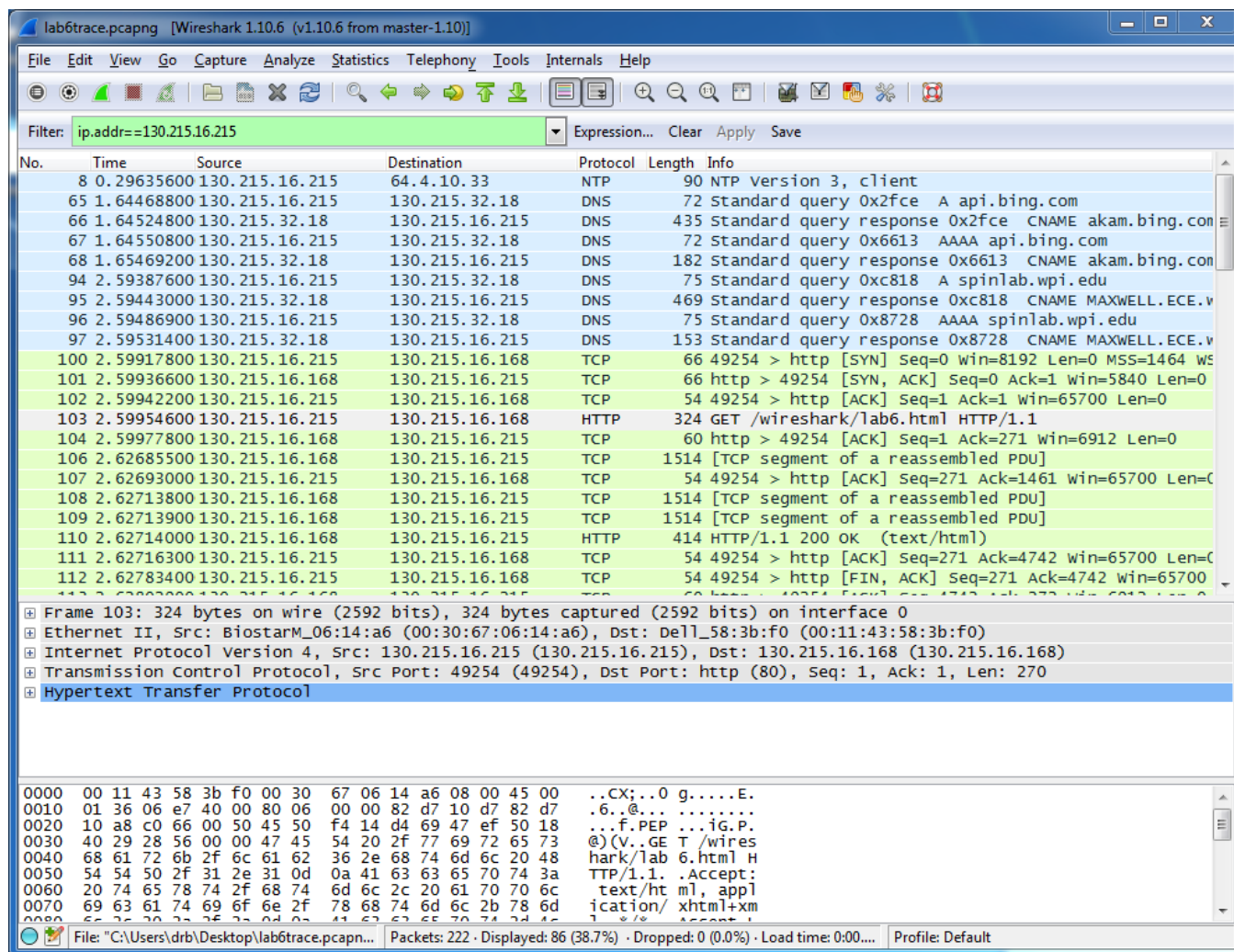
