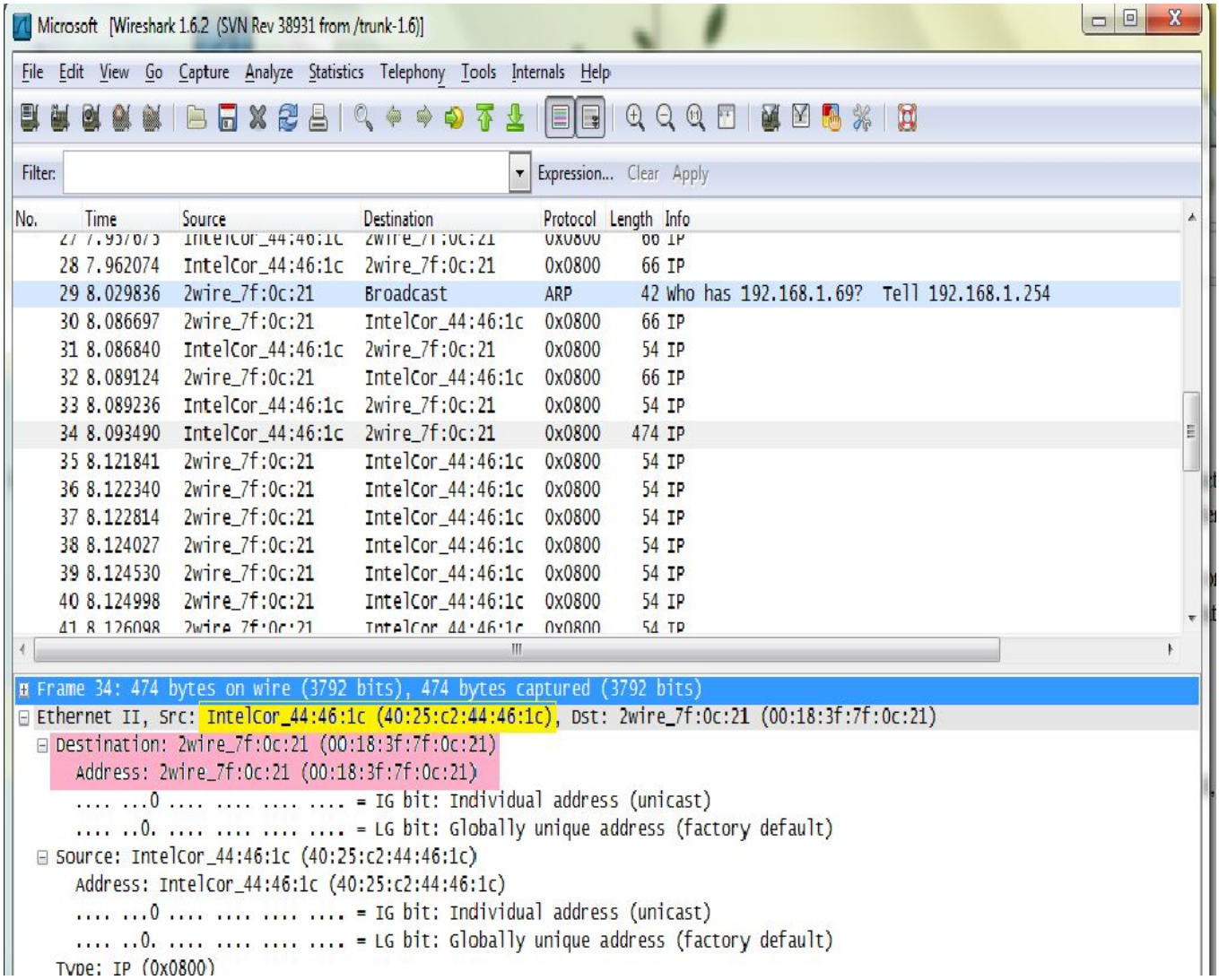
Paul Williams Diaz
CIS 151 Prof. Brown

Wireshark Lab Ethernet
GET Request - Ethernet Information



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

Answer: The 48-bit Ethernet address of my computer is...

`Intelcor_44:16:1c (40:25:c2:44:46:1c)`

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 get it wrong. Reread pages 468-469 in the text to make sure you understand the answer here.]

   Answer: The 48-bit destination address in the Ethernet frame is...
   `Destination: 2wire_7f:0c:21 (00:18:3f:7f:0c:21`
   `Address: 2wire_7f:)c:21 (00:18:3f:7f:0c:21.`
   No, this Ethernet address is the address of my router not gaia.cs.umass.edu.

