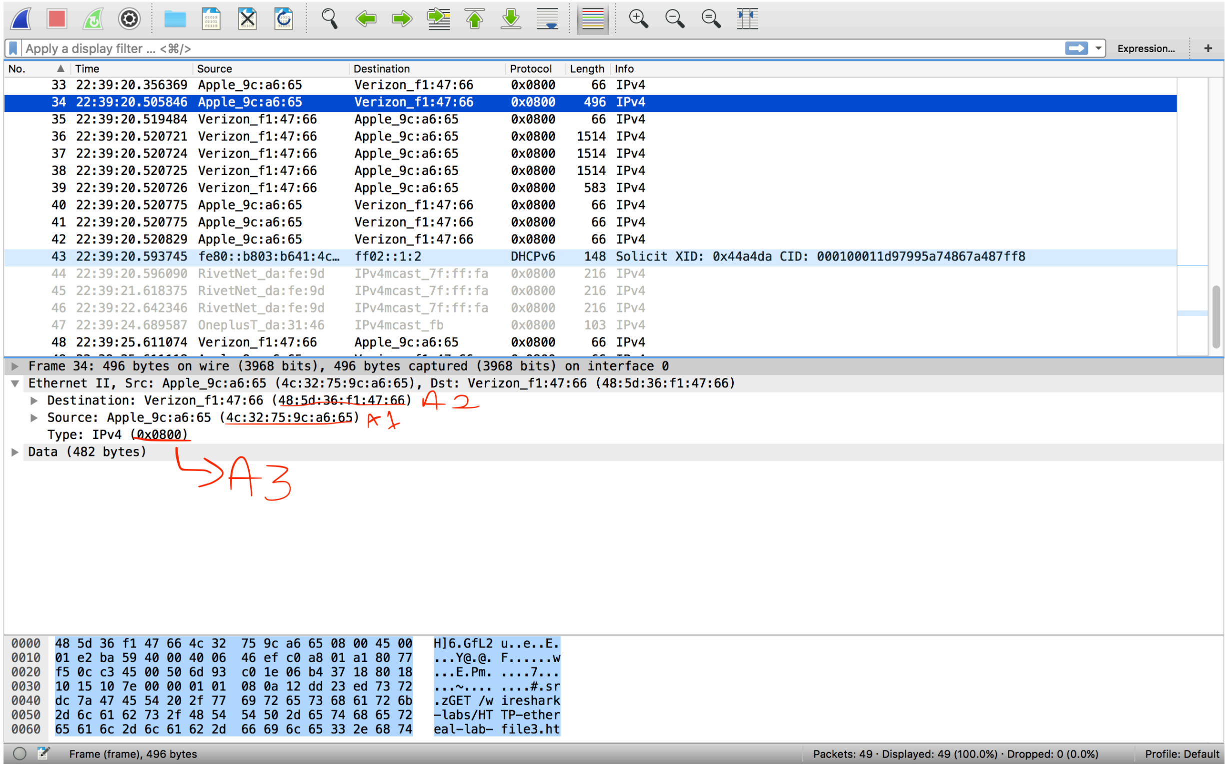
CN Homework Ethernet and ARP
By:
Monil Shah(mds747)

1. What is the 48-bit Ethernet address of your computer?
Ans.) 4c:32:75:9c:a6:65

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.]
Ans.)As per the screenshot below the 48-bit destination address in the Ethernet frame is “48:5d:36:f1:47:66”. No this is not the Ethernet address of “gaia.cs.umass.edu”, it is the Ethernet address of my “Verizon” router through which the HTTP request is sent.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
Ans.)As per the screenshot below the hexadecimal value for the two-byte Frame type field is “0x0800” and it corresponds to the IP as the upper layer protocol.