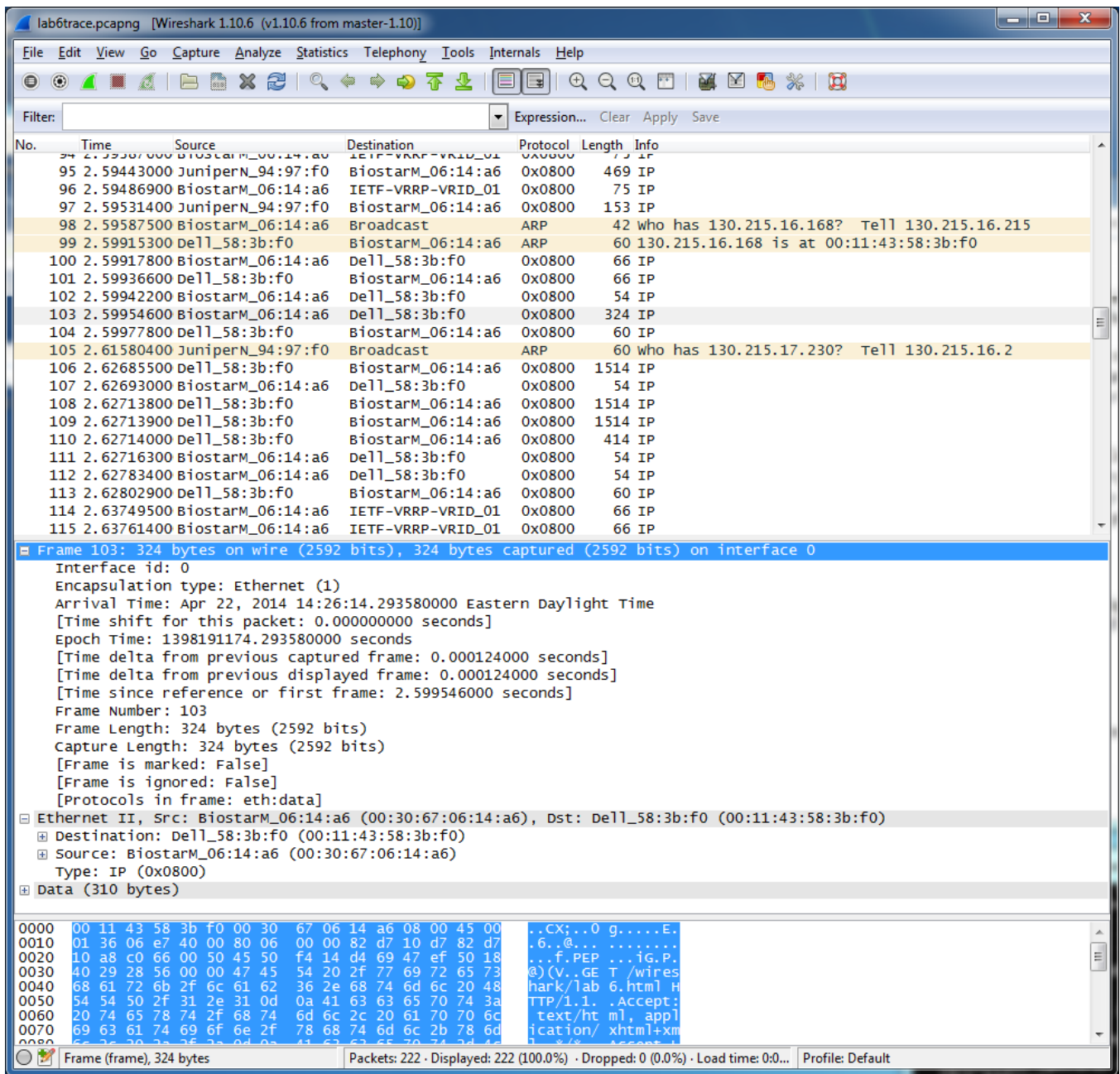


