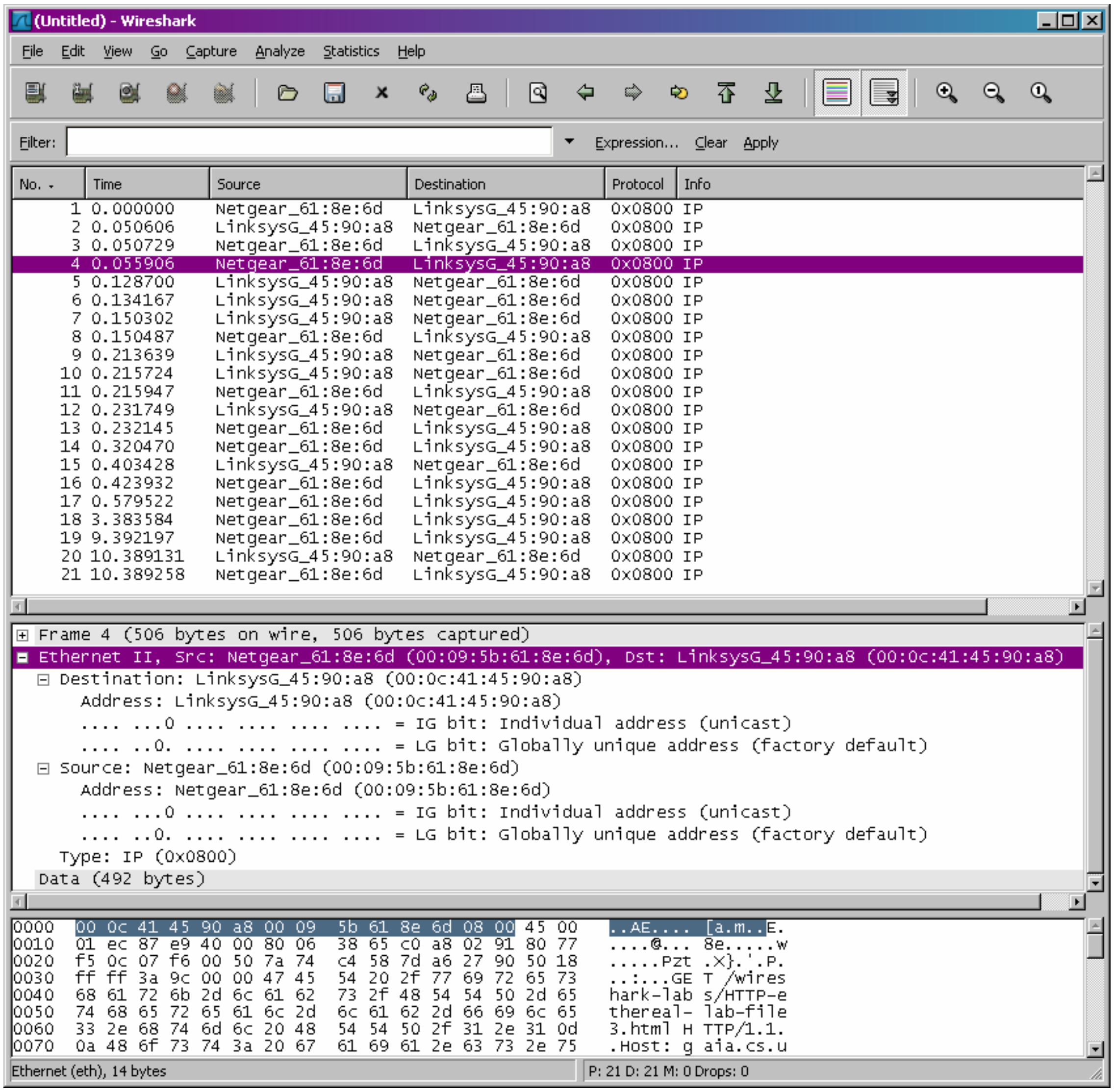
Solution to Wireshark Lab: Ethernet and ARP


