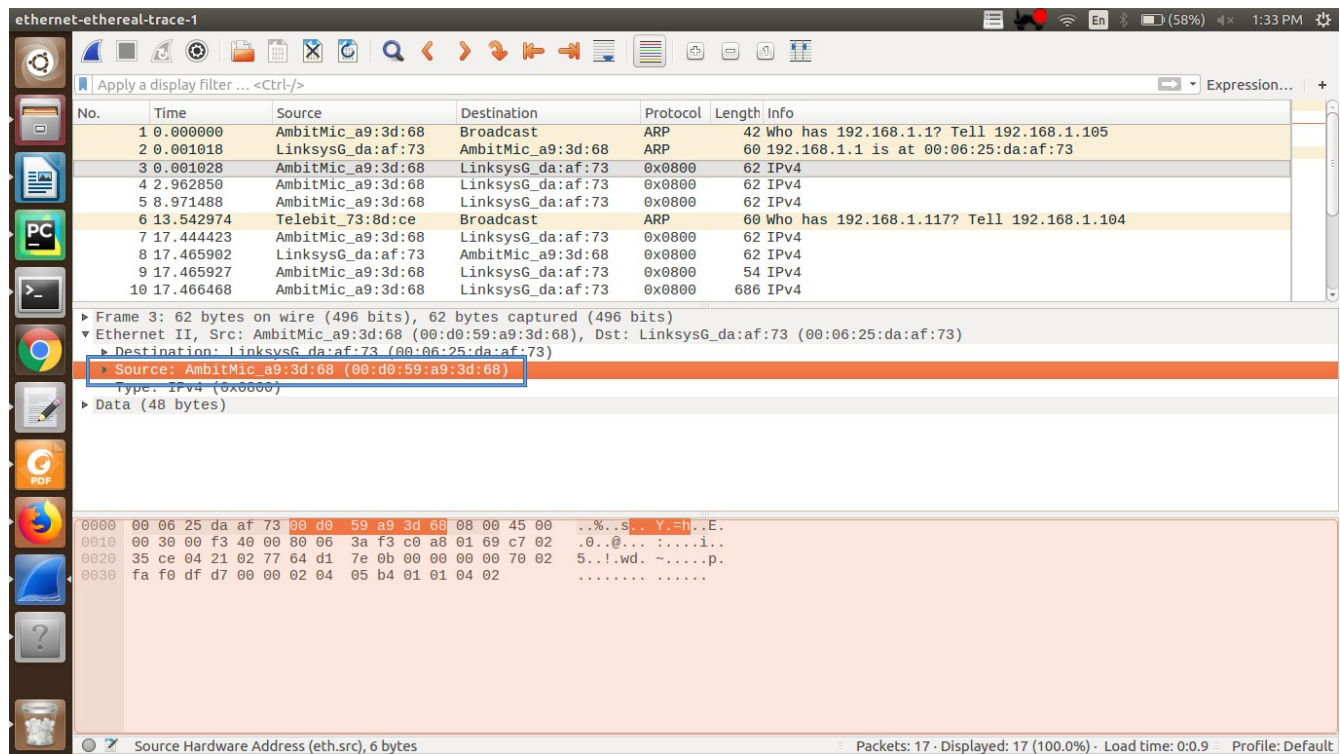


Q1 - What is the 48-bit Ethernet address of your computer?

Ans: Ethernet Address of computer: 00:d0:59:a9:3d:68



Q2. 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?

Ans: 1) Destination address of ethernet frame: 00:06:25:da:af:73

2) No, this is not the ethernet address of gaia.cs.umass.edu.

3) It is the ethernet address of the LinkSys router, which is the link used to get off the subnet.

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG\_da:af:73 (00:06:25:da:af:73)

Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)

Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Type: IPv4 (0x0800)

Data (48 bytes)

```

0000 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00  ..%..s..Y.=h..E.
0010 00 30 00 f3 40 00 00 06 3a f3 c0 a8 01 69 c7 02  .0..@...:....i..
0020 35 ce 04 21 02 77 64 d1 7e 0b 00 00 00 00 70 02  5..!wd.~.....p.
0030 fa f0 df d7 00 00 02 04 05 b4 01 01 04 02      .....

