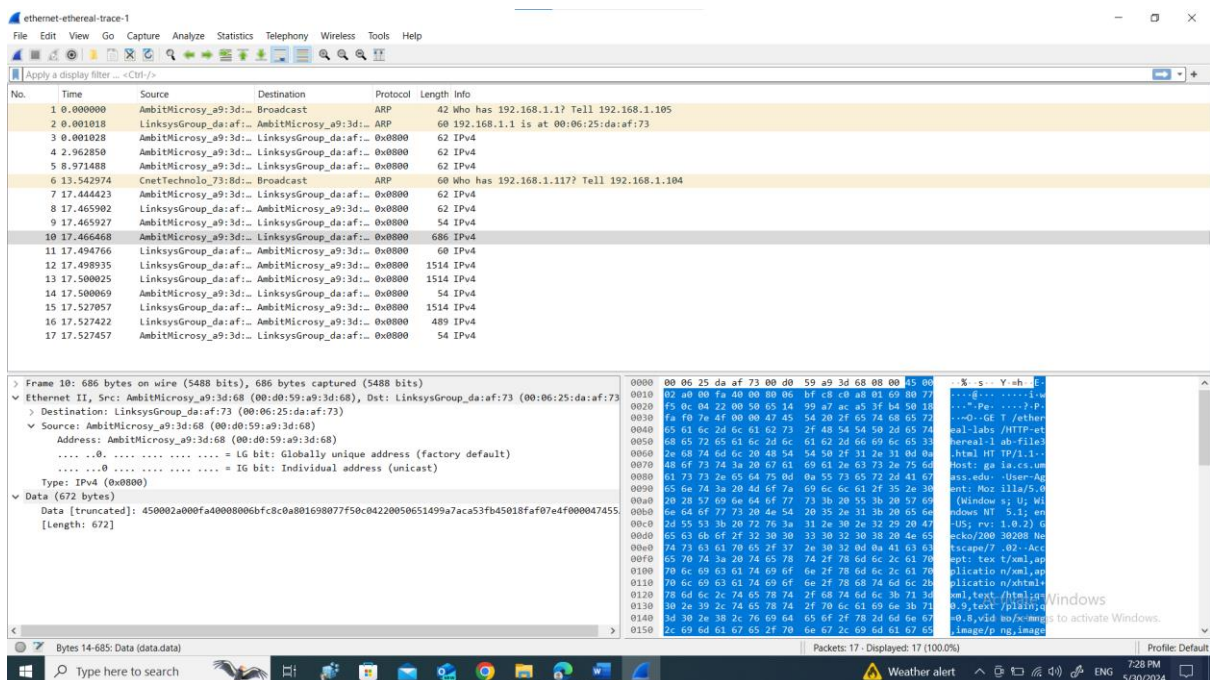


1. What is the 48-bit Ethernet address of your computer?



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.]

```

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
▼ Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  ▼ Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    Address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▼ Data (672 bytes)
  Data [truncated]: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf07e4f000047455
  [Length: 672]