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info

```
No. .  Time       Source             Destination        Protocol Info
    1 0.000000   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
    2 0.050606   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
    3 0.050729   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
    4 0.055906   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
    5 0.128700   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
    6 0.134167   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
    7 0.150302   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
    8 0.150487   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
    9 0.213639   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
   10 0.215724   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
   11 0.215947   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   12 0.231749   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
   13 0.232145   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   14 0.320470   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   15 0.403428   LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
   16 0.423932   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   17 0.579522   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   18 3.383584   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   19 9.392197   Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
   20 10.389131  LinksysG_45:90:a8  Netgear_61:8e:6d   0x0800 IP
   21 10.389258  Netgear_61:8e:6d   LinksysG_45:90:a8  0x0800 IP
```

```
⊞ Frame 4 (506 bytes on wire, 506 bytes captured)
⊟ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
  ⊟ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
      Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
      Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
  Data (492 bytes)
```

```
0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  01 ec 87 e9 40 00 80 06  38 65 c0 a8 02 91 80 77   ....@... 8e.....w
0020  f5 0c 07 f6 00 50 7a 74  c4 58 7d a6 27 90 50 18   .....Pzt .X}.'.P.
0030  ff ff 3a 9c 00 00 47 45  54 20 2f 77 69 72 65 73   ..:...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
```

```
Ethernet (eth), 14 bytes        P: 21 D: 21 M: 0 Drops: 0
```

Fig. 1 GET request Ethernet information

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

   The Ethernet address of my computer is 00:09:5b:61:8e:6d

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.]

The destination address 00:0c:41:45:90:a8 is not the Ethernet address of gaia.cs.umass.edu. It is the address of my Linksys router, which is the link used to get off the subnet.

3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

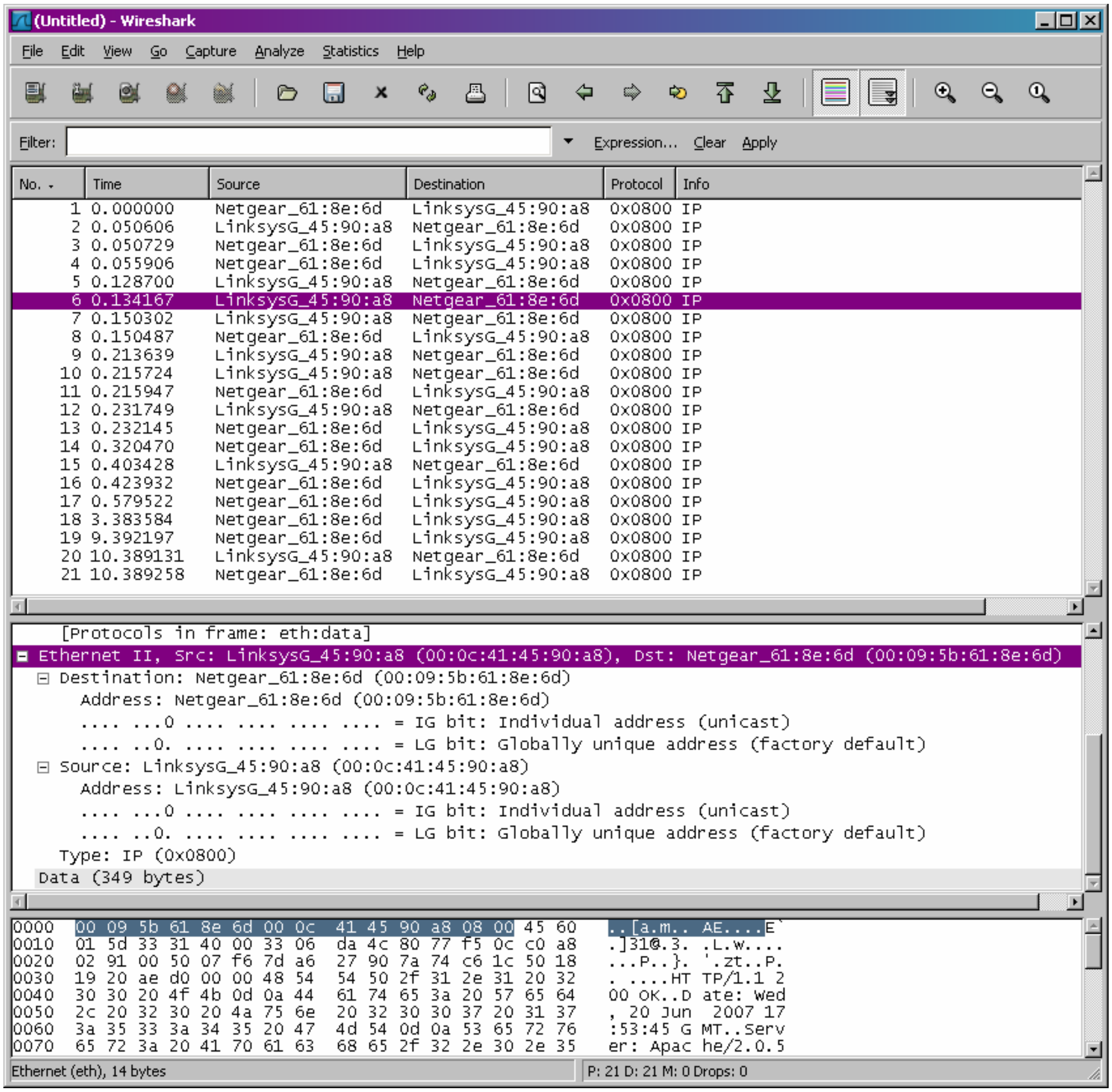
   The hex value for the Frame type field is 0x0800.