```

Destination Hardware Address (eth.dst), 6 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

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

Ans: a) Hexadecimal value in frame type field: 0x0800

b) It corresponds to IPv4 network layer protocol

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG\_da:af:73 (00:06:25:da:af:73)

Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)

Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Type: IPv4 (0x0800)

Data (48 bytes)

```

0000 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00  ..%..s..Y.=h..E.
0010 00 30 00 f3 40 00 00 06 3a f3 c0 a8 01 69 c7 02  .0..@...:....i..
0020 35 ce 04 21 02 77 64 d1 7e 0b 00 00 00 00 70 02  5..!wd.~.....p.
0030 fa f0 df d7 00 00 02 04 05 b4 01 01 04 02      .....

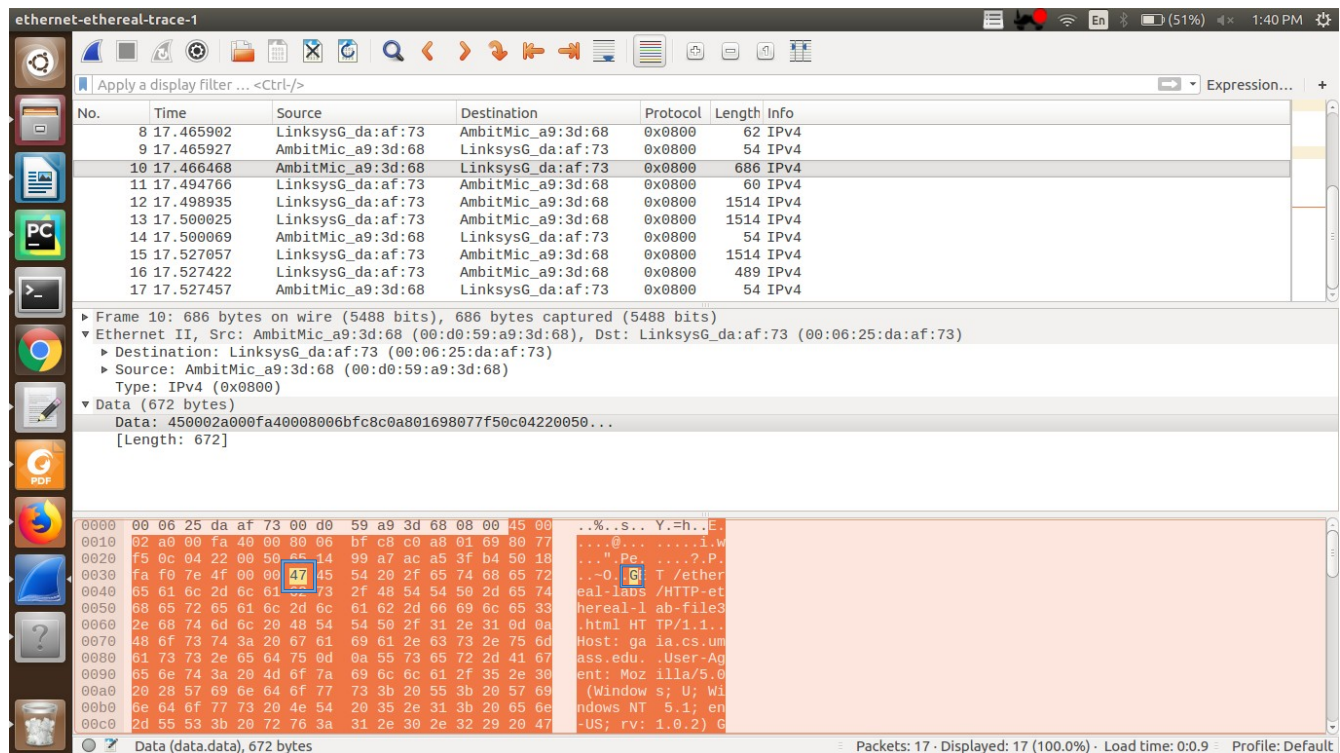
```

Type (eth.type), 2 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · 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: 54 bytes



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: 1) Ethernet Source Address: 00:06:25:da:af:73

2) No, this is not the IP address of gaia.cs.umass.edu

3) No, it is the IP address of gateway router



ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

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)

Source: LinksysG\_da:af:73 (00:06:25:da:af:73)

Type: IPv4 (0x0800)

Data (1500 bytes)

Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422...

[Length: 1500]

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ...Y.=h...%.s..E

0010 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 .../0.7. v..w...

0020 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 ..i.P"...?e...P.

0030 1b 28 5e 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 53 61 74 00 OK..D ate: Sat

0050 2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 : 28 Aug 2004 17

0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 :19:37 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux

0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 )..Last- Modified

00a0 3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30 : Sat, 2 8 Aug 20

00b0 30 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d 04 17:18 :53 GMT.

00c0 0a 45 54 61 67 3a 20 22 31 62 61 35 63 2d 31 31 .ETag: " 1ba5c-11

Data (data.data), 1500 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

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

Ans: Destination address of the ethernet frame: 00:d0:59:a9:3d:68, Yes this is the ethernet address of my computer.

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

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)

Source: LinksysG\_da:af:73 (00:06:25:da:af:73)

Type: IPv4 (0x0800)

Data (1500 bytes)

Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422...