In my test, the HTTP GET request is at packet 103 (the easiest way to see this is by filtering by ip.addr==xxx.xxx.xxx.xxx). See the screenshot below. The HTTP response message is at packet 106.



Then I cleared the ip.addr filter, disabled IPv4 and got the screenshot below.



1. What is the 48-bit Ethernet address of your computer?
00:30:67:06:14:A6 (see previous screenshot)
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of spinlab.wpi.edu? What device has this as its Ethernet address?
From the previous screenshot, we see the 48-bit destination address is 00:11:43:58:3B:F0. This is not the Ethernet address of spinlab.wpi.edu. Rather, it is the Ethernet address of the router to which my computer is connected.
3. What is the hexadecimal value for the two-byte Frame type field? This field is also sometimes called the EtherType, and specifies what higher layer protocol is contained within this Ethernet frame. Using the table in the Wikipedia article on “EtherType” (or, just using the

middle window on Wireshark), what is the higher layer protocol that is encapsulated in this Ethernet frame?

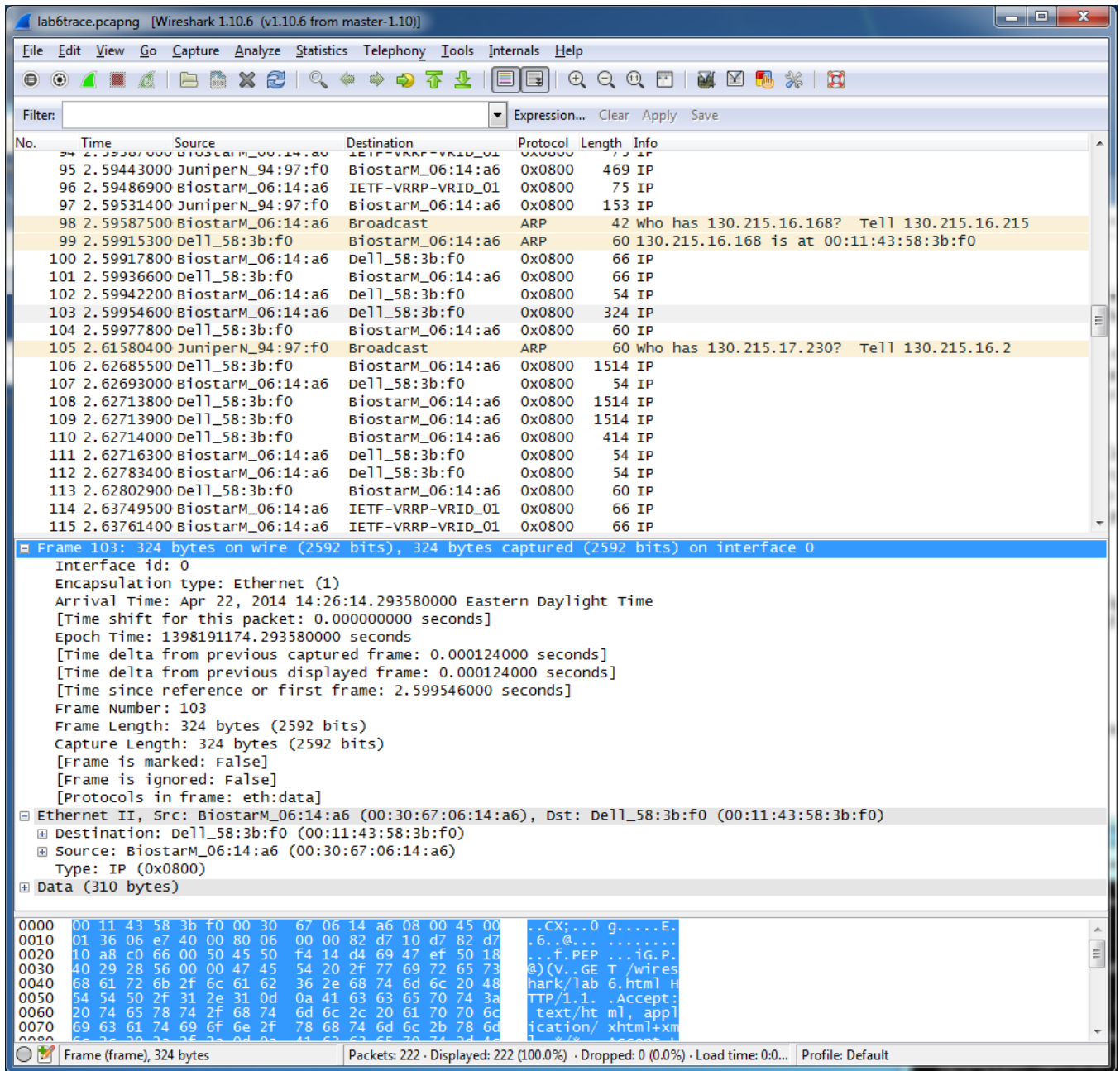
From the previous screenshot we see the frame type is 0x0800. From the Wikipedia article, we see that the higher layer protocol that is encapsulated in this Ethernet frame is IPv4.