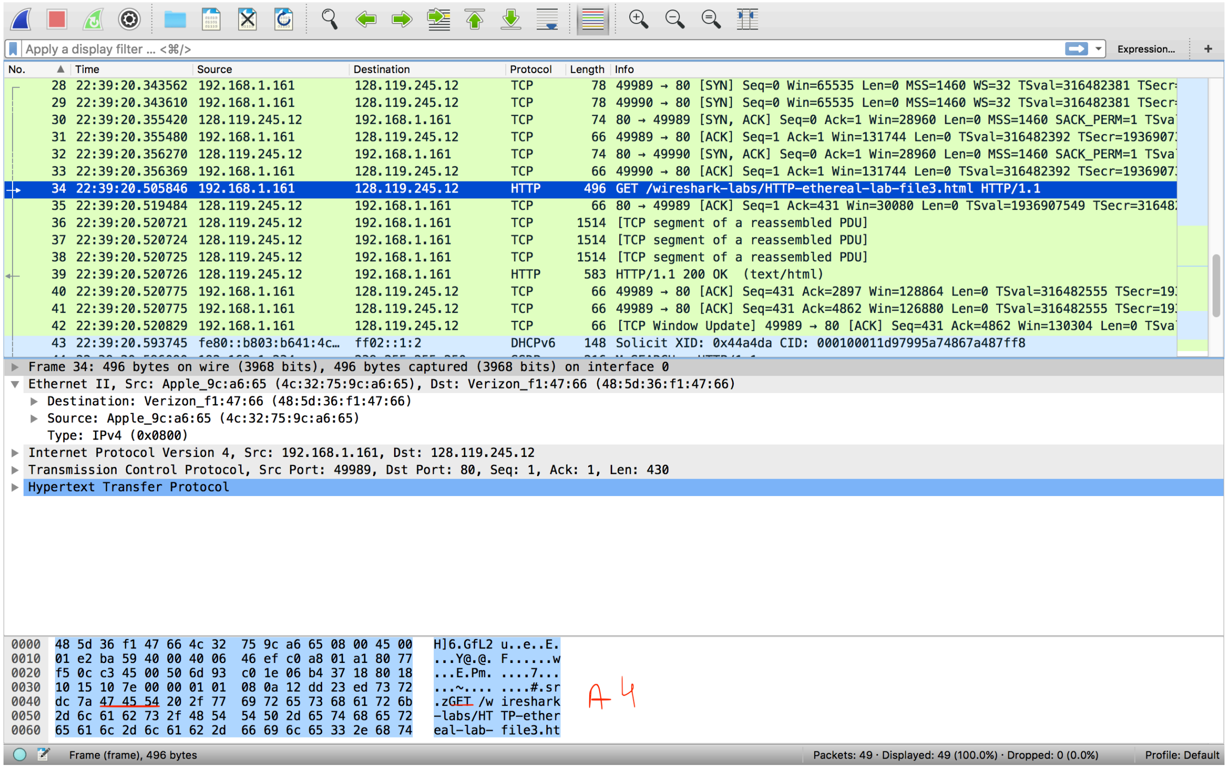
```
No.  ▲ Time            Source                Destination          Protocol  Length  Info
   33 22:39:20.356369  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66  IPv4
   34 22:39:20.505846  Apple_9c:a6:65        Verizon_f1:47:66     0x0800     496  IPv4
   35 22:39:20.519484  Verizon_f1:47:66      Apple_9c:a6:65       0x0800      66  IPv4
   36 22:39:20.520721  Verizon_f1:47:66      Apple_9c:a6:65       0x0800    1514  IPv4
   37 22:39:20.520724  Verizon_f1:47:66      Apple_9c:a6:65       0x0800    1514  IPv4
   38 22:39:20.520725  Verizon_f1:47:66      Apple_9c:a6:65       0x0800    1514  IPv4
   39 22:39:20.520726  Verizon_f1:47:66      Apple_9c:a6:65       0x0800     583  IPv4
   40 22:39:20.520775  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66  IPv4
   41 22:39:20.520775  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66  IPv4
   42 22:39:20.520829  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66  IPv4
   43 22:39:20.593745  fe80::b803:b641:4c…   ff02::1:2            DHCPv6     148  Solicit XID: 0x44a4da CID: 000100011d97995a74867a487ff8
   44 22:39:20.596090  RivetNet_da:fe:9d     IPv4mcast_7f:ff:fa   0x0800     216  IPv4
   45 22:39:21.618375  RivetNet_da:fe:9d     IPv4mcast_7f:ff:fa   0x0800     216  IPv4
   46 22:39:22.642346  RivetNet_da:fe:9d     IPv4mcast_7f:ff:fa   0x0800     216  IPv4
   47 22:39:24.689587  OneplusT_da:31:46     IPv4mcast_fb         0x0800     103  IPv4
   48 22:39:25.611074  Verizon_f1:47:66      Apple_9c:a6:65       0x0800      66  IPv4
```

```
▶ Frame 34: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface 0
▼ Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Destination: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Source: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
    Type: IPv4 (0x0800)
▶ Data (482 bytes)
```

```
0000  48 5d 36 f1 47 66 4c 32  75 9c a6 65 08 00 45 00   H]6.GfL2 u..e..E.
0010  01 e2 ba 59 40 00 40 06  46 ef c0 a8 01 a1 80 77   ...Y@.@. F......w
0020  f5 0c c3 45 00 50 6d 93  c0 1e 06 b4 37 18 80 18   ...E.Pm. ....7...
0030  10 15 10 7e 00 00 01 01  08 0a 12 dd 23 ed 73 72   ...~.... ....#.sr
0040  dc 7a 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   .zGET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 65 74 68 65 72   -labs/HT TP-ether
0060  65 61 6c 2d 6c 61 62 2d  66 69 6c 65 33 2e 68 74   eal-lab- file3.ht
```

Frame (frame), 496 bytes   Packets: 49 · Displayed: 49 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?
Ans.)As per the screenshot below the ASCII “G” in “GET” appear on the 54th byte starting from 0 from the very start of the Ethernet frame as the first 14 byte for Ethernet frame, then next 20 bytes for IP header, next 20 bytes for TCP header and then HTTP data starts.



```
No.   Time             Source              Destination      Protocol  Length Info
  28 22:39:20.343562  192.168.1.161       128.119.245.12   TCP         78 49989 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=316482381 TSecr=
  29 22:39:20.343610  192.168.1.161       128.119.245.12   TCP         78 49990 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=316482381 TSecr=
  30 22:39:20.355420  128.119.245.12      192.168.1.161    TCP         74 80 → 49989 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva
  31 22:39:20.355480  192.168.1.161       128.119.245.12   TCP         66 49989 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=316482392 TSecr=1936907
  32 22:39:20.356270  128.119.245.12      192.168.1.161    TCP         74 80 → 49990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva
  33 22:39:20.356369  192.168.1.161       128.119.245.12   TCP         66 49990 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=316482392 TSecr=1936907
  34 22:39:20.505846  192.168.1.161       128.119.245.12   HTTP       496 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
  35 22:39:20.519484  128.119.245.12      192.168.1.161    TCP         66 80 → 49989 [ACK] Seq=1 Ack=431 Win=30080 Len=0 TSval=1936907549 TSecr=31648
  36 22:39:20.520721  128.119.245.12      192.168.1.161    TCP       1514 [TCP segment of a reassembled PDU]
  37 22:39:20.520724  128.119.245.12      192.168.1.161    TCP       1514 [TCP segment of a reassembled PDU]
  38 22:39:20.520725  128.119.245.12      192.168.1.161    TCP       1514 [TCP segment of a reassembled PDU]
  39 22:39:20.520726  128.119.245.12      192.168.1.161    HTTP       583 HTTP/1.1 200 OK  (text/html)
  40 22:39:20.520775  192.168.1.161       128.119.245.12   TCP         66 49989 → 80 [ACK] Seq=431 Ack=2897 Win=128864 Len=0 TSval=316482555 TSecr=19
  41 22:39:20.520775  192.168.1.161       128.119.245.12   TCP         66 49989 → 80 [ACK] Seq=431 Ack=4862 Win=126880 Len=0 TSval=316482555 TSecr=19
  42 22:39:20.520829  192.168.1.161       128.119.245.12   TCP         66 [TCP Window Update] 49989 → 80 [ACK] Seq=431 Ack=4862 Win=130304 Len=0 TSva
  43 22:39:20.593745  fe80::b803:b641:4c…  ff02::1:2        DHCPv6     148 Solicit XID: 0x44a4da CID: 000100011d97995a74867a487ff8
```

```
▶ Frame 34: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface 0
▼ Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Destination: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Source: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 49989, Dst Port: 80, Seq: 1, Ack: 1, Len: 430
▶ Hypertext Transfer Protocol
```

```
0000  48 5d 36 f1 47 66 4c 32  75 9c a6 65 08 00 45 00   H]6.GfL2 u..e..E.
0010  01 e2 ba 59 40 00 40 06  46 ef c0 a8 01 a1 80 77   ...Y@.@. F......w
0020  f5 0c c3 45 00 50 6d 93  c0 1e 06 b4 37 18 80 18   ...E.Pm. ....7...
0030  10 15 10 7e 00 00 01 01  08 0a 12 dd 23 ed 73 72   ...~.... ....#.sr
0040  dc 7a 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   .zGET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 65 74 68 65 72   -labs/HT TP-ether
0060  65 61 6c 2d 6c 61 62 2d  66 69 6c 65 33 2e 68 74   eal-lab- file3.ht
```