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 52 bytes from the start of the ethernet frame. There are 14 B Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.

5. What is the hexadecimal value of the CRC field in this Ethernet frame?

   The hex value for the CRC field is 0x 0d0a 0d0a.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time       Source              Destination         Protocol Info
    1 0.000000   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
    2 0.050606   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
    3 0.050729   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
    4 0.055906   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
    5 0.128700   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
    6 0.134167   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
    7 0.150302   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
    8 0.150487   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
    9 0.213639   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
   10 0.215724   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
   11 0.215947   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   12 0.231749   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
   13 0.232145   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   14 0.320470   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   15 0.403428   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
   16 0.423932   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   17 0.579522   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   18 3.383584   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   19 9.392197   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
   20 10.389131  LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800 IP
   21 10.389258  Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800 IP
```

```
    [Protocols in frame: eth:data]
⊟ Ethernet II, Src: LinksysG_45:90:a8 (00:0c:41:45:90:a8), Dst: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
  ⊟ Destination: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
      Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
      Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
  Data (349 bytes)
```

```
0000  00 09 5b 61 8e 6d 00 0c  41 45 90 a8 08 00 45 60   ..[a.m.. AE....E`
0010  01 5d 33 31 40 00 33 06  da 4c 80 77 f5 0c c0 a8   .]31@.3. .L.w....
0020  02 91 00 50 07 f6 7d a6  27 90 7a 74 c6 1c 50 18   ...P..}. '.zt..P.
0030  19 20 ae d0 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 57 65 64   00 OK..D ate: Wed
0050  2c 20 32 30 20 4a 75 6e  20 32 30 30 37 20 31 37   , 20 Jun  2007 17
0060  3a 35 33 3a 34 35 20 47  4d 54 0d 0a 53 65 72 76   :53:45 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 30 2e 35   er: Apac he/2.0.5
```

Ethernet (eth), 14 bytes | P: 21 D: 21 M: 0 Drops: 0

Fig. 2 OK response Ethernet information

6. 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?

   The source address 00:0c:41:45:90:a8 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my Linksys router, which is the link used to get onto my subnet.

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

   The destination address 00:09:5b:61:8e:6d is the address of computer.

8. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

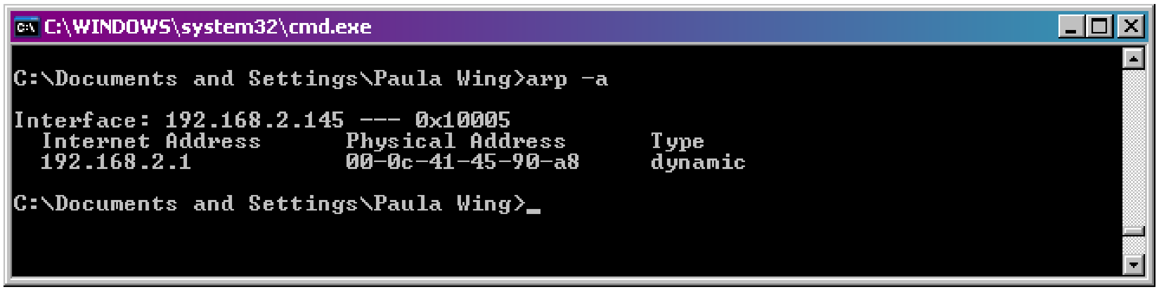
The hex value for the Frame type field is 0x0800.

9. 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?

   The ASCII "O" appears 52 bytes from the start of the ethernet frame. Again, there are 14 bytes of Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.

10. What is the hexadecimal value of the CRC field in this Ethernet frame?

    The hex value for the CRC field is 0x 0d0a 0d0a.

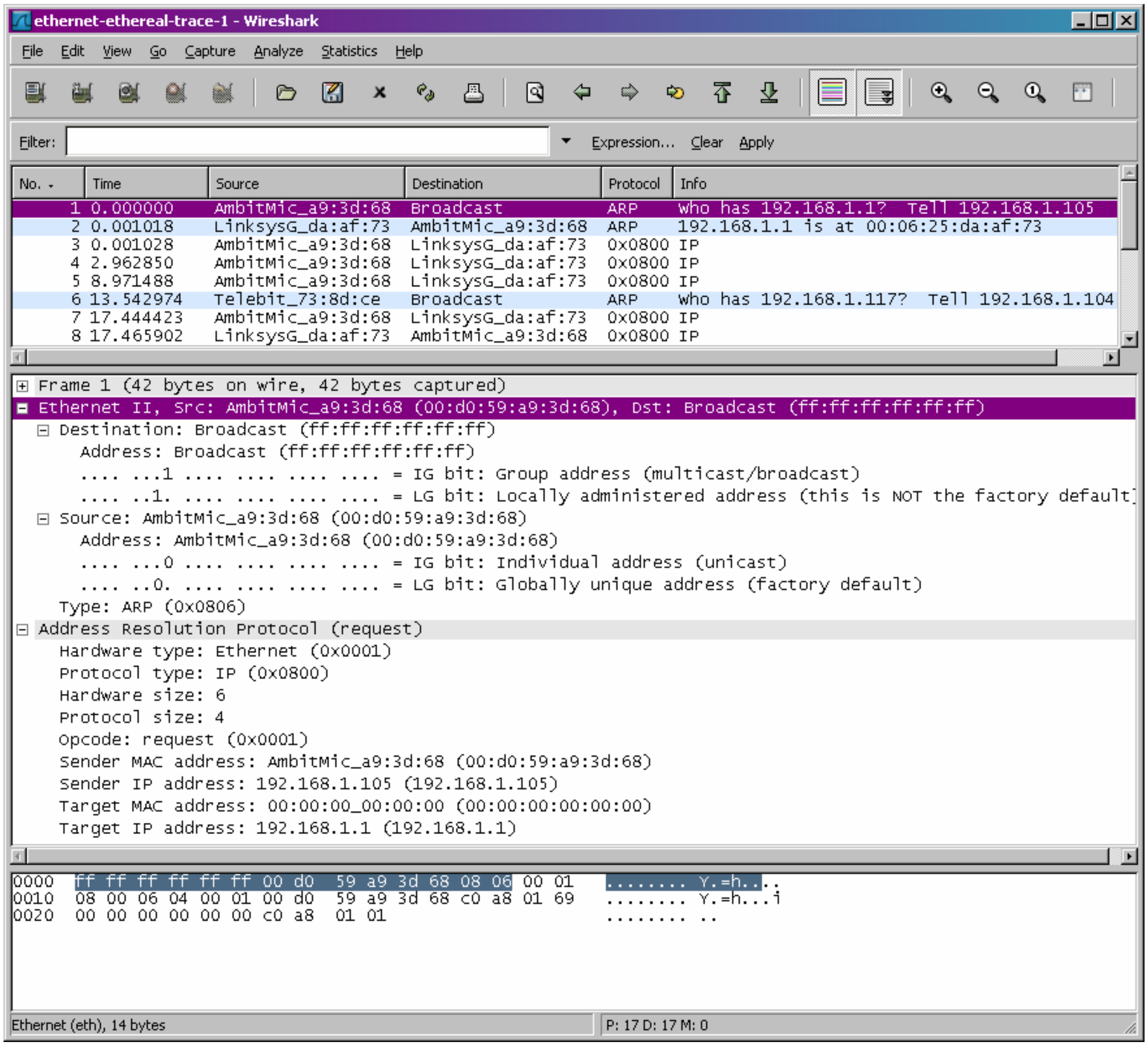


