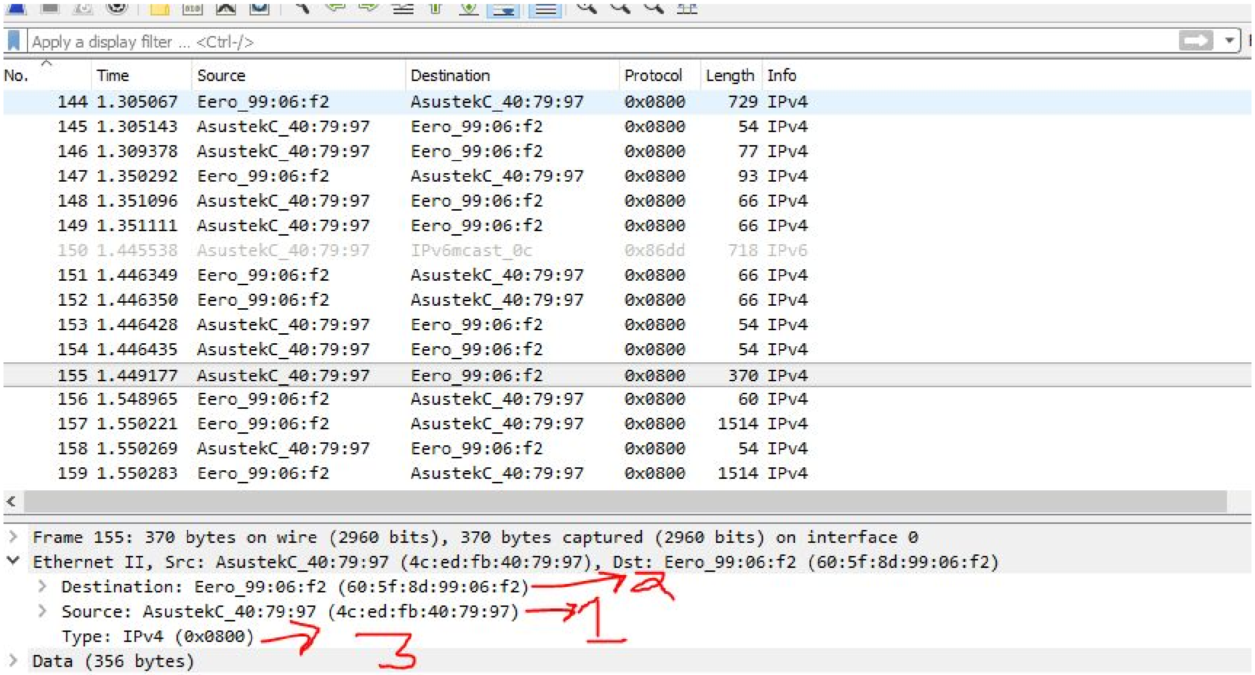
CS372 Lab 5
Hudson Dean

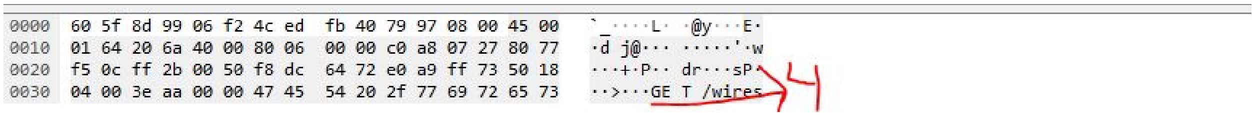
1. 4c:ed:fb:40:79:97
2. 60:5f:8d:99:06:f2
   - This is the ethernet address of the external router in the home network
3. 0x0800 is the IPv4 protocol type
4. 54 bytes into the frame