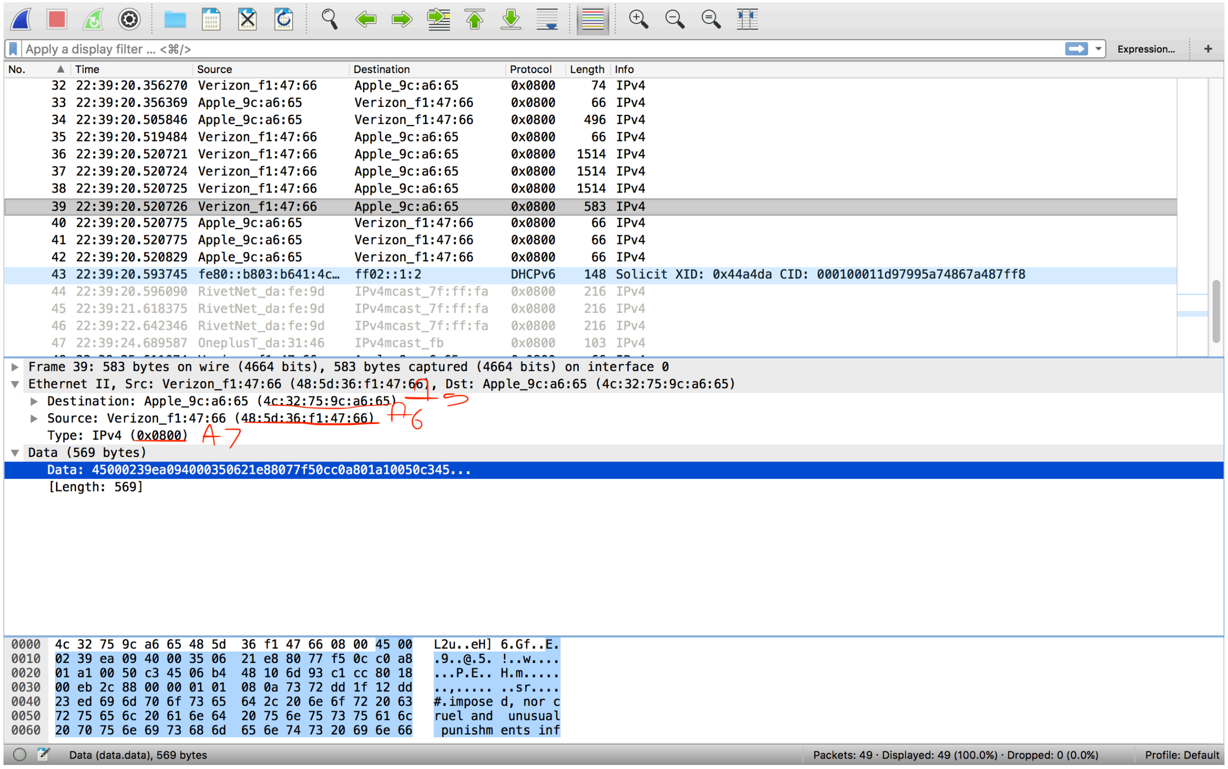
A 4

Frame (frame), 496 bytes   Packets: 49 · Displayed: 49 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

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?
Ans.) As per the screenshot below the value of the Ethernet source address is “48:5d: 36:f1:47:36” and this address is neither of my computer nor of gaia.cs.umass.edu, instead it is the address of my “Verizon” router.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
Ans.) 4c:32:75:9c:a6:65 , my pc.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
Ans.) As per the screenshot below the hexadecimal value for the two-byte Frame type field is “0x0800” and it corresponds to the IP as the upper layer protocol.



```
No.  ▲ Time             Source                Destination          Protocol  Length Info
    32 22:39:20.356270  Verizon_f1:47:66      Apple_9c:a6:65       0x0800      74 IPv4
    33 22:39:20.356369  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66 IPv4
    34 22:39:20.505846  Apple_9c:a6:65        Verizon_f1:47:66     0x0800     496 IPv4
    35 22:39:20.519484  Verizon_f1:47:66      Apple_9c:a6:65       0x0800      66 IPv4
    36 22:39:20.520721  Verizon_f1:47:66      Apple_9c:a6:65       0x0800    1514 IPv4
    37 22:39:20.520724  Verizon_f1:47:66      Apple_9c:a6:65       0x0800    1514 IPv4
    38 22:39:20.520725  Verizon_f1:47:66      Apple_9c:a6:65       0x0800    1514 IPv4
    39 22:39:20.520726  Verizon_f1:47:66      Apple_9c:a6:65       0x0800     583 IPv4
    40 22:39:20.520775  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66 IPv4
    41 22:39:20.520775  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66 IPv4
    42 22:39:20.520829  Apple_9c:a6:65        Verizon_f1:47:66     0x0800      66 IPv4
    43 22:39:20.593745  fe80::b803:b641:4c…   ff02::1:2            DHCPv6     148 Solicit XID: 0x44a4da CID: 000100011d97995a74867a487ff8
    44 22:39:20.596090  RivetNet_da:fe:9d     IPv4mcast_7f:ff:fa   0x0800     216 IPv4
    45 22:39:21.618375  RivetNet_da:fe:9d     IPv4mcast_7f:ff:fa   0x0800     216 IPv4
    46 22:39:22.642346  RivetNet_da:fe:9d     IPv4mcast_7f:ff:fa   0x0800     216 IPv4
    47 22:39:24.689587  OneplusT_da:31:46     IPv4mcast_fb         0x0800     103 IPv4
```