```
C:\Documents and Settings\Paula Wing>arp -a

Interface: 192.168.2.145 --- 0x10005
  Internet Address      Physical Address      Type
  192.168.2.1           00-0c-41-45-90-a8     dynamic

C:\Documents and Settings\Paula Wing>_
```

Fig. 3 Command prompt after executing arp

11. 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 indicates the protocol type.



```
No. .  Time        Source               Destination          Protocol Info
     1 0.000000    AmbitMic_a9:3d:68    Broadcast            ARP      who has 192.168.1.1?  Tell 192.168.1.105
     2 0.001018    LinksysG_da:af:73    AmbitMic_a9:3d:68    ARP      192.168.1.1 is at 00:06:25:da:af:73
     3 0.001028    AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800 IP
     4 2.962850    AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800 IP
     5 8.971488    AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800 IP
     6 13.542974   Telebit_73:8d:ce     Broadcast            ARP      who has 192.168.1.117?  Tell 192.168.1.104
     7 17.444423   AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800 IP
     8 17.465902   LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800 IP
```

```
⊞ Frame 1 (42 bytes on wire, 42 bytes captured)
⊟ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default]
  ⊟ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105 (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 (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                     ........ ..
```

Ethernet (eth), 14 bytes   P: 17 D: 17 M: 0

Fig. 4 ARP request message

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

    The hex value for the source address is 00:d0:59:a9:3d:68. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.

13. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

    The hex value for the Ethernet Fram type field is 0x0806, for ARP.

14. 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?

    The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

    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?

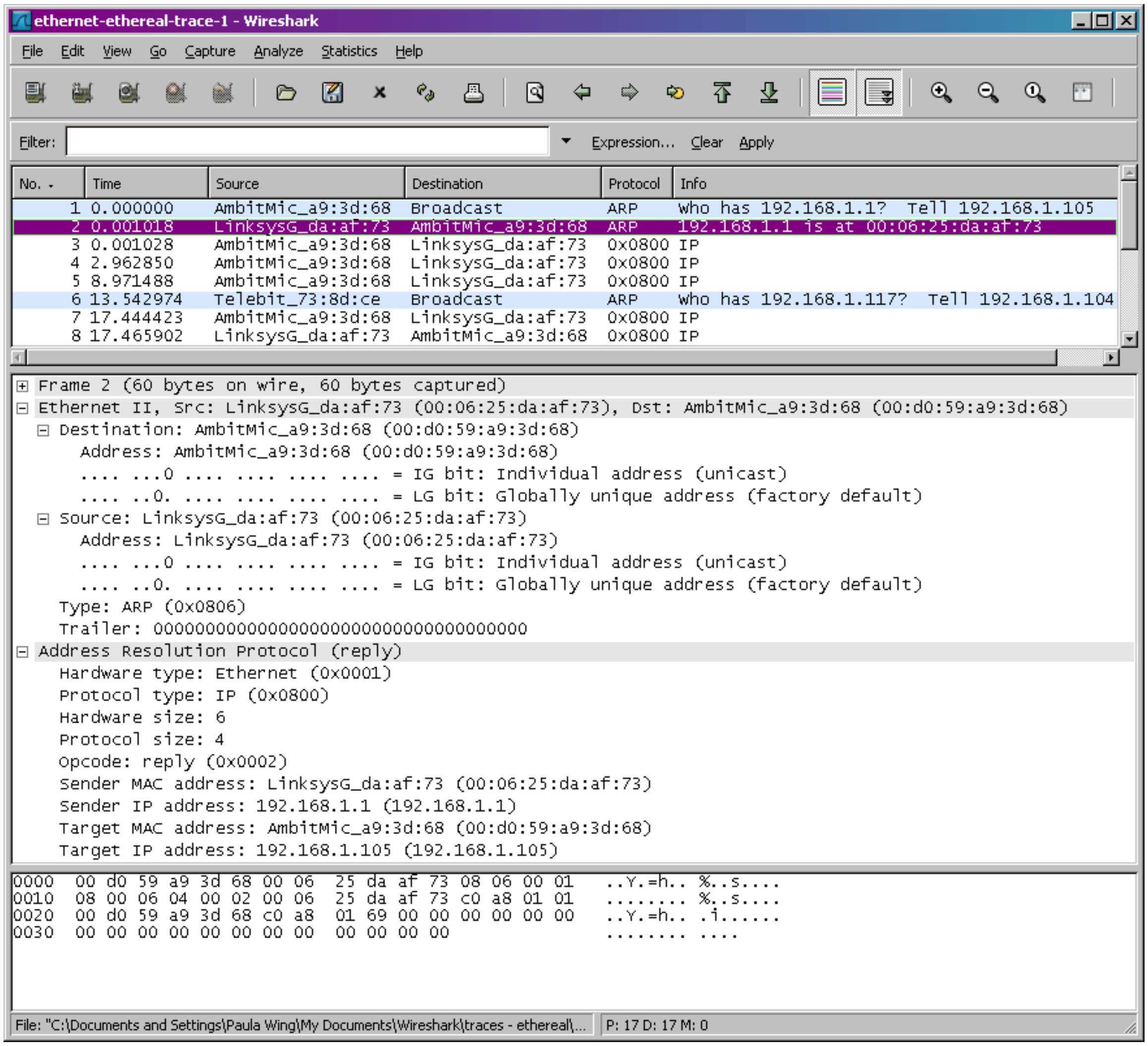
    The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request.

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