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

```
No.   Time      Source              Destination         Protocol  Length Info
  144 1.305067  Eero_99:06:f2       AsustekC_40:79:97   0x0800     729 IPv4
  145 1.305143  AsustekC_40:79:97   Eero_99:06:f2       0x0800      54 IPv4
  146 1.309378  AsustekC_40:79:97   Eero_99:06:f2       0x0800      77 IPv4
  147 1.350292  Eero_99:06:f2       AsustekC_40:79:97   0x0800      93 IPv4
  148 1.351096  AsustekC_40:79:97   Eero_99:06:f2       0x0800      66 IPv4
  149 1.351111  AsustekC_40:79:97   Eero_99:06:f2       0x0800      66 IPv4
  150 1.445538  AsustekC_40:79:97   IPv6mcast_0c        0x86dd     718 IPv6
  151 1.446349  Eero_99:06:f2       AsustekC_40:79:97   0x0800      66 IPv4
  152 1.446350  Eero_99:06:f2       AsustekC_40:79:97   0x0800      66 IPv4
  153 1.446428  AsustekC_40:79:97   Eero_99:06:f2       0x0800      54 IPv4
  154 1.446435  AsustekC_40:79:97   Eero_99:06:f2       0x0800      54 IPv4
  155 1.449177  AsustekC_40:79:97   Eero_99:06:f2       0x0800     370 IPv4
  156 1.548965  Eero_99:06:f2       AsustekC_40:79:97   0x0800      60 IPv4
  157 1.550221  Eero_99:06:f2       AsustekC_40:79:97   0x0800    1514 IPv4
  158 1.550269  AsustekC_40:79:97   Eero_99:06:f2       0x0800      54 IPv4
  159 1.550283  Eero_99:06:f2       AsustekC_40:79:97   0x0800    1514 IPv4
```

```
> Frame 155: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
v Ethernet II, Src: AsustekC_40:79:97 (4c:ed:fb:40:79:97), Dst: Eero_99:06:f2 (60:5f:8d:99:06:f2)
  > Destination: Eero_99:06:f2 (60:5f:8d:99:06:f2)
  > Source: AsustekC_40:79:97 (4c:ed:fb:40:79:97)
    Type: IPv4 (0x0800)
> Data (356 bytes)
```



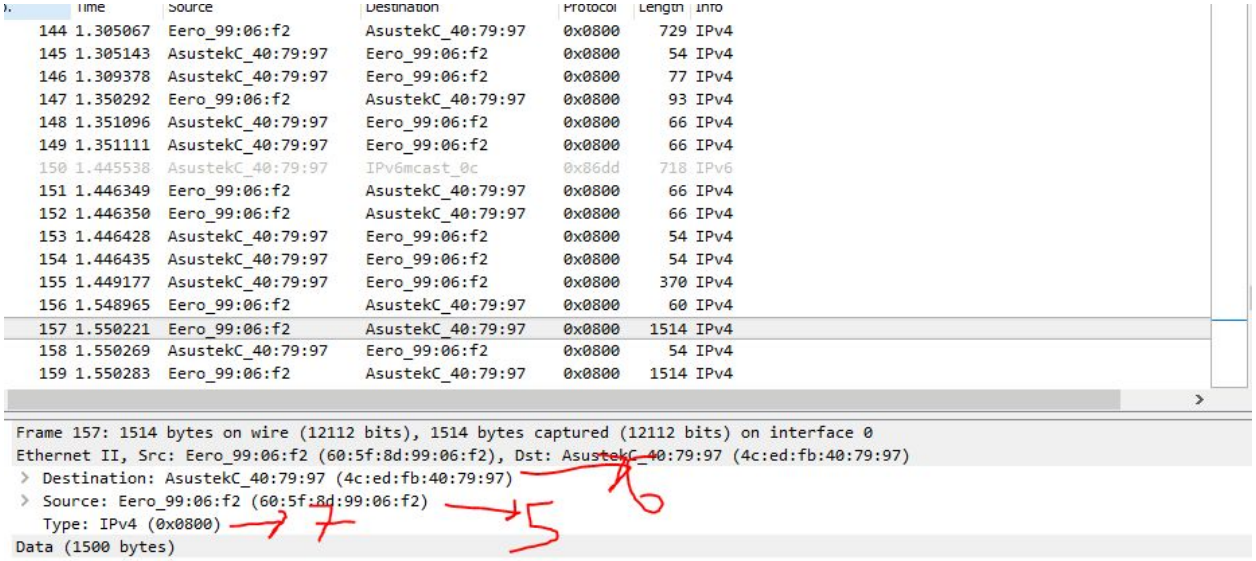
```
0000  60 5f 8d 99 06 f2 4c ed  fb 40 79 97 08 00 45 00   `_····L· ·@y···E·
0010  01 64 20 6a 40 00 80 06  00 00 c0 a8 07 27 80 77   ·d j@··· ·····'·w
0020  f5 0c ff 2b 00 50 f8 dc  64 72 e0 a9 ff 73 50 18   ···+·P·· dr···sP·
0030  04 00 3e aa 00 00 47 45  54 20 2f 77 69 72 65 73   ··>···GE T /wires
```

