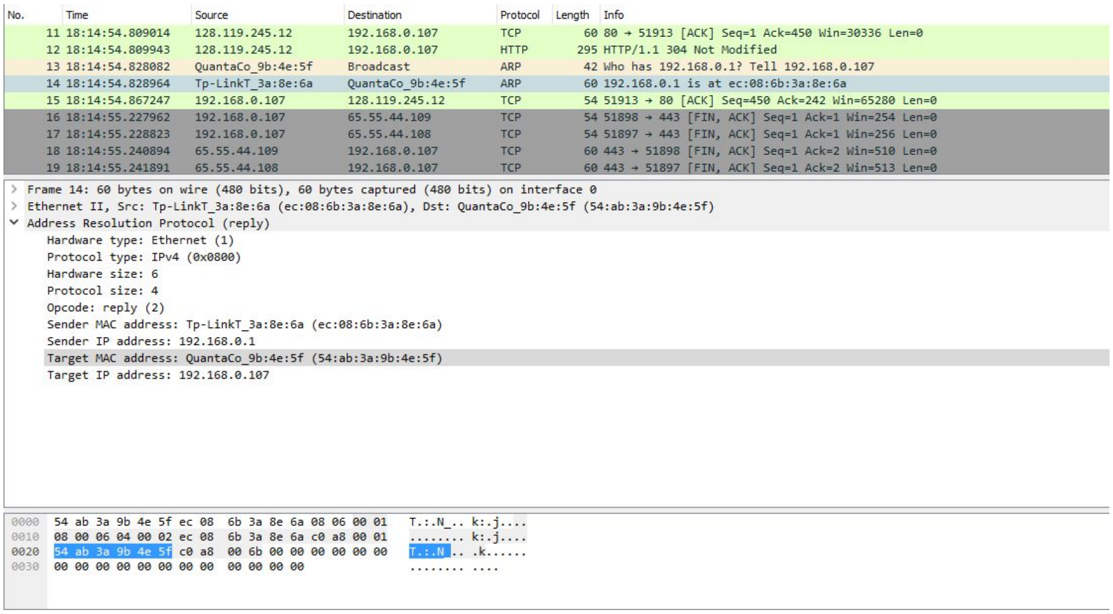
Hex value for the opcode field is 0x0001

c)   Does the ARP message contain the IP address of the sender?

In this case it is 192.168.0.107

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

The target MAC addr is set to 00:00:00:00:00:00 which will question which device has the IP we are looking for



```
No.   Time             Source              Destination         Protocol Length Info
   11 18:14:54.809014  128.119.245.12      192.168.0.107       TCP        60 80 → 51913 [ACK] Seq=1 Ack=450 Win=30336 Len=0
   12 18:14:54.809943  128.119.245.12      192.168.0.107       HTTP      295 HTTP/1.1 304 Not Modified
   13 18:14:54.828082  QuantaCo_9b:4e:5f   Broadcast           ARP        42 Who has 192.168.0.1? Tell 192.168.0.107
   14 18:14:54.828964  Tp-LinkT_3a:8e:6a   QuantaCo_9b:4e:5f   ARP        60 192.168.0.1 is at ec:08:6b:3a:8e:6a
   15 18:14:54.867247  192.168.0.107       128.119.245.12      TCP        54 51913 → 80 [ACK] Seq=450 Ack=242 Win=65280 Len=0
   16 18:14:55.227962  192.168.0.107       65.55.44.109        TCP        54 51898 → 443 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
   17 18:14:55.228823  192.168.0.107       65.55.44.108        TCP        54 51897 → 443 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
   18 18:14:55.240894  65.55.44.109        192.168.0.107       TCP        60 443 → 51898 [FIN, ACK] Seq=1 Ack=2 Win=510 Len=0
   19 18:14:55.241891  65.55.44.108        192.168.0.107       TCP        60 443 → 51897 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0
```

```
> Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a), Dst: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
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: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a)
    Sender IP address: 192.168.0.1
    Target MAC address: QuantaCo_9b:4e:5f (54:ab:3a:9b:4e:5f)
    Target IP address: 192.168.0.107
```

```
0000  54 ab 3a 9b 4e 5f ec 08  6b 3a 8e 6a 08 06 00 01   T.:.N_.. k:.j....
0010  08 00 06 04 00 02 ec 08  6b 3a 8e 6a c0 a8 00 01   ........ k:.j....
0020  54 ab 3a 9b 4e 5f c0 a8  00 6b 00 00 00 00 00 00   T.:.N... .k......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Figure 4: Shows the response to the first ARP message

Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

19 bytes from the beginning at byte number 20

b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of the op-code is 2 which is associated with reply.

c) 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 to the question from the earlier ARP packet is found in the sender MAC address which in this case is ec:08:6b:3a:8e:6a with a IP address of 192.168.0.1.

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Src: ec:08:6b:3a:8e:6a
Dest: 54:ab:3a:9b:5e:5f

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?

There is no reply in this trace, because we are not at the device that sent the request. The ARP request is sent back to the device that requested or send the request .