[Length: 1500]

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ...Y.=h...%.s..E

0010 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 .../0.7. v..w...

0020 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 ..i.P"...?e...P.

0030 1b 28 5e 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 53 61 74 00 OK..D ate: Sat

0050 2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 : 28 Aug 2004 17

0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 :19:37 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux

0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 )..Last- Modified

00a0 3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30 : Sat, 2 8 Aug 20

00b0 30 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d 04 17:18 :53 GMT.

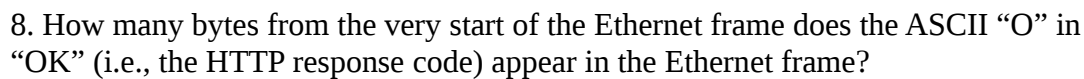
00c0 0a 45 54 61 67 3a 20 22 31 62 61 35 63 2d 31 31 .ETag: " 1ba5c-11

Destination Hardware Address (eth.dst), 6 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

Ans: 1) Hexadecimal value of type field: 0x0080  
2) It corresponds to the IPv4 network layer protocol

2) It corresponds to the IPv4 network layer protocol



Ans: "O" appears 52 bytes from the start of the ethernet frame.

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

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)

Source: LinksysG\_da:af:73 (00:06:25:da:af:73)

Type: IPv4 (0x0800)

Data (1500 bytes)

Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422...

[Length: 1500]

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ...Y.=h...%.s..E

0010 85 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 .../0.7. v..w....

0020 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 ...i.P."...?e...P.

0030 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 ...(\A...HT TP/1.1 2

0040 39 30 28 4f 1b 0d 0a 44 61 74 65 3a 20 53 61 74 ...00[OK]..D ate: Sat

0050 2c 20 32 39 20 41 75 67 20 32 30 30 34 20 31 37 ...20 Aug 2004 17

0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 ...:19:37 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 ...er: Apac he/2.0.4

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 ...0 (Red H at Linux

0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 ...)..Last- Modified

00a0 3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 36 ...: Sat, 2 0 Aug 20

00b0 30 3a 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d ...04 17:18 :53 GMT.

00c0 3a 45 54 61 67 3a 20 2d 31 62 61 35 63 2d 31 31 ...ETag: " 1ba5c-11

Data (data.data), 1500 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

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

Ans: Source: 00:d0:59:a9:3d:68

Destination: ff:ff:ff:ff:ff:ff

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

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)

Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Type: ARP (0x0806)

Address Resolution Protocol (request)

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-ethereal-trace-1

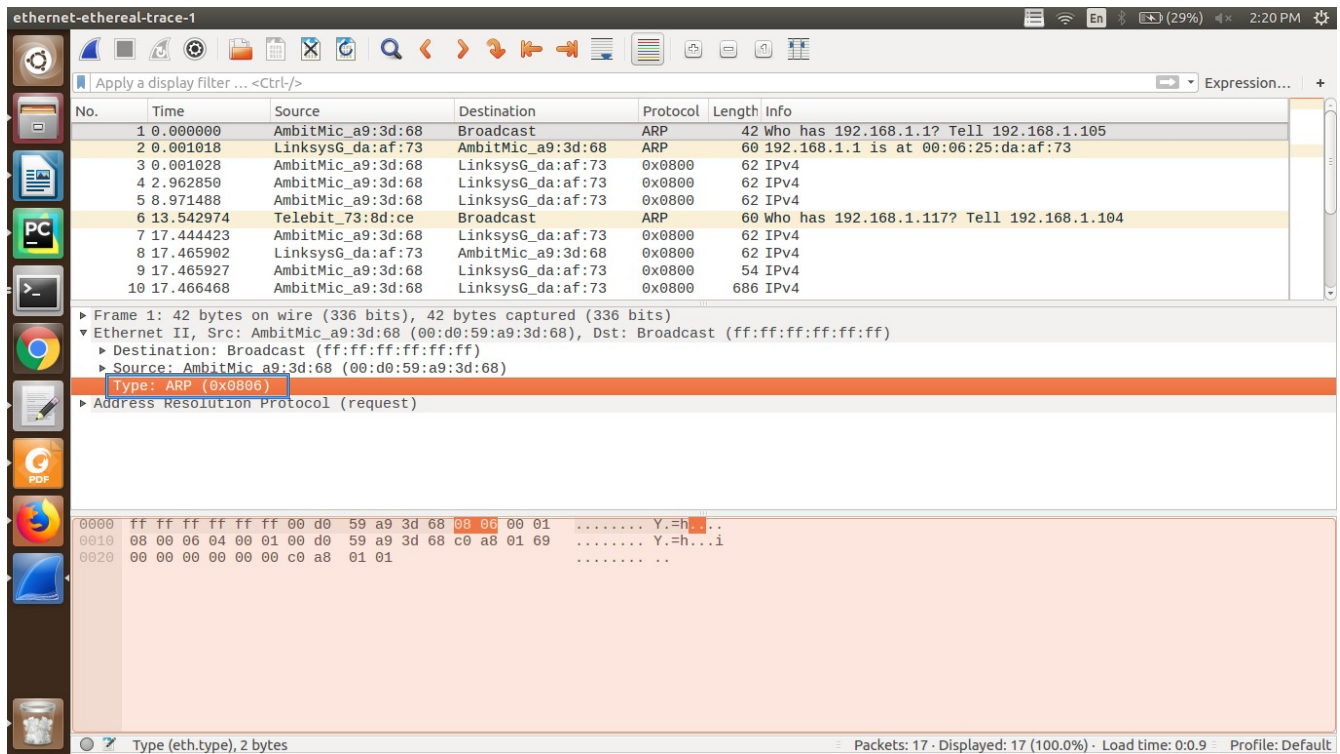
Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default