5. 60:5f:8d:99:06:f2
   - This is the ethernet address of the external router in the home network
6. 4c:ed:fb:40:79:97

- yes

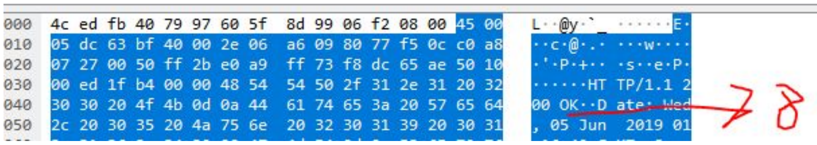
7. 0x0800 is the IPv4 protocol type

8. 67 bytes into the frame



```
).   Time      Source             Destination        Protocol  Length Info
 144 1.305067  Eero_99:06:f2      AsustekC_40:79:97  0x0800     729 IPv4
 145 1.305143  AsustekC_40:79:97  Eero_99:06:f2      0x0800      54 IPv4
 146 1.309378  AsustekC_40:79:97  Eero_99:06:f2      0x0800      77 IPv4
 147 1.350292  Eero_99:06:f2      AsustekC_40:79:97  0x0800      93 IPv4
 148 1.351096  AsustekC_40:79:97  Eero_99:06:f2      0x0800      66 IPv4
 149 1.351111  AsustekC_40:79:97  Eero_99:06:f2      0x0800      66 IPv4
 150 1.445538  AsustekC_40:79:97  IPv6mcast_0c       0x86dd     718 IPv6
 151 1.446349  Eero_99:06:f2      AsustekC_40:79:97  0x0800      66 IPv4
 152 1.446350  Eero_99:06:f2      AsustekC_40:79:97  0x0800      66 IPv4
 153 1.446428  AsustekC_40:79:97  Eero_99:06:f2      0x0800      54 IPv4
 154 1.446435  AsustekC_40:79:97  Eero_99:06:f2      0x0800      54 IPv4
 155 1.449177  AsustekC_40:79:97  Eero_99:06:f2      0x0800     370 IPv4
 156 1.548965  Eero_99:06:f2      AsustekC_40:79:97  0x0800      60 IPv4
 157 1.550221  Eero_99:06:f2      AsustekC_40:79:97  0x0800    1514 IPv4
 158 1.550269  AsustekC_40:79:97  Eero_99:06:f2      0x0800      54 IPv4
 159 1.550283  Eero_99:06:f2      AsustekC_40:79:97  0x0800    1514 IPv4

Frame 157: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Eero_99:06:f2 (60:5f:8d:99:06:f2), Dst: AsustekC_40:79:97 (4c:ed:fb:40:79:97)
 > Destination: AsustekC_40:79:97 (4c:ed:fb:40:79:97)
 > Source: Eero_99:06:f2 (60:5f:8d:99:06:f2)
   Type: IPv4 (0x0800)
Data (1500 bytes)
```



```
000  4c ed fb 40 79 97 60 5f  8d 99 06 f2 08 00 45 00   L··@y·`_ ······E·
010  05 dc 63 bf 40 00 2e 06  a6 09 80 77 f5 0c c0 a8   ··c·@·.· ···w····
020  07 27 00 50 ff 2b e0 a9  ff 73 f8 dc 65 ae 50 10   ·'·P·+·· ·s··e·P·
030  00 ed 1f b4 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
050  2c 20 30 35 20 4a 75 6e  20 32 30 31 39 20 30 31   , 05 Jun  2019 01
```