4. There should be between 54 to 66 bytes from the very start of the Ethernet frame to the ASCII “G” in the http “GET”. How many bytes are there, and what three things do you think these bytes contain? Hint: Think of which layers are below http.

As seen in the screenshot below, there are exactly 54 bytes prior to the ASCII “G” for the GET request. These bytes represent:

- The ethernet frame (first 14 bytes containing destination address, source address, and frame type)
 - The IP header (20 bytes)
 - The TCP header (20 bytes)
5. What is the value of the Ethernet source address? Is this the address of your computer, or of `spinlab.wpi.edu`? What device has this as its Ethernet address?

As shown in the screenshot below, the ethernet source address is 00:11:43:58:3B:F0. This is not the Ethernet address of `spinlab.wpi.edu`. Rather, it is the Ethernet address of the router to which my computer is connected.



- What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
From the previous screenshot, we see the 48-bit destination address is 00:11:43:58:3B:F0. This is not the Ethernet address of spinlab.wpi.edu. Rather, it is the Ethernet address of the router to which my computer is connected.
- What is the hexadecimal value for the two-byte Frame type field?
Same as before: 0x0800 corresponding to an IPv4 frame.
- 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?
There are 67 bytes before the “O” (or “O” appears as the 68th byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text.

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

The ARP cache for my computer is shown below.

```
C:\Users\drb>arp -a
```

```
Interface: 130.215.16.215 — 0xb
Internet Address      Physical Address      Type
130.215.16.1         00-00-5e-00-01-01    dynamic
130.215.16.68        00-23-ae-8c-80-61    dynamic
130.215.16.79        18-03-73-c5-e5-16    dynamic
130.215.16.109       b8-ca-3a-95-43-ce     dynamic
130.215.16.119       84-2b-2b-b5-33-be     dynamic
130.215.16.140       84-2b-2b-b5-33-f8     dynamic
130.215.16.141       b8-ca-3a-95-62-23     dynamic
130.215.16.155       b8-ca-3a-95-3a-50     dynamic
130.215.16.158       b8-ca-3a-95-38-e6     dynamic
130.215.16.168       00-11-43-58-3b-f0     dynamic
130.215.16.171       b8-ca-3a-95-43-12     dynamic
130.215.16.176       84-2b-2b-b5-1d-12     dynamic
130.215.16.186       b8-ca-3a-95-37-22     dynamic
130.215.16.206       b8-ca-3a-95-64-27     dynamic
130.215.16.222       b8-ca-3a-95-44-68     dynamic
130.215.16.230       b8-ca-3a-95-af-28     dynamic
130.215.16.233       b8-ac-6f-a6-db-28     dynamic
130.215.16.235       b8-ca-3a-95-ad-7c     dynamic
130.215.17.12        00-1b-a9-23-90-20     dynamic
130.215.17.16        b8-ca-3a-95-ac-ba     dynamic
130.215.17.39        84-2b-2b-b5-33-88     dynamic
130.215.17.40        84-2b-2b-b5-33-e8     dynamic
130.215.17.52        78-2b-cb-ad-66-41     dynamic
130.215.17.67        00-13-72-28-00-af     dynamic
130.215.17.88        78-2b-cb-ad-74-10     dynamic
130.215.17.103       5c-f9-dd-70-8e-e5     dynamic
130.215.17.141       00-0f-1f-87-20-7e     dynamic
130.215.17.142       00-09-3d-14-3b-0a     dynamic
130.215.17.179       b8-ca-3a-76-ee-37     dynamic
130.215.17.193       00-1a-a0-ab-41-5a     dynamic
130.215.17.209       d4-be-d9-56-4f-bf     dynamic
130.215.17.234       18-03-73-32-34-64     dynamic
130.215.17.249       90-b1-1c-67-48-6e     dynamic
130.215.18.66        00-1a-a0-ab-3d-51     dynamic
130.215.23.23        5c-26-0a-1f-41-b8     dynamic
130.215.23.36        68-b5-99-e2-35-10     dynamic
130.215.23.38        b8-88-e3-15-28-72     dynamic
130.215.23.48        d4-3d-7e-55-3c-96     dynamic
130.215.23.49        20-89-84-95-a4-dd     dynamic
```