```

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

```

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
▼ Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  > Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  > Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Type: IPv4 (0x0800)
> Data (672 bytes)

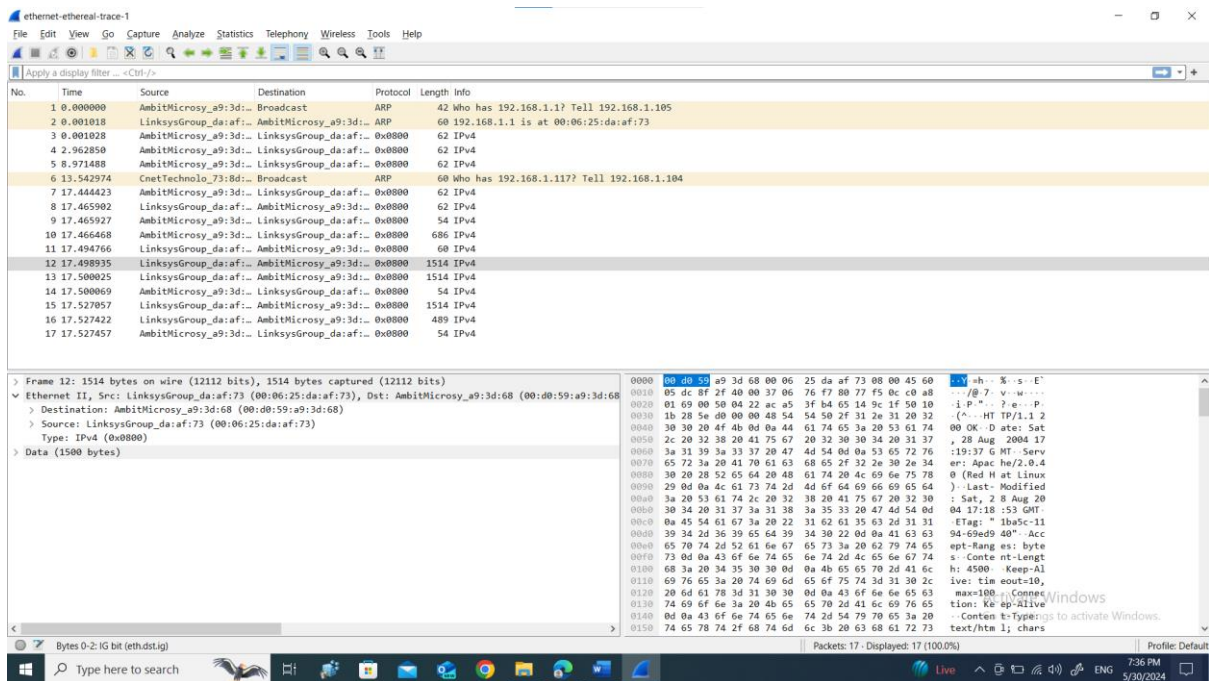
```

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

0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%.s..Y.=h..E.
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77@... ..i.w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	...".Pe.?.P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	...~0..GET /ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	real-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..
0070	48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: ga ia.cs.um
0080	61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67	ass.edu. ·User-Ag
0090	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00a0	20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69	(Window s; U; Wi
00b0	6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e	ndows NT 5.1; en
00c0	2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47	-US; rv: 1.0.2) G
00d0	65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65	ecko/200 30208 Ne
00e0	74 73 63 61 70 65 2f 37 2e 30 32 0d 0a 41 63 63	tscape/7 .02·Acc
00f0	65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70	ept: tex t/xml,ap
0100	70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70	plicatio n/xml,ap
0110	70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtml+
0120	78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d	xml,text /html;q=
0130	30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71	0.9,text /plain;q
0140	3d 30 2e 38 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67	=0.8,vid eo/;img
0150	2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65	,image/p ng,image

|| Packets: 17 · Displaved: 17 (100.0%)

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?



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

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  > Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  > Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Type: IPv4 (0x0800)
  > Data (1500 bytes)
```

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

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  > Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  > Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Type: IPv4 (0x0800)
  > Data (1500 bytes)
```

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?