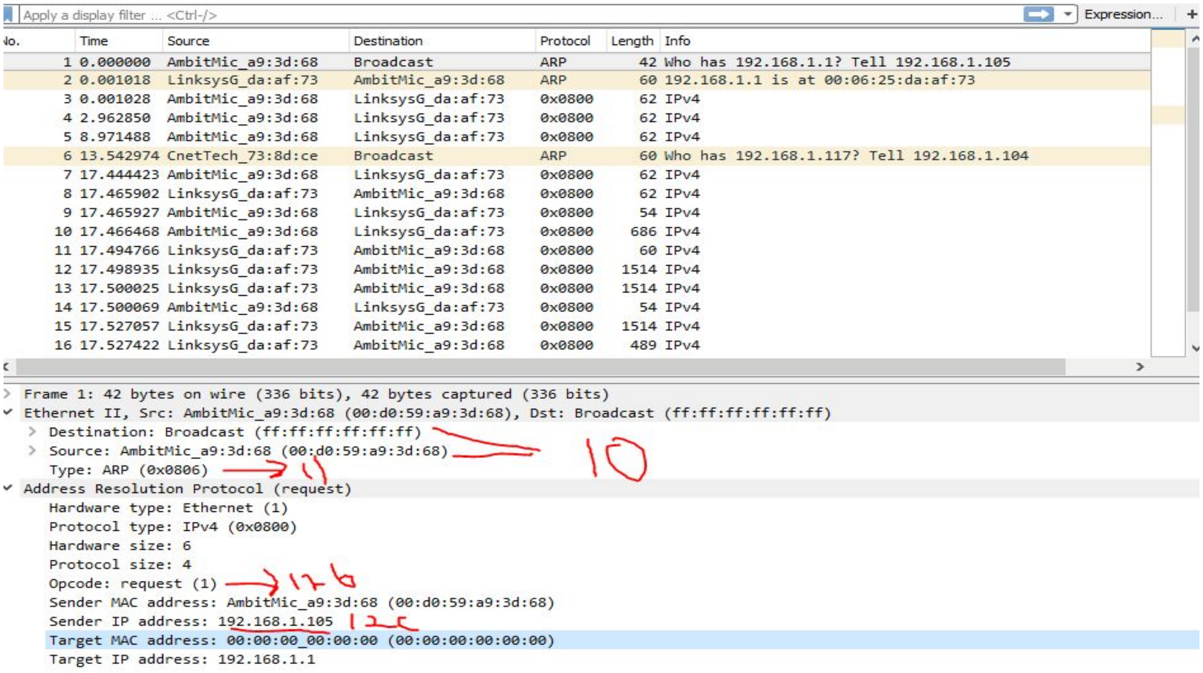
9. The internet Address is the IP address associated with a machine. Physical Address is the MAC address of a given machine. Type means that the ARP entry is given by the ARP or ARP entry is manually set. Arp cache is listed below:

```
Interface: 192.168.7.39 --- 0xb
  Internet Address      Physical Address      Type
  192.168.7.1           60-5f-8d-99-06-f2     dynamic
  192.168.7.27          38-f7-3d-42-66-4a     dynamic
  192.168.7.28          30-59-b7-62-e6-54     dynamic
  192.168.7.31          00-1e-8f-1d-a4-1f     dynamic
  192.168.7.42          40-99-22-6f-97-bd     dynamic
  192.168.7.47          64-00-6a-63-dd-62     dynamic
```

192.168.7.69	cc-e1-d5-a6-16-bd	dynamic
192.168.7.255	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

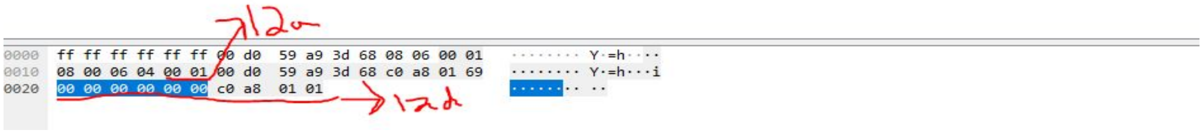
****FROM THIS SECTION FORWARD ethernet-ethereal-trace-1 file was used!**

