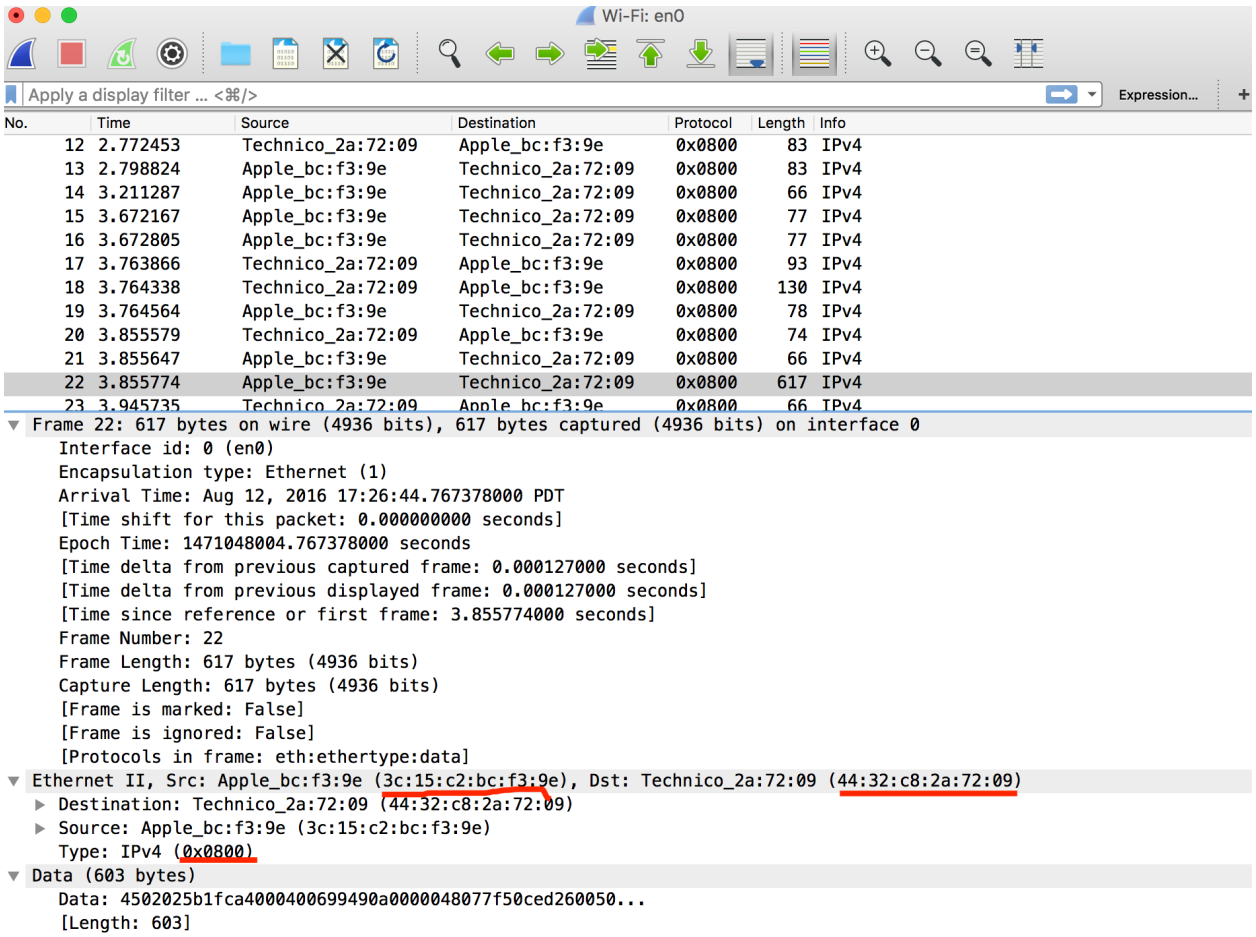
Colleen Minor
Lab 4
Introduction to Networking, Oregon State University
Summer 2016

This image is for questions 1-3:



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

3c:15:c2:bc:f3:9e

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 is 44:32:c8:2a:72:09. As the question says, no, it is not address of gaia.cs.umass.edu, it is the address of the my computer, it is the address of my router.

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

0x0800, and this corresponds to IPv4 protocol.