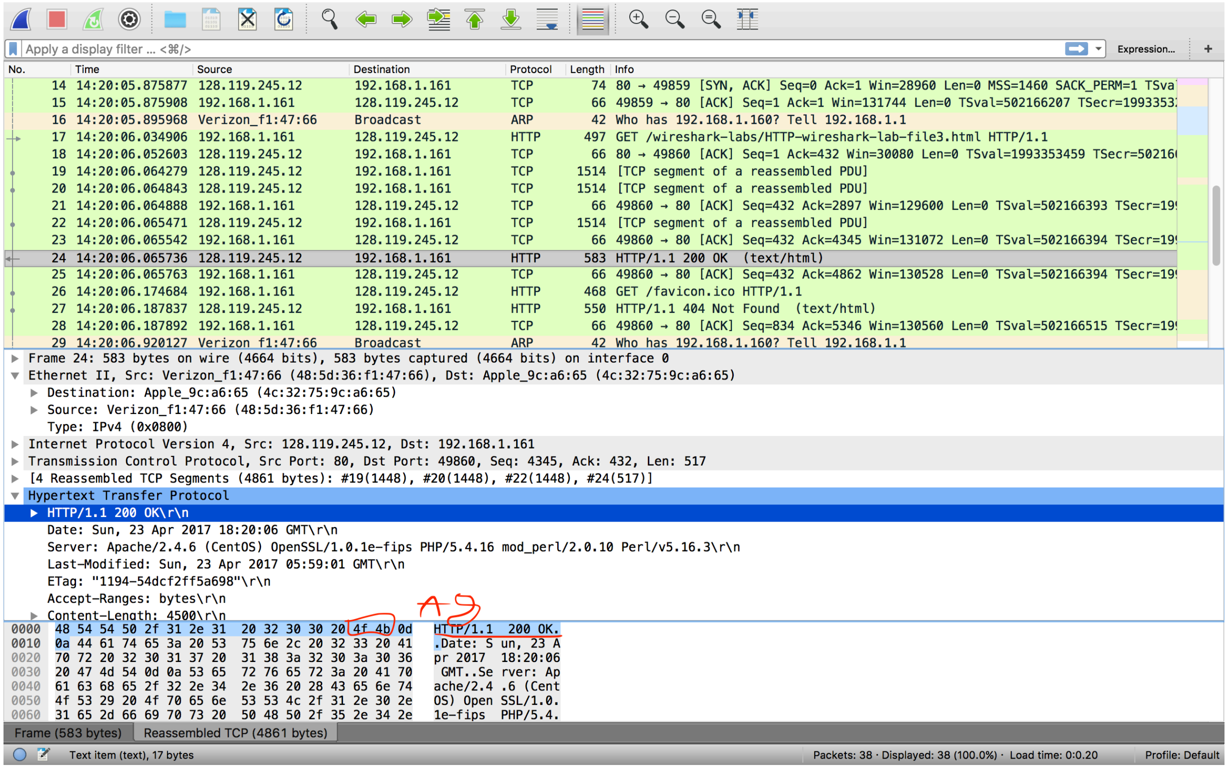
```
▶ Frame 39: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
▼ Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
  ▶ Destination: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
  ▶ Source: Verizon_f1:47:66 (48:5d:36:f1:47:66)
    Type: IPv4 (0x0800)
▼ Data (569 bytes)
    Data: 45000239ea094000350621e88077f50cc0a801a10050c345...
    [Length: 569]
```

```
0000  4c 32 75 9c a6 65 48 5d  36 f1 47 66 08 00 45 00   L2u..eH] 6.Gf..E.
0010  02 39 ea 09 40 00 35 06  21 e8 80 77 f5 0c c0 a8   .9..@.5. !..w....
0020  01 a1 00 50 c3 45 06 b4  48 10 6d 93 c1 cc 80 18   ...P.E.. H.m.....
0030  00 eb 2c 88 00 00 01 01  08 0a 73 72 dd 1f 12 dd   ..,..... ..sr....
0040  23 ed 69 6d 70 6f 73 65  64 2c 20 6e 6f 72 20 63   #.impose d, nor c
0050  72 75 65 6c 20 61 6e 64  20 75 6e 75 73 75 61 6c   ruel and  unusual
0060  20 70 75 6e 69 73 68 6d  65 6e 74 73 20 69 6e 66    punishm ents inf
```

```
Data (data.data), 569 bytes          Packets: 49 · Displayed: 49 (100.0%) · Dropped: 0 (0.0%)     Profile: Default
```

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?

Ans.) As per the screenshot below the first 14 bytes are for Ethernet frame, next 20 bytes for IP header, next 20 bytes for TCP header and then the HTTP data starts. So HTTP data starts after first 54 bytes and after the HTTP data is received the HTTP response code “OK” is encountered on the 14th byte from start.



```
No.  Time             Source             Destination        Protocol  Length  Info
  14 14:20:05.875877  128.119.245.12     192.168.1.161      TCP         74  80 → 49859 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva
  15 14:20:05.875908  192.168.1.161      128.119.245.12     TCP         66  49859 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=502166207 TSecr=1993353
  16 14:20:05.895968  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
  17 14:20:06.034906  192.168.1.161      128.119.245.12     HTTP       497  GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1
  18 14:20:06.052603  128.119.245.12     192.168.1.161      TCP         66  80 → 49860 [ACK] Seq=1 Ack=432 Win=30080 Len=0 TSval=1993353459 TSecr=50216
  19 14:20:06.064279  128.119.245.12     192.168.1.161      TCP       1514  [TCP segment of a reassembled PDU]
  20 14:20:06.064843  128.119.245.12     192.168.1.161      TCP       1514  [TCP segment of a reassembled PDU]
  21 14:20:06.064888  192.168.1.161      128.119.245.12     TCP         66  49860 → 80 [ACK] Seq=432 Ack=2897 Win=129600 Len=0 TSval=502166393 TSecr=19
  22 14:20:06.065471  128.119.245.12     192.168.1.161      TCP       1514  [TCP segment of a reassembled PDU]
  23 14:20:06.065542  192.168.1.161      128.119.245.12     TCP         66  49860 → 80 [ACK] Seq=432 Ack=4345 Win=131072 Len=0 TSval=502166394 TSecr=19
  24 14:20:06.065736  128.119.245.12     192.168.1.161      HTTP       583  HTTP/1.1 200 OK  (text/html)
  25 14:20:06.065763  192.168.1.161      128.119.245.12     TCP         66  49860 → 80 [ACK] Seq=432 Ack=4862 Win=130528 Len=0 TSval=502166394 TSecr=19
  26 14:20:06.174684  192.168.1.161      128.119.245.12     HTTP       468  GET /favicon.ico HTTP/1.1
  27 14:20:06.187837  128.119.245.12     192.168.1.161      HTTP       550  HTTP/1.1 404 Not Found  (text/html)
  28 14:20:06.187892  192.168.1.161      128.119.245.12     TCP         66  49860 → 80 [ACK] Seq=834 Ack=5346 Win=130560 Len=0 TSval=502166515 TSecr=19
  29 14:20:06.920127  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
```