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

Ans: a) Type: 0x0806

b) It corresponds to ARP protocol



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

Ans: 20 bytes from the beginning of the ethernet frame

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

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)

Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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 .....Y.=h...i

Opcode (arp.opcode), 2 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

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?

Ans: The value of OpCode field is 1.

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

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)

Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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 .....Y.=h...i

Opcode (arp.opcode), 2 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default



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

Ans: Yes, the ARP message contain the IP address of the sender

ethernet-ethereal-trace-1

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	686	IPv4

Type: ARP (0x0006)  
▼ Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0006)  
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 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 .....

Opcode (arp.opcode), 2 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

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

Ans: In the Target IP address field of the ARP request 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.



Ans: Value of Opcode in the ARP payload part: 0x002 (Reply)

The screenshot shows a Wireshark packet capture of an ARP request and its reply. The packet list on the left shows 10 packets. Packet 2, at time 0.001018, is an ARP request from LinksysG\_da:af:73 to AmbitMic\_a9:3d:68. Packet 6, at time 13.542974, is an ARP reply from Telebit\_73:8d:ce to LinksysG\_da:af:73. The packet details pane for packet 6 shows the following fields:

- Type: ARP (0x0806)
- Padding: 00000000000000000000000000000000
- 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

The packet bytes pane shows the raw data of the ARP reply, with the opcode field (0002) highlighted in red.

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: The Answer to the earlier ARP request appear in the Sender MAC address of the ARP field i.e. 00:06:25:da:af:73

The screenshot shows a Wireshark packet capture of an ARP request and its reply. The packet list on the left shows 10 packets. Packet 2, at time 0.001018, is an ARP request from LinksysG\_da:af:73 to AmbitMic\_a9:3d:68. Packet 6, at time 13.542974, is an ARP reply from Telebit\_73:8d:ce to LinksysG\_da:af:73. The packet details pane for packet 6 shows the following fields:

- Type: ARP (0x0806)
- Padding: 00000000000000000000000000000000
- 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

The packet bytes pane shows the raw data of the ARP reply, with the sender MAC address field (00 06 25 da af 73) highlighted in red.



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

Ans: Source address in the Ethernet frame: 00:06:25:da:af:73

Destination Address in the Ethernet frame: 00:d0:59:a9:3d:68

The image shows a Wireshark packet capture titled "ethernet-ethereal-trace-1". The packet list on the left shows 10 packets. Packet 2, at time 0.001018, is an ARP reply from LinksysG\_da:af:73 to AmbitMic\_a9:3d:68. The packet details pane on the right shows the "Address Resolution Protocol (reply)" section. The "Sender MAC address" is highlighted as "LinksysG\_da:af:73 (00:06:25:da:af:73)". The "Target MAC address" is highlighted as "AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)". The packet bytes pane at the bottom shows the raw data of the packet, with the first 6 bytes (00 d0 59 a9 3d 68) highlighted in orange, corresponding to the destination MAC address.

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

Padding: 00000000000000000000000000000000

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 00 00 .....  
.....

Sender MAC address (arp.src.hw\_mac), 6 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default

Q15) Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?  
 Ans: Because we are not at the sender and the reply of the ARP request is sent to the Sender, which in this case is 00:80:ad:73:8d:ce. Whereas our computer has sender address 00:d0:59:a9:3d:68.

The screenshot shows the Wireshark interface with a packet capture of an ARP request. The packet list on the left shows 17 packets, with packet 6 selected. The packet details pane on the right shows the structure of the ARP request, including the sender and target MAC and IP addresses. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	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	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	686	IPv4

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

Packet bytes (hex):  
 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 .....U.....  
 0030 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 .....

Sender MAC address (arp.src.hw\_mac), 6 bytes

Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:0.9 · Profile: Default