    Yes, the ARP message containg the IP address 192.168.1.105 for 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?

    The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.


ethernet-ethereal-trace-1 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time         Source              Destination         Protocol  Info
     1 0.000000     AmbitMic_a9:3d:68   Broadcast           ARP       Who has 192.168.1.1?  Tell 192.168.1.105
     2 0.001018     LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP       192.168.1.1 is at 00:06:25:da:af:73
     3 0.001028     AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800 IP
     4 2.962850     AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800 IP
     5 8.971488     AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800 IP
     6 13.542974    Telebit_73:8d:ce    Broadcast           ARP       Who has 192.168.1.117?  Tell 192.168.1.104
     7 17.444423    AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800 IP
     8 17.465902    LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800 IP
```

```
⊞ Frame 2 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  ⊟ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1 (192.168.1.1)
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105 (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               ........ ....
```

File: "C:\Documents and Settings\Paula Wing\My Documents\Wireshark\traces - ethereal\... P: 17 D: 17 M: 0

Fig. 5 ARP reply message

15. 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?

The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

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 hex value for opcode field withing the ARP-payload of the request is 0x0002, for 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 earlier ARP request appears in the"Sender MAC address" field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.

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

    The hex value for the source address is 00:06:25:da:af:73 and for the destination is 00:d0:59:a9:3d:68 .

17. 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 indiated 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 machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.