00	d0	59	a9	3d	68	00	06	25	da	af	73	08	00	45	60	..Y.=h..%.s..E`
05	dc	8f	2f	40	00	37	06	76	f7	80	77	f5	0c	c0	a8	.../@.7.v..w....
01	69	00	50	04	22	ac	a5	3f	b4	65	14	9c	1f	50	10	.i.P."..?.e...P.
1b	28	5e	d0	00	00	48	54	54	50	2f	31	2e	31	20	32	.(^...HT TP/1.1 2
30	30	20	4f	4b	0d	0a	44	61	74	65	3a	20	53	61	74	00 OK..D ate: Sat
2c	20	32	38	20	41	75	67	20	32	30	30	34	20	31	37	, 28 Aug 2004 17
3a	31	39	3a	33	37	20	47	4d	54	0d	0a	53	65	72	76	:19:37 G MT..Serv
65	72	3a	20	41	70	61	63	68	65	2f	32	2e	30	2e	34	er: Apac he/2.0.4
30	20	28	52	65	64	20	48	61	74	20	4c	69	6e	75	78	0 (Red H at Linux
29	0d	0a	4c	61	73	74	2d	4d	6f	64	69	66	69	65	64)..Last- Modified
3a	20	53	61	74	2c	20	32	38	20	41	75	67	20	32	30	: Sat, 2 8 Aug 20
30	34	20	31	37	3a	31	38	3a	35	33	20	47	4d	54	0d	04 17:18 :53 GMT.
0a	45	54	61	67	3a	20	22	31	62	61	35	63	2d	31	31	.ETag: " 1ba5c-11
39	34	2d	36	39	65	64	39	34	30	22	0d	0a	41	63	63	94-69ed9 40"..Acc
65	70	74	2d	52	61	6e	67	65	73	3a	20	62	79	74	65	ept-Rang es: byte
73	0d	0a	43	6f	6e	74	65	6e	74	2d	4c	65	6e	67	74	s..Conte nt-Lengt
68	3a	20	34	35	30	30	0d	0a	4b	65	65	70	2d	41	6c	h: 4500. ·Keep-Al
69	76	65	3a	20	74	69	6d	65	6f	75	74	3d	31	30	2c	ive: tim eout=10,
20	6d	61	78	3d	31	30	30	0d	0a	43	6f	6e	6e	65	63	max=100. ·Conne
74	69	6f	6e	3a	20	4b	65	65	70	2d	41	6c	69	76	65	tion: Ke ep-Alive
0d	0a	43	6f	6e	74	65	6e	74	2d	54	79	70	65	3a	20	·Content-Type: t
74	65	78	74	2f	68	74	6d	6c	3b	20	63	68	61	72	73	text/html; chars

```

Command Prompt
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Al Amin>arp -a

Interface: 10.126.33.252 --- 0xd
Internet Address      Physical Address      Type
10.126.32.1           00-09-0f-09-00-1d    dynamic
10.126.63.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Al Amin>

```

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

```

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▼ Ethernet II, Src: AmbitMicrosy_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: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: ARP (0x0806)
> Address Resolution Protocol (request)

```

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

```

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▼ Ethernet II, Src: AmbitMicrosy_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: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: ARP (0x0806)
> Address Resolution Protocol (request)

```

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

The image shows the Wireshark interface. The 'Packet Details' pane on the left shows the following structure:

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: AmbitMicrosy_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

The 'Packet Bytes' pane on the right shows the raw data in hexadecimal and ASCII:

```

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

```

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. 00 01

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

The image shows the Wireshark interface. The 'Packet Details' pane on the left shows the following structure:

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- Ethernet II, Src: AmbitMicrosy_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: AmbitMicrosy_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: AmbitMicrosy_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

The 'Packet Bytes' pane on the right shows the raw data in hexadecimal and ASCII:

```

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

```

Activate Windows
Go to Settings to activate Windows

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

Wireshark packet capture showing an ARP request. The packet list shows a broadcast ARP request from AmbitMicrosy_a9:3d:68 to LinksysGroup_da:af:73. The packet details pane shows the ARP request structure with fields for Hardware type, Protocol type, Hardware size, Protocol size, Opcode, and MAC addresses. The packet bytes pane shows the raw data of the ARP request.

