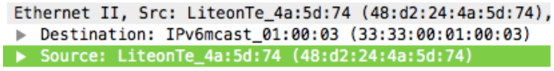
实验报告 Lab 7

姓名：王钦　学号：13349112

Capturing and analyzing Ethernet frames

1. My address: `84:38:35:68:46:ea`



```
Ethernet II, Src: LiteonTe_4a:5d:74 (48:d2:24:4a:5d:74),
▶ Destination: IPv6mcast_01:00:03 (33:33:00:01:00:03)
▶ Source: LiteonTe_4a:5d:74 (48:d2:24:4a:5d:74)
```

Figure 1: ethernet frame

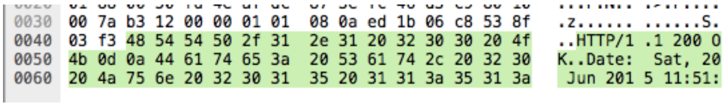
2. destination address: `b0:48:7a:41:45:46`,isn't the Ethernet address of gaia.cs.umass.edu. This is the address of my router, the link is used to depart off the subnet.

3. 0x0086

4. it's 52 bytes from the start.

5.

6. source address: `b0:48:7a:41:45:46`



```
0030  00 7a b3 12 00 00 01 01  08 0a ed 1b 06 c8 53 8f   .z...... ......S.
0040  03 f3 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ..HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 53 61 74 2c 20 32 30   K..Date:  Sat, 20
0060  20 4a 75 6e 20 32 30 31  35 20 31 31 3a 35 31 3a    Jun 201 5 11:51:
```

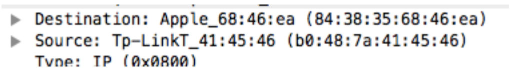
Figure 2: ethernet frame

   ,isn't the Ethernet address of gaia.cs.umass.edu. This is the address of my router, the link is used just get in my subnet.

7. destination address: `84:38:35:68:46:ea`,this is my address.

8. 0x0086

9. it's 52 bytes from the very start of the ethernet frame.



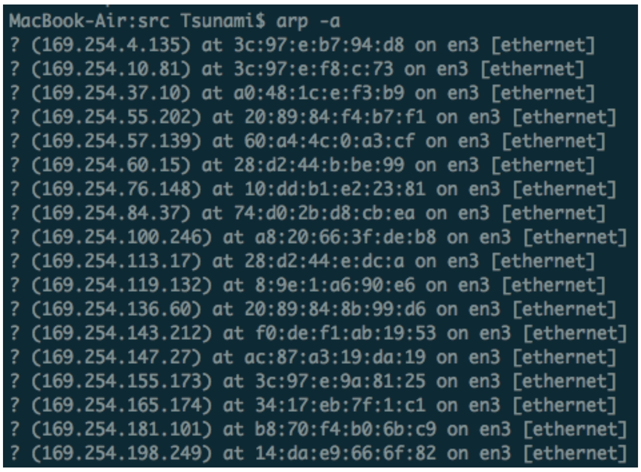
```
▶ Destination: Apple_68:46:ea (84:38:35:68:46:ea)
▶ Source: Tp-LinkT_41:45:46 (b0:48:7a:41:45:46)
  Type: IP (0x0800)
```

Figure 3: ethernet frame

10.

The Address Resolution Protocol

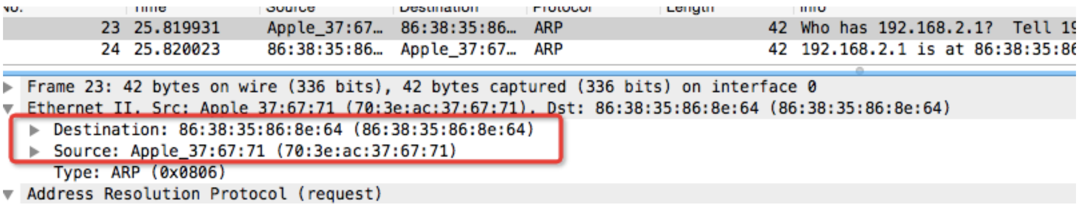
11. first column mean the IP address, the second column mean the MAC address, and the third column mean the adapter card.



```
MacBook-Air:src Tsunami$ arp -a
? (169.254.4.135) at 3c:97:e:b7:94:d8 on en3 [ethernet]
? (169.254.10.81) at 3c:97:e:f8:c:73 on en3 [ethernet]
? (169.254.37.10) at a0:48:1c:e:f3:b9 on en3 [ethernet]
? (169.254.55.202) at 20:89:84:f4:b7:f1 on en3 [ethernet]
? (169.254.57.139) at 60:a4:4c:0:a3:cf on en3 [ethernet]
? (169.254.60.15) at 28:d2:44:b:be:99 on en3 [ethernet]
? (169.254.76.148) at 10:dd:b1:e2:23:81 on en3 [ethernet]
? (169.254.84.37) at 74:d0:2b:d8:cb:ea on en3 [ethernet]
? (169.254.100.246) at a8:20:66:3f:de:b8 on en3 [ethernet]
? (169.254.113.17) at 28:d2:44:e:dc:a on en3 [ethernet]
? (169.254.119.132) at 8:9e:1:a6:90:e6 on en3 [ethernet]
? (169.254.136.60) at 20:89:84:8b:99:d6 on en3 [ethernet]
? (169.254.143.212) at f0:de:f1:ab:19:53 on en3 [ethernet]
? (169.254.147.27) at ac:87:a3:19:da:19 on en3 [ethernet]
? (169.254.155.173) at 3c:97:e:9a:81:25 on en3 [ethernet]
? (169.254.165.174) at 34:17:eb:7f:1:c1 on en3 [ethernet]
? (169.254.181.101) at b8:70:f4:b0:6b:c9 on en3 [ethernet]
? (169.254.198.249) at 14:da:e9:66:6f:82 on en3 [ethernet]
```

Figure 4: ARP Caching

12. source address: `70:3e:ac:37:67:71`,destination address: `86:38:35:86:8e:64`.