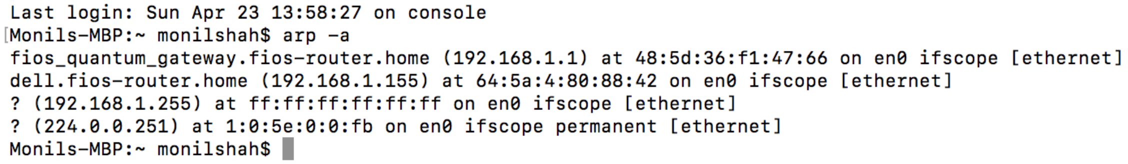
```
▶ Frame 24: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
▼ Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
  ▶ Destination: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
  ▶ Source: Verizon_f1:47:66 (48:5d:36:f1:47:66)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.161
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49860, Seq: 4345, Ack: 432, Len: 517
▶ [4 Reassembled TCP Segments (4861 bytes): #19(1448), #20(1448), #22(1448), #24(517)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sun, 23 Apr 2017 18:20:06 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 23 Apr 2017 05:59:01 GMT\r\n
    ETag: "1194-54dcf2ff5a698"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 4500\r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 33 20 41   .Date: S un, 23 A
0020  70 72 20 32 30 31 37 20  31 38 3a 32 30 3a 30 36   pr 2017  18:20:06
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  31 65 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   1e-fips  PHP/5.4.
```

```
Frame (583 bytes)   Reassembled TCP (4861 bytes)
Text item (text), 17 bytes          Packets: 38 · Displayed: 38 (100.0%) · Load time: 0:0.20          Profile: Default
```

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

Ans.) The contents of my computer's ARP cache is as shown in the screenshot below. There are 3 columns, first is Internet Address which is the IP address or logical address, next is Physical address which is the MAC address and the last column is Type which states the protocol type i.e. ethernet here but it is actually my wireless router.



```
Last login: Sun Apr 23 13:58:27 on console
Monils-MBP:~ monilshah$ arp -a
fios_quantum_gateway.fios-router.home (192.168.1.1) at 48:5d:36:f1:47:66 on en0 ifscope [ethernet]
dell.fios-router.home (192.168.1.155) at 64:5a:4:80:88:42 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
Monils-MBP:~ monilshah$ 
```

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

Ans.)As per the screenshot below the hexadecimal value for the source address is "48:5d: 36:f1:47:66" and the same for the destination address is "ff:ff:ff:ff:ff:ff" which is the broadcast address.

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

Ans.) As per the screenshot below the hexadecimal value for the two-byte Ethernet Frame type field is "0x0806" and it corresponds to ARP as the upper layer protocol.

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/

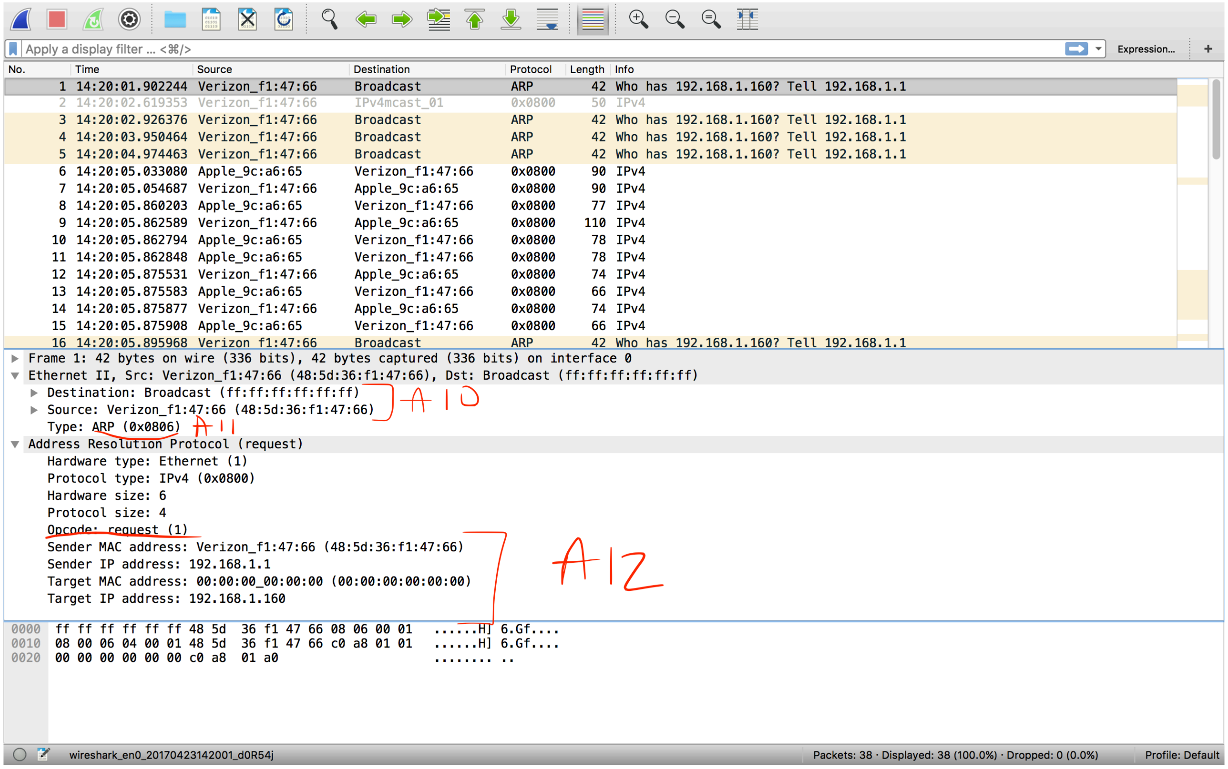
inet-pages/arp.html. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made? c) Does the ARP message contain the IP address of the sender? d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

Ans.) A) As per the screenshot below the ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

B) As per the screenshot above the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made is "1" or in hex "0x0001".

C) Yes the ARP message contains the IP address of the sender which is "192.168.1.1".

D) As per the screenshot below the Target MAC address is "00:00:00:00:00:00" and the Target IP address is "192.168.1.160" which says that the sender is questioning for MAC address of the target with IP address "192.168.1.160".