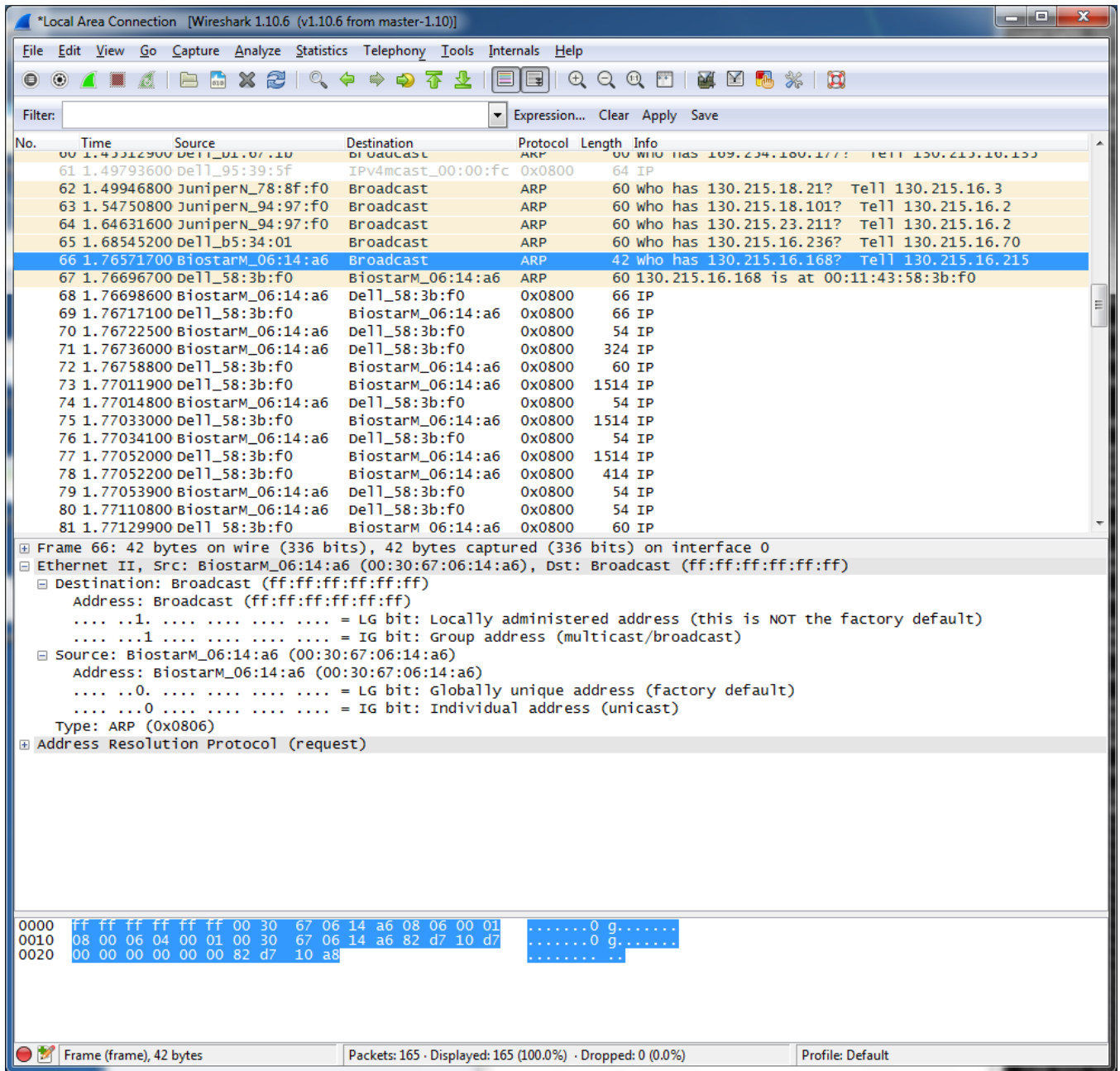
130.215.23.51	f4-6d-04-c2-0a-84	dynamic
130.215.23.54	28-d2-44-39-25-76	dynamic
130.215.23.61	ec-e0-9b-b1-1c-be	dynamic
130.215.23.69	3c-97-0e-72-7c-3c	dynamic
130.215.23.74	a0-b3-cc-47-85-03	dynamic
130.215.23.81	1c-c1-de-af-3c-f2	dynamic
130.215.23.83	28-d2-44-23-16-66	dynamic
130.215.23.87	f0-de-f1-70-2d-72	dynamic
130.215.23.97	60-a4-4c-d9-f8-09	dynamic
130.215.23.105	74-d0-2b-46-7f-34	dynamic
130.215.23.114	5c-ff-35-07-ca-45	dynamic
130.215.23.124	a0-48-1c-c3-f1-db	dynamic
130.215.23.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	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\drb>