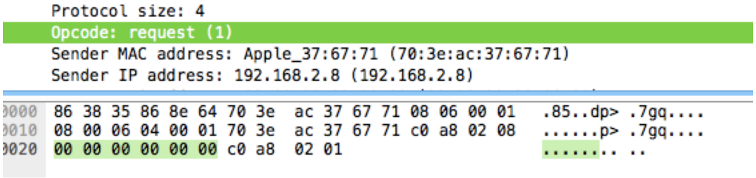
```
No.         Time          Source         Destination    Protocol   Length   Info
       23   25.819931     Apple_37:67…   86:38:35:86…   ARP                42   Who has 192.168.2.1?  Tell 19
       24   25.820023     86:38:35:86…   Apple_37:67…   ARP                42   192.168.2.1 is at 86:38:35:8

▶ Frame 23: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Apple_37:67:71 (70:3e:ac:37:67:71), Dst: 86:38:35:86:8e:64 (86:38:35:86:8e:64)
  ▶ Destination: 86:38:35:86:8e:64 (86:38:35:86:8e:64)
  ▶ Source: Apple_37:67:71 (70:3e:ac:37:67:71)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
```

Figure 5: ARP Caching

13. `0x0806`.

14. ARP request

a it's 20 bytes from the very beginning of the Ethernet frame

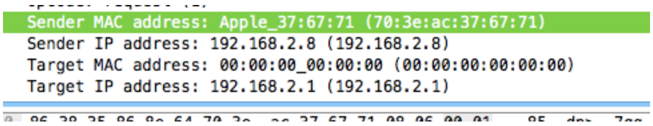


```
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Apple_37:67:71 (70:3e:ac:37:67:71)
    Sender IP address: 192.168.2.8 (192.168.2.8)

0000  86 38 35 86 8e 64 70 3e  ac 37 67 71 08 06 00 01   .85..dp> .7gq....
0010  08 00 06 04 00 01 70 3e  ac 37 67 71 c0 a8 02 08   ......p> .7gq....
0020  00 00 00 00 00 00 c0 a8  02 01                     ........ ..
```

Figure 6: ARP Caching

b the value of opcode field is 1

c Yes, it containg the IP address `192.168.2.8` which is sender.



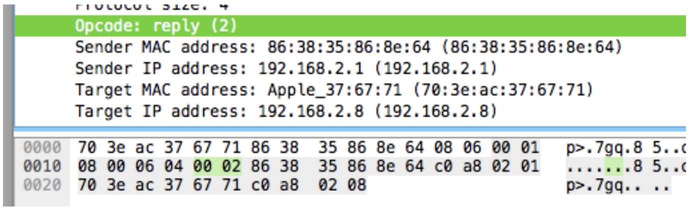
```
    Sender MAC address: Apple_37:67:71 (70:3e:ac:37:67:71)
    Sender IP address: 192.168.2.8 (192.168.2.8)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.2.1 (192.168.2.1)
```

Figure 7: ARP Caching

d The of of `Target MAC address` is `00:00:00:00:00:00` mean address `192.168.2.1` is queried.

15. ARP replay

a it's 20 bytes from the very beginning of the Ethernet frame

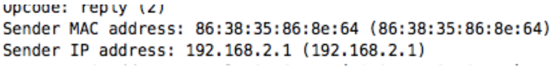


```
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 86:38:35:86:8e:64 (86:38:35:86:8e:64)
Sender IP address: 192.168.2.1 (192.168.2.1)
Target MAC address: Apple_37:67:71 (70:3e:ac:37:67:71)
Target IP address: 192.168.2.8 (192.168.2.8)

0000  70 3e ac 37 67 71 86 38  35 86 8e 64 08 06 00 01   p>.7gq.8 5..
0010  08 00 06 04 00 02 86 38  35 86 8e 64 c0 a8 02 01   .......8 5..
0020  70 3e ac 37 67 71 c0 a8  02 08                     p>.7gq.. ..
```

Figure 8: ARP Caching

b the value of opcode field is 2

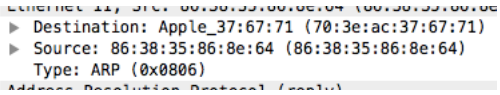
c The answer to the earlier ARP request appears in the `send MAC address`,the value `86:38:35:86:8e:64` is the MAC address of `192.168.2.1`



```
Opcode: reply (2)
Sender MAC address: 86:38:35:86:8e:64 (86:38:35:86:8e:64)
Sender IP address: 192.168.2.1 (192.168.2.1)
```

Figure 9: ARP Caching

16. source address: `86:38:35:86:8e:64`,destination address: `70:3e:ac:37:67:71`.



```
Ethernet II, Src: 86:38:35:86:8e:64 (86:38:35:86:8e
▶ Destination: Apple_37:67:71 (70:3e:ac:37:67:71)
▶ Source: 86:38:35:86:8e:64 (86:38:35:86:8e:64)
  Type: ARP (0x0806)
Address Resolution Protocol (reply)
```

Figure 10: ARP Caching

17. We can't receive this reply.Because ARP reply is sent back directly not broadcast.Only that send computer could receive the reply.