Apply a display filter ... <⌘/>
Expression...
+
A10
A11
A12
Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

```
No.  Time             Source             Destination     Protocol  Length  Info
  1  14:20:01.902244  Verizon_f1:47:66   Broadcast       ARP           42  Who has 192.168.1.160? Tell 192.168.1.1
  2  14:20:02.619353  Verizon_f1:47:66   IPv4mcast_01    0x0800        50  IPv4
  3  14:20:02.926376  Verizon_f1:47:66   Broadcast       ARP           42  Who has 192.168.1.160? Tell 192.168.1.1
  4  14:20:03.950464  Verizon_f1:47:66   Broadcast       ARP           42  Who has 192.168.1.160? Tell 192.168.1.1
  5  14:20:04.974463  Verizon_f1:47:66   Broadcast       ARP           42  Who has 192.168.1.160? Tell 192.168.1.1
  6  14:20:05.033080  Apple_9c:a6:65    Verizon_f1:47:66  0x0800       90  IPv4
  7  14:20:05.054687  Verizon_f1:47:66   Apple_9c:a6:65  0x0800        90  IPv4
  8  14:20:05.860203  Apple_9c:a6:65    Verizon_f1:47:66  0x0800       77  IPv4
  9  14:20:05.862589  Verizon_f1:47:66   Apple_9c:a6:65  0x0800       110  IPv4
 10  14:20:05.862794  Apple_9c:a6:65    Verizon_f1:47:66  0x0800       78  IPv4
 11  14:20:05.862848  Apple_9c:a6:65    Verizon_f1:47:66  0x0800       78  IPv4
 12  14:20:05.875531  Verizon_f1:47:66   Apple_9c:a6:65  0x0800        74  IPv4
 13  14:20:05.875583  Apple_9c:a6:65    Verizon_f1:47:66  0x0800       66  IPv4
 14  14:20:05.875877  Verizon_f1:47:66   Apple_9c:a6:65  0x0800        74  IPv4
 15  14:20:05.875908  Apple_9c:a6:65    Verizon_f1:47:66  0x0800       66  IPv4
 16  14:20:05.895968  Verizon_f1:47:66   Broadcast       ARP           42  Who has 192.168.1.160? Tell 192.168.1.1
```

```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ▶ Source: Verizon_f1:47:66 (48:5d:36:f1:47:66)
     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: Verizon_f1:47:66 (48:5d:36:f1:47:66)
     Sender IP address: 192.168.1.1
     Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
     Target IP address: 192.168.1.160
```

```
0000  ff ff ff ff ff ff 48 5d  36 f1 47 66 08 06 00 01   ......H] 6.Gf....
0010  08 00 06 04 00 01 48 5d  36 f1 47 66 c0 a8 01 01   ......H] 6.Gf....
0020  00 00 00 00 00 00 c0 a8  01 a0                     ........ ..
```

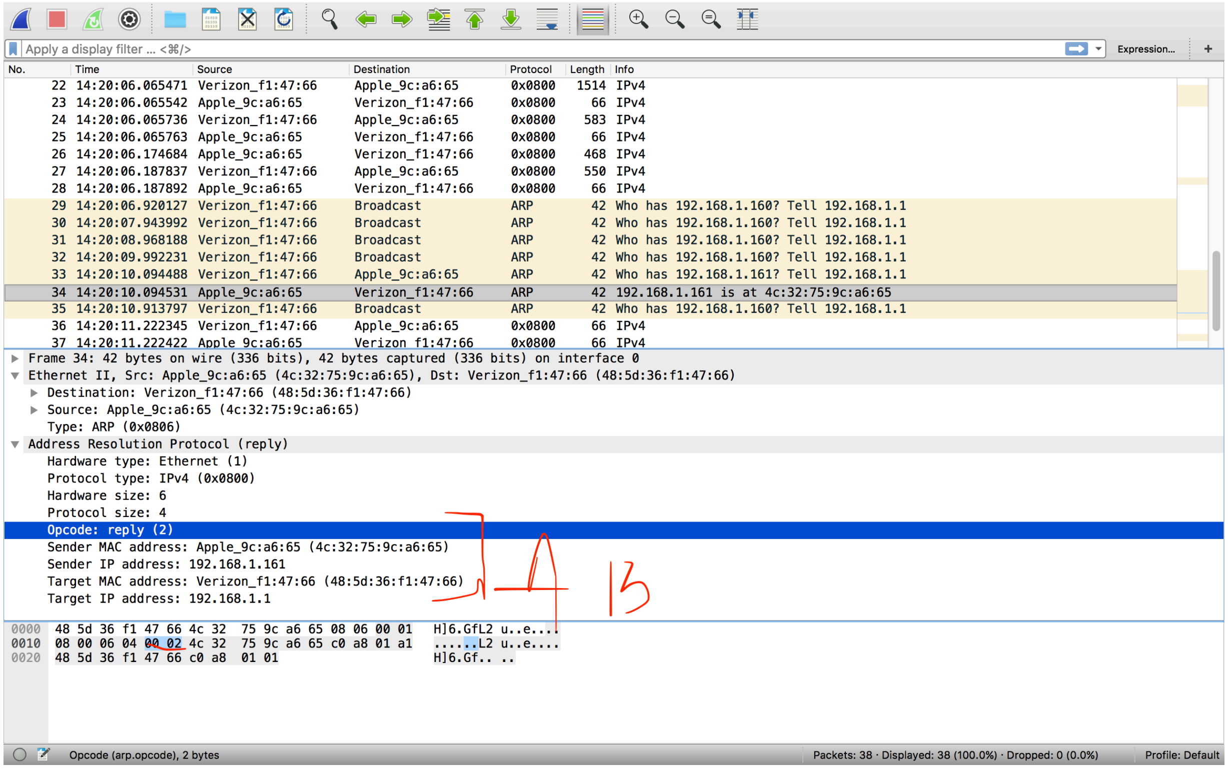
wireshark_en0_20170423142001_d0R54j

13. 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? 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? 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?

Ans.) A) As per the screenshot below the ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

B) As per the screenshot above the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made is "reply (2)" or hex "0x0002".