10. SOURCE: 00:0d:59:a9:3d:68
    DESTINATION: ff:ff:ff:ff:ff:ff
11. 0x0806 is the ARP protocol type
12.
    a) 20 bytes from the beginning
    b) request (1) 0x0001
    c) yes 192.168.1.105
    d) byte #33 - 42 From Target MAC address and Target IP address fields



```
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 CnetTech_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
  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

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



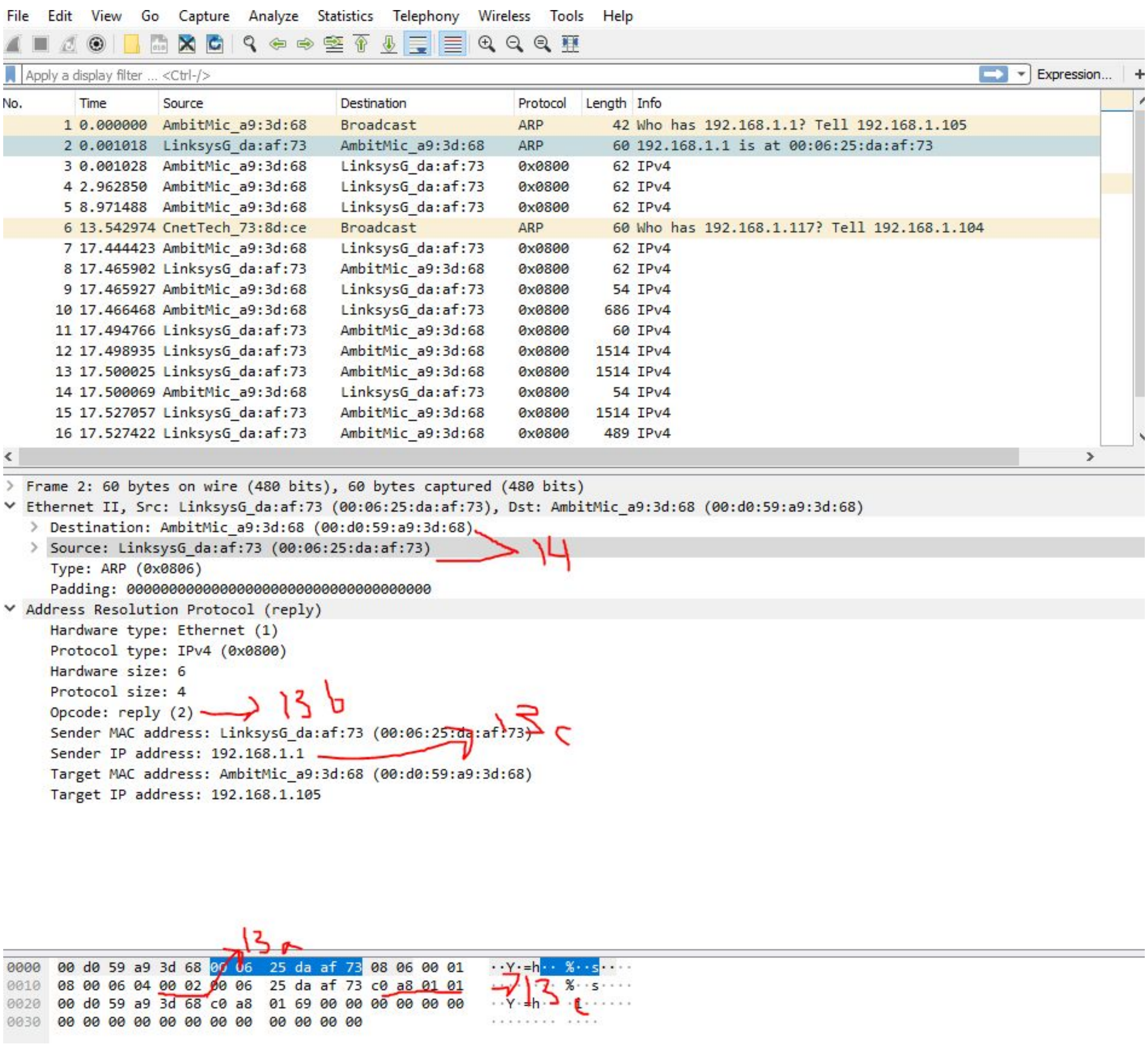
```
0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

13.

a) 20 bytes from the beginning
b) reply (2) 0x0002
c) 7 Bytes after the opcode (byte #29). The Sender IP address field answers the question. The 6 bytes after the opcode is used for the Ethernet address of the queried machine

14. SOURCE: 00:06:25:da:af:73
DESTINATION: 00:0d:59:a9:3d:68

15. Because the ARP request is broadcast, but the ARP reply is not broadcast. The reply will be sent to the computer who made the request directly and not to this machine



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	CnetTech_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
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

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v 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: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v 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               ········ ····
```

Extra Credit:

1. The called interface would be disables and all outbound requests go nowhere/never be received.

2. On windows there is no default time only Reachable Time somewhere between 15 - 45 seconds (source: https://support.microsoft.com/en-us/help/949589/description-of-address-resolution-protocol-arp-caching-behavior-in-win)

   on UNIX: Default time = 60 seconds. The command: cat /proc/sys/net/ipv4/neigh/default/gc_stale_time will tell the default time