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

G is 71 in ASCII, I went show the G is shown at position 3 on the byte 40 line, making it the 43rd byte, and the number there is 47, which is hex for 71. So the answer is **43**.

```
0000  44 32 c8 2a 72 09 3c 15  c2 bc f3 9e 08 00 45 02   D2.*r.<. ......E.
0010  02 5b 1f ca 40 00 40 06  99 49 0a 00 00 04 80 77   .[..@.@. .I.....w
0020  f5 0c ed 26 00 50 da 97  f4 d9 66 04 4f 4a 80 18   ...&.P.. ..f.OJ..
0030  10 15 39 55 00 00 01 01  08 0a 3a 72 1a ee 01 85   ..9U.... ..:r....
0040  d8 4a 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   .JGET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 65 74 68 65 72   -labs/HT TP-ether
0060  65 61 6c 2d 6c 61 62 2d  66 69 6c 65 33 2e 68 74   eal-lab- file3.ht
0070  6d 6c 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   ml HTTP/ 1.1..Hos
0080  74 3a 20 67 61 69 61 2e  63 73 2e 75 6d 61 73 73   t: gaia. cs.umass
0090  2e 65 64 75 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .edu..Co nnection
00a0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live..Ca
00b0  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
00c0  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0.. Upgrade-
00d0  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
00e0  73 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   s: 1..Us er-Agent
00f0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 4d   : Mozill a/5.0 (M
0100  61 63 69 6e 74 6f 73 68  3b 20 49 6e 74 65 6c 20   acintosh ; Intel
0110  4d 61 63 20 4f 53 20 58  20 31 30 5f 31 31 5f 36   Mac OS X  10_11_6
```

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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?

The source address is 44:32:c8:2a:72:09. The device that has this ethernet address is my router.

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

The destination address is 3c:15:c2:bc:f3:9e, yes that is the address of my computer.

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

That is also 0x0800, IPv4.

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?

At first mine said not modified instead of OK, I guess because I had just refreshed the page for my capture, so then I cleared my history and tried it again, and this time the HTTP OK response didn't say ok in the body at all (even though it's labeled HTTP/1.1 200 OK under info when I turn the IP protocols back on), instead it went straight to the bill of rights, so null answer.

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

```
? (10.0.0.1) at 44:32:c8:2a:72:9 on en0 ifscope [ethernet]
? (10.0.0.3) at 4:4b:ed:22:4a:6d on en0 ifscope [ethernet]
? (10.0.0.4) at 3c:15:c2:bc:f3:9e on en0 ifscope permanent [ethernet]
? (10.0.0.5) at 44:d2:44:78:f9:b5 on en0 ifscope [ethernet]
? (10.0.0.255) at (incomplete) on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
broadcasthost (255.255.255.255) at (incomplete) on en0 ifscope
[ethernet]
```

