In answering the questions below[1], you can use either your own live trace, or use the Wireshark captured packet file *Ethernet-wireshark-trace1* in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip .

---

[1] For the author's class, when answering the following questions with hand-in assignments, students sometimes need to print out specific packets (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the packet they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are also learning management system (LMS) modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

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

- Source address = e0:be:03:3f:cd:79

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 483-484 in the text and make sure you understand the answer here.]

- Destination address = 1c:61:b4:47:3f:f0
- Router Address

3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?

- Type = 0x0800
- Ipv4

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

- 54 bytes

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?

- Source address = 1c:61:b4:47:3f:f0
- Router address

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

- Destination address = e0:be:03:3f:cd:79
- Yes , it is.

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

- Type = 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? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

- 54 bytes + 13 bytes before OK = 67 bytes

9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP "OK 200 ..." reply message?

- 4 frames which contains #356(1412), #358(1412), #360(1412), #361(625)

10. How many entries are stored in your ARP cache?

- 25 entries
- Interface: 192.168.72.162 --- 0xa

Internet Address	Physical Address	Type
192.168.72.113	e0-be-03-3f-b6-f6	dynamic
192.168.72.116	e0-be-03-3f-ca-77	dynamic
192.168.72.122	e0-be-03-3f-b7-9f	dynamic
192.168.72.123	e0-be-03-3f-b7-a0	dynamic
192.168.72.125	e0-be-03-3f-ce-53	dynamic
192.168.72.126	e0-be-03-3f-b7-a1	dynamic

192.168.72.144	e0-be-03-3f-ca-96	dynamic
192.168.72.160	e0-be-03-3f-cd-76	dynamic
192.168.72.164	e0-be-03-3f-cd-7a	dynamic
192.168.72.166	e0-be-03-3f-b7-c8	dynamic
192.168.72.198	e0-be-03-3f-ce-07	dynamic
192.168.72.200	e0-be-03-3f-b8-bb	dynamic
192.168.72.228	e0-be-03-3f-d0-59	dynamic
192.168.72.238	e0-be-03-3f-cd-5f	dynamic
192.168.72.241	e0-be-03-3f-cd-f9	dynamic
192.168.72.244	e0-be-03-3f-cd-67	dynamic
192.168.72.254	1c-61-b4-47-3f-f0	dynamic
192.168.72.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	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
239.255.102.18	01-00-5e-7f-66-12	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

11. What is contained in each displayed entry of the ARP cache?

- Internet Address
- Physical Address
- Type