The columns show the internet address (IPv4) and the physical address (Ethernet). The last column shows whether the IPv4 address is dynamic or static.

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

See screenshot below. The source address is 00:30:67:06:14:A6 and the destination address is FF:FF:FF:FF:FF:FF. The source address is the Ethernet address of my computer and the destination address is broadcast.

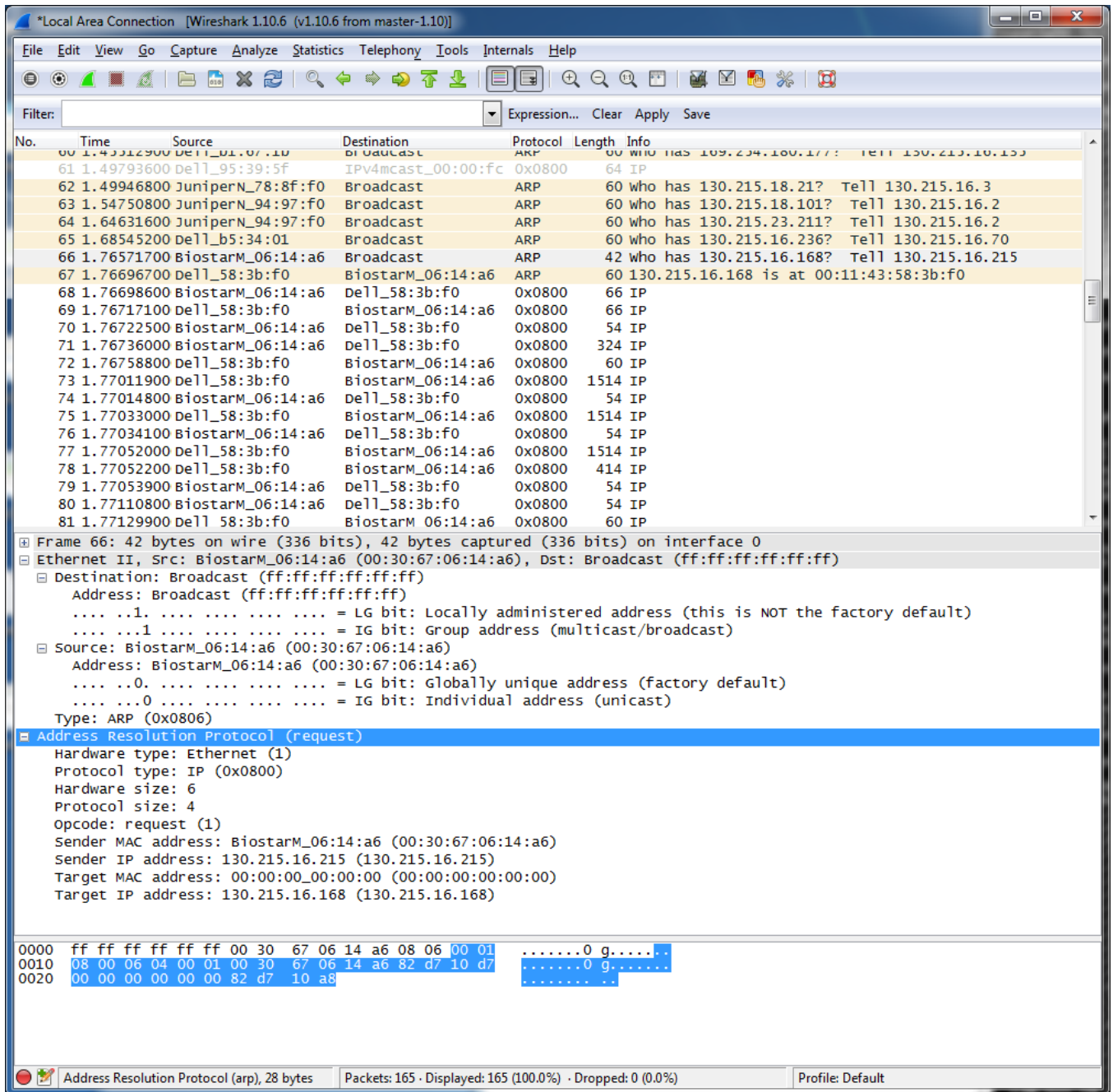


11. What is the hexadecimal value for the two-byte Ethernet Frame type field. Again, you may want to consult the Wikipedia article on EtherType.

The type value is 0x0806 which corresponds to ARP (as seen in the previous screenshot).

12. As you can see from the ARP header format in the Wikipedia article, the ARP opcode field begins 6 bytes (48 bits) from the beginning of the ARP frame. Since the Ethernet frame (consisting of 6-byte source and 6-byte destination MAC addresses, as well as 2-byte Frame type) is 14 bytes long, the opcode appears 20 bytes from the start of the packet. What is the value of the opcode field within the ARP payload, and what does it mean?

From the screenshot below, we see the opcode is 01. This corresponds to a “request”.