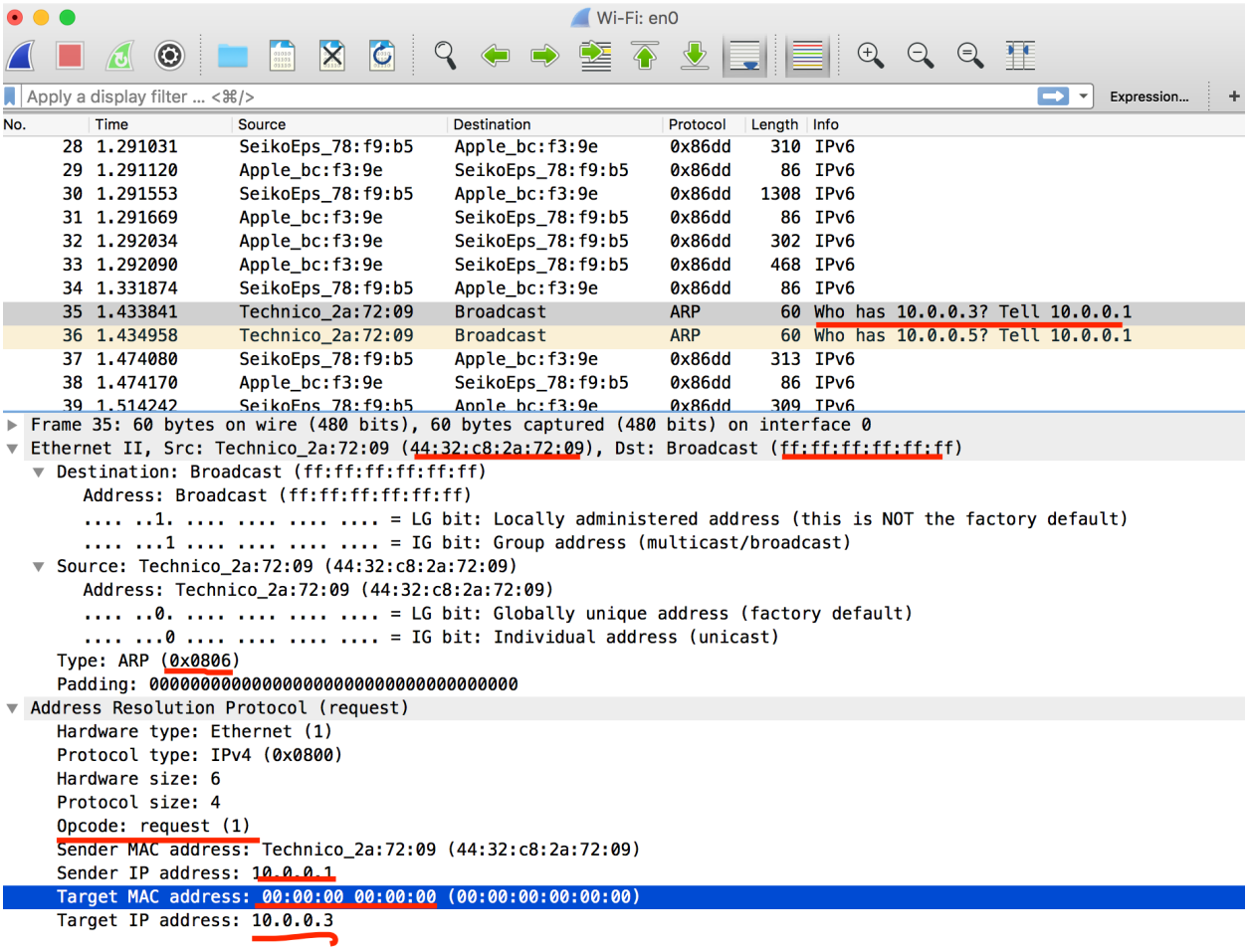
The table matches MAC addresses to IP addresses.

The first column is the internet (IP) address, the addresses after "at" are the physical (MAC) addresses, the "en0" after "on" is referring to the bsd name for the ports, and en0 means it's probably ethernet, and the last column that says ethernet for all of them means that they are all indeed ethernet.

For the last one, broadcasthost means 255.255.255.255 is a broadcast address.

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

The source address is 44:32:c8:2a:72:09 and the destination address is the broadcast address ff:ff:ff:ff:ff:ff. This next image is for questions 10-12:



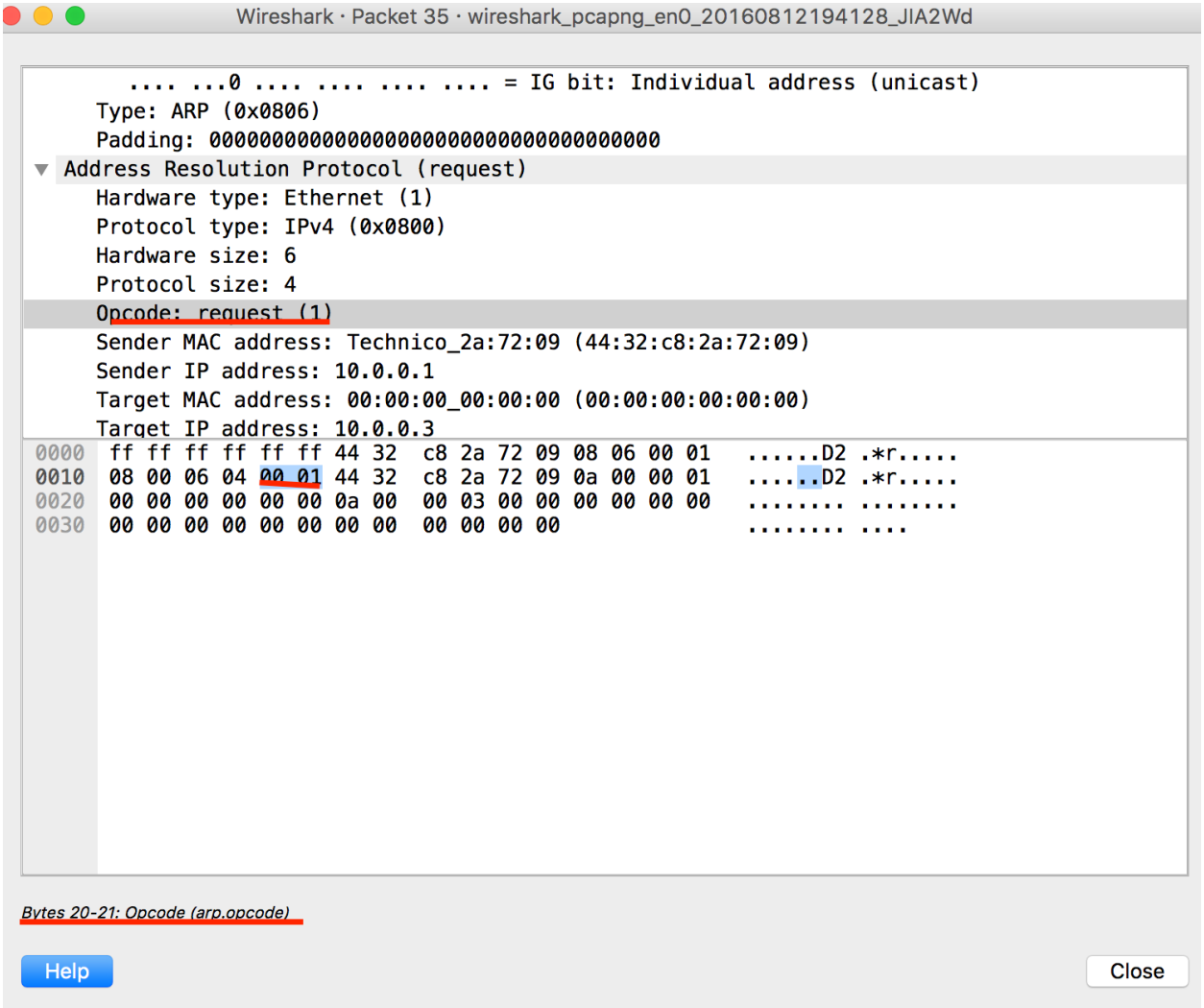
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

0x0806, which corresponds to ARP.

12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txthttp://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html. A readable, detailed discussion of ARP is also at .

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

20 bytes. The first 14 bytes are for the Ethernet frame header and the next 6 are for other ARP fields.



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?

1 for request.

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

Yes, the sender address is 10.0.0.1.

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

The Target MAC address is set to 00:00:00:00:00:00 so that the target IP address, 10.0.0.3 will be questioned.

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?

Mine doesn't have any ARP replies, only requests, but it would also be 20 bytes.

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?

That would be 2 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?

That would be in the "Sender MAC address" field.

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

Well I don't have any ARP reply messages, but the destination address would be 44:32:c8:2a:72:09, which was the source of the request, my router. The source should be the MAC address of 10.0.0.3… I ran arp -a again to see and it says '(10.0.0.3) at (incomplete) on en0 ifscope [ethernet]' whereas last time (before I cleared the ARP cache) there was an address of 4:4b:ed:22:4a:6d there. I decided to charge my iPhone, then I looked in settings—>about and saw that that was the device with a MAC address of 4:4b:ed:22:4a:6d.

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?

There is no ARP reply because the machine running wireshark was not the machine that sent the request, so it sent the reply straight back to the machine that sent the request.

EX-1. The *arp* command: [*arp -s InetAddr EtherAddr*] allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

It will start learning again by sending out more requests. I changed a bunch of them on mine and there were different results depending on the device.

When I changed my the mac address for my iPhone to the IP address for another device I have, I started seeing

Gratuitous ARP for 10.0.0.5 (Request)

and something about ‘locally administered address (that is NOT the factory default)’.

When I try changing the MAC address for the IP address my computer is set to it says, ‘set: can only proxy for 10.0.0.4’, but the values don’t change.

Eventually I decided to try

```
sudo arp -d || sudo arp -s 10.0.0.4 29:da:9b:13:d8:21
```

to clear and change mine at the same time, and nothing seemed to happen except the next time I checked the table with
arp -a, it had a list of the first 5 IPs like it had before, and then it had incomplete for the numbers 10.0.0.6 all the way to 10.0.0.255 as ‘incomplete.’

I checked wireshark and there were ARP requests for the address of 10.0.0.01-10.0.0.255, and all of the ones that didn’t really have a device that matched them were from my computer, 10.0.0.4, but the MAC address value for my computer was still the same.