C) The answer to the earlier ARP request which was "who has 192.168.1.161 tell 192.168.1.1" is in the "Sender MAC address" field, which contains the Ethernet address "4c:32:75:9c:a6:65" for the sender with IP address “192.168.1.161”.



```
No.   Time             Source           Destination      Protocol  Length  Info
   22 14:20:06.065471 Verizon_f1:47:66 Apple_9c:a6:65   0x0800    1514  IPv4
   23 14:20:06.065542 Apple_9c:a6:65   Verizon_f1:47:66 0x0800      66  IPv4
   24 14:20:06.065736 Verizon_f1:47:66 Apple_9c:a6:65   0x0800     583  IPv4
   25 14:20:06.065763 Apple_9c:a6:65   Verizon_f1:47:66 0x0800      66  IPv4
   26 14:20:06.174684 Apple_9c:a6:65   Verizon_f1:47:66 0x0800     468  IPv4
   27 14:20:06.187837 Verizon_f1:47:66 Apple_9c:a6:65   0x0800     550  IPv4
   28 14:20:06.187892 Apple_9c:a6:65   Verizon_f1:47:66 0x0800      66  IPv4
   29 14:20:06.920127 Verizon_f1:47:66 Broadcast        ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
   30 14:20:07.943992 Verizon_f1:47:66 Broadcast        ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
   31 14:20:08.968188 Verizon_f1:47:66 Broadcast        ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
   32 14:20:09.992231 Verizon_f1:47:66 Broadcast        ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
   33 14:20:10.094488 Verizon_f1:47:66 Apple_9c:a6:65   ARP         42  Who has 192.168.1.161? Tell 192.168.1.1
   34 14:20:10.094531 Apple_9c:a6:65   Verizon_f1:47:66 ARP         42  192.168.1.161 is at 4c:32:75:9c:a6:65
   35 14:20:10.913797 Verizon_f1:47:66 Broadcast        ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
   36 14:20:11.222345 Verizon_f1:47:66 Apple_9c:a6:65   0x0800      66  IPv4
   37 14:20:11.222422 Apple_9c:a6:65   Verizon_f1:47:66 0x0800      66  IPv4
```

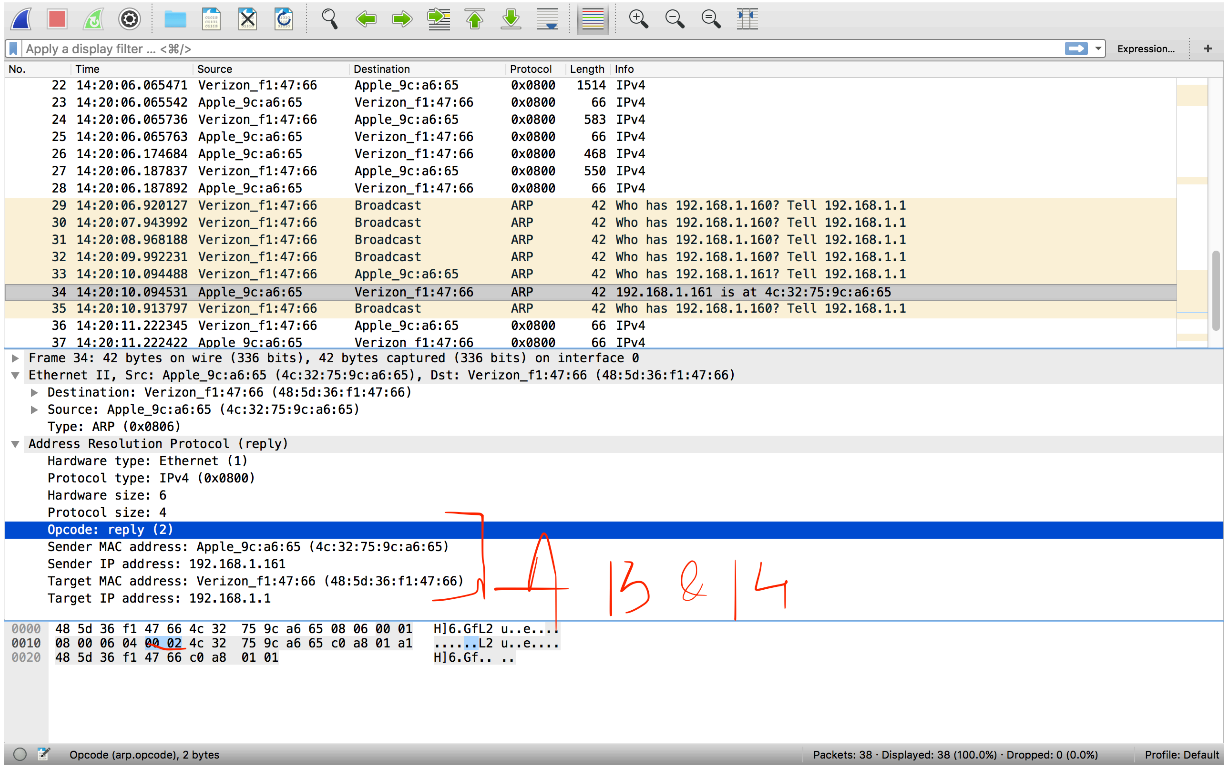
```
▶ Frame 34: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Destination: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Source: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
    Sender IP address: 192.168.1.161
    Target MAC address: Verizon_f1:47:66 (48:5d:36:f1:47:66)
    Target IP address: 192.168.1.1
```

```
0000  48 5d 36 f1 47 66 4c 32  75 9c a6 65 08 06 00 01   H]6.GfL2 u..e....
0010  08 00 06 04 00 02 4c 32  75 9c a6 65 c0 a8 01 a1   ......L2 u..e....
0020  48 5d 36 f1 47 66 c0 a8  01 01                     H]6.Gf.. ..
```

Opcode (arp.opcode), 2 bytes
Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

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

Ans.) As per the screenshot below the hexadecimal values for the source address is “4c: 32:75:9c:a6:65” and that for destination address is “48:5d:36:f1:47:66”.



```
No.  Time             Source             Destination        Protocol  Length  Info
  22 14:20:06.065471  Verizon_f1:47:66   Apple_9c:a6:65     0x0800    1514  IPv4
  23 14:20:06.065542  Apple_9c:a6:65     Verizon_f1:47:66   0x0800      66  IPv4
  24 14:20:06.065736  Verizon_f1:47:66   Apple_9c:a6:65     0x0800     583  IPv4
  25 14:20:06.065763  Apple_9c:a6:65     Verizon_f1:47:66   0x0800      66  IPv4
  26 14:20:06.174684  Apple_9c:a6:65     Verizon_f1:47:66   0x0800     468  IPv4
  27 14:20:06.187837  Verizon_f1:47:66   Apple_9c:a6:65     0x0800     550  IPv4
  28 14:20:06.187892  Apple_9c:a6:65     Verizon_f1:47:66   0x0800      66  IPv4
  29 14:20:06.920127  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
  30 14:20:07.943992  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
  31 14:20:08.968188  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
  32 14:20:09.992231  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
  33 14:20:10.094488  Verizon_f1:47:66   Apple_9c:a6:65     ARP         42  Who has 192.168.1.161? Tell 192.168.1.1
  34 14:20:10.094531  Apple_9c:a6:65     Verizon_f1:47:66   ARP         42  192.168.1.161 is at 4c:32:75:9c:a6:65
  35 14:20:10.913797  Verizon_f1:47:66   Broadcast          ARP         42  Who has 192.168.1.160? Tell 192.168.1.1
  36 14:20:11.222345  Verizon_f1:47:66   Apple_9c:a6:65     0x0800      66  IPv4
  37 14:20:11.222422  Apple_9c:a6:65     Verizon_f1:47:66   0x0800      66  IPv4
```