13. Does the ARP message contain the IP address of the sender?

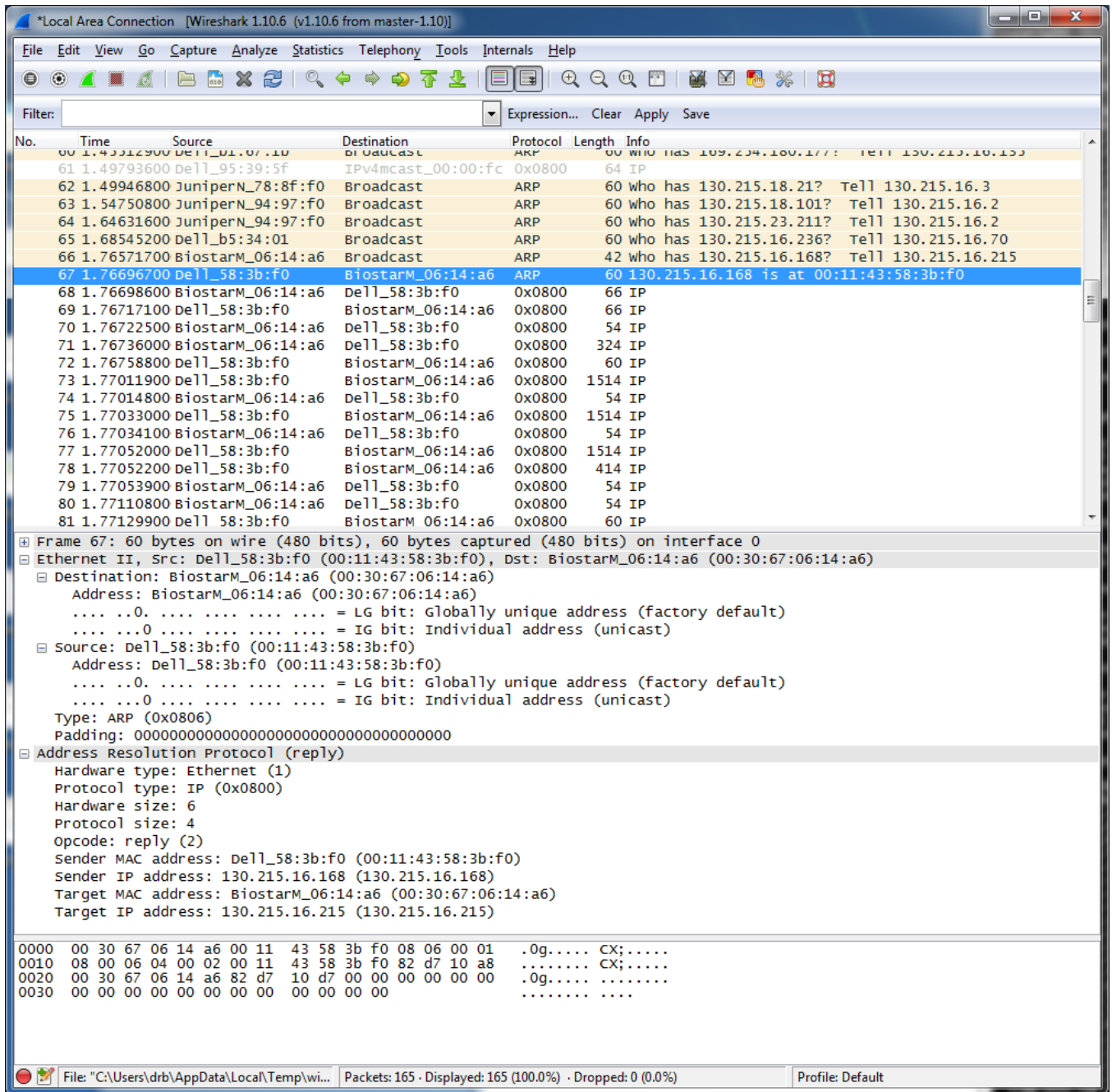
Yes (as seen in the previous screenshot).

14. Where in the ARP request does the “question” appear, i.e. the Ethernet address of the machine whose corresponding IP address is being queried?

In the “target IP address” (see previous screenshot).

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

From the screenshot below, we see the opcode is 02. This corresponds to a “reply”.



16. 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?

In the sender MAC address (see previous screenshot).

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

Source: 00:11:43:58:3B:F0. Destination: 00:30:67:06:14:A6 (see previous screenshot).