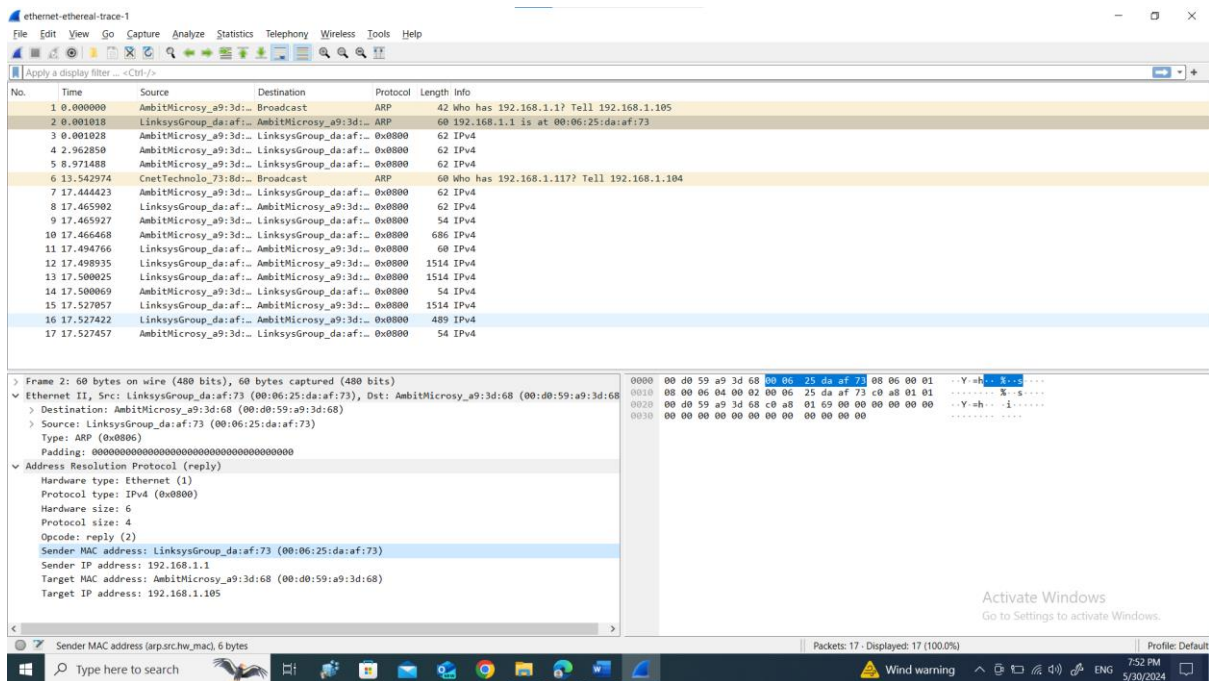
13. Now find the ARP reply that was sent in response to the ARP request. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Wireshark packet capture showing an ARP reply. The packet list shows a unicast ARP reply from LinksysGroup_da:af:73 to AmbitMicrosy_a9:3d:68. The packet details pane shows the ARP reply structure with fields for Hardware type, Protocol type, Hardware size, Protocol size, Opcode, and MAC addresses. The packet bytes pane shows the raw data of the ARP reply.

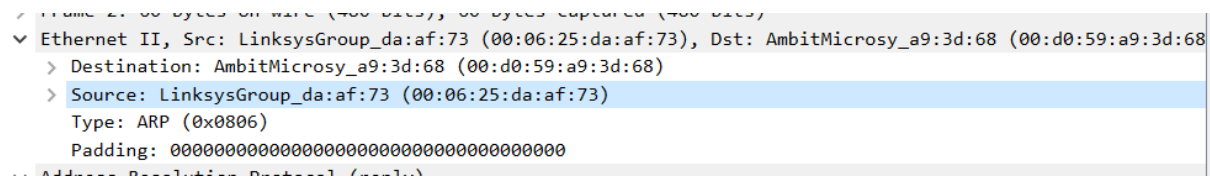
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Ans. 00 02

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?



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



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?

1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	62	IPv4
4	2.962850	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	62	IPv4
5	8.971488	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	62	IPv4
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	62	IPv4
8	17.465902	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	0x0800	62	IPv4
9	17.465927	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	54	IPv4
10	17.466468	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	686	IPv4
11	17.494766	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	0x0800	60	IPv4
12	17.498935	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	0x0800	1514	IPv4
13	17.500025	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	0x0800	1514	IPv4
14	17.500069	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	54	IPv4
15	17.527057	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	0x0800	1514	IPv4
16	17.527422	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	0x0800	489	IPv4
17	17.527457	AmbitMicrosy_a9:3d:...	LinksysGroup_da:af:...	0x0800	54	IPv4

Ans. The destination is broadcast so it dose not know who has the ip ithernet address.