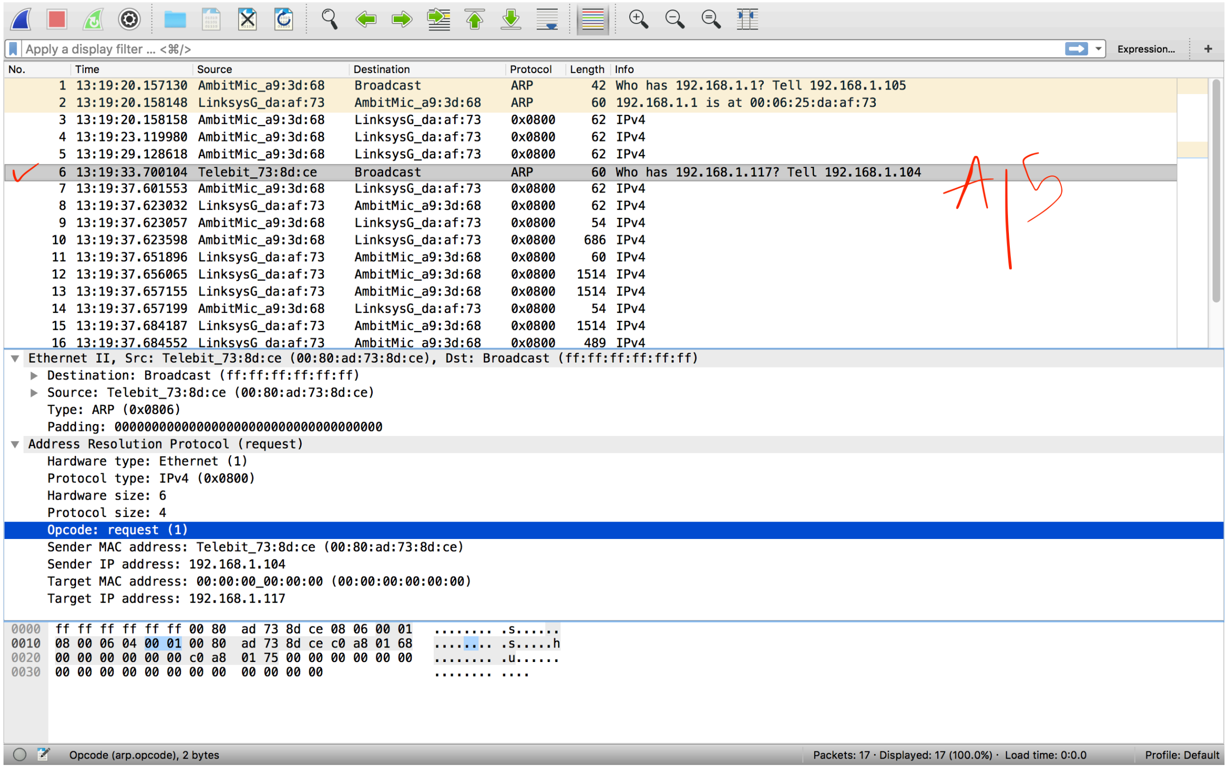
```
▶ Frame 34: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Destination: Verizon_f1:47:66 (48:5d:36:f1:47:66)
  ▶ Source: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
    Sender IP address: 192.168.1.161
    Target MAC address: Verizon_f1:47:66 (48:5d:36:f1:47:66)
    Target IP address: 192.168.1.1
```

```
0000  48 5d 36 f1 47 66 4c 32  75 9c a6 65 08 06 00 01   H]6.GfL2 u..e....
0010  08 00 06 04 00 02 4c 32  75 9c a6 65 c0 a8 01 a1   ......L2 u..e....
0020  48 5d 36 f1 47 66 c0 a8  01 01                     H]6.Gf.. ..
```

```
Opcode (arp.opcode), 2 bytes          Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

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?

Ans.) As per the screenshot below there is no reply in this trace for the ARP request in packet 6 because my computer is not the machine "192.168.1.117". The request says that the machine with "192.168.1.117" has to reply with its MAC address to the machine with IP address "192.168.1.104".



```
No.  Time             Source              Destination         Protocol  Length  Info
  1  13:19:20.157130  AmbitMic_a9:3d:68   Broadcast           ARP           42  Who has 192.168.1.1? Tell 192.168.1.105
  2  13:19:20.158148  LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP           60  192.168.1.1 is at 00:06:25:da:af:73
  3  13:19:20.158158  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        62  IPv4
  4  13:19:23.119980  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        62  IPv4
  5  13:19:29.128618  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        62  IPv4
✓ 6  13:19:33.700104  Telebit_73:8d:ce    Broadcast           ARP           60  Who has 192.168.1.117? Tell 192.168.1.104
  7  13:19:37.601553  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        62  IPv4
  8  13:19:37.623032  LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800        62  IPv4
  9  13:19:37.623057  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        54  IPv4
 10  13:19:37.623598  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800       686  IPv4
 11  13:19:37.651896  LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800        60  IPv4
 12  13:19:37.656065  LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      1514  IPv4
 13  13:19:37.657155  LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      1514  IPv4
 14  13:19:37.657199  AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        54  IPv4
 15  13:19:37.684187  LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      1514  IPv4
 16  13:19:37.684552  LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800       489  IPv4
```

A15

```
▼ Ethernet II, Src: Telebit_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Telebit_73:8d:ce (00:80:ad:73:8d:ce)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Telebit_73:8d:ce (00:80:ad:73:8d:ce)
    Sender IP address: 192.168.1.104
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.117
```

```
0000  ff ff ff ff ff ff 00 80  ad 73 8d ce 08 06 00 01   ........ .s......
0010  08 00 06 04 00 01 00 80  ad 73 8d ce c0 a8 01 68   ........ .s.....h
0020  00 00 00 00 00 00 c0 a8  01 75 00 00 00 00 00 00   ........ .u......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Opcode (arp.opcode), 2 bytes   Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.0   Profile: Default