3. Give the hexadecimal value for the two-byte Frame type field. Whats do the bit(s) whose value is 1 mean without the flag field?

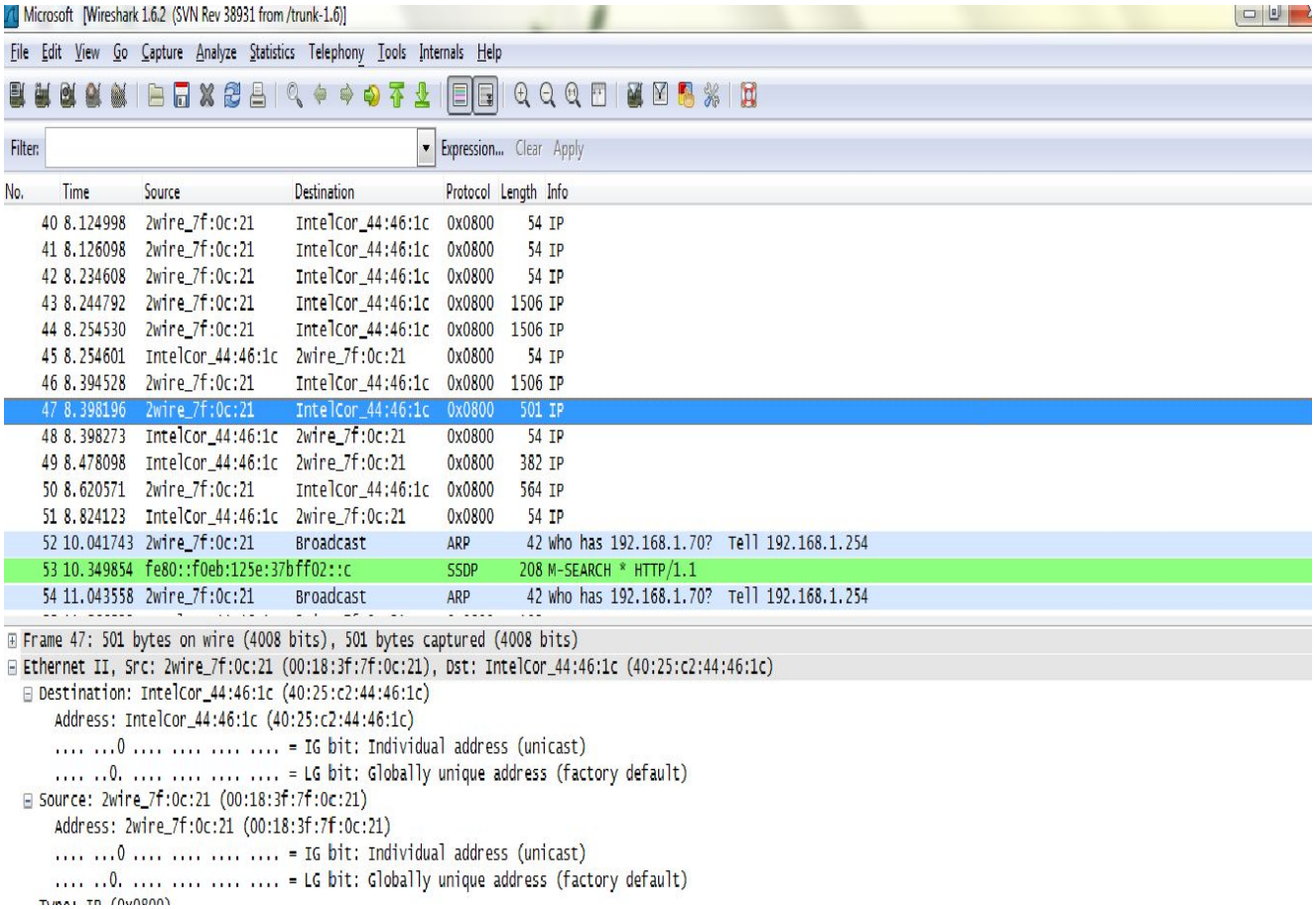
   Answer: The hexadecimal value for the tow-byte Frame type field is `0x0800`.

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

   Answer: From the start, there 474 bytes of ASCII “G” in GET appeared.

5. What is the hexadecimal value of the CRC field in this Ethernet frame?

   Answer: The is no hexadecimal value of the CRC field shown in this Ethernet frame.



OK Response OK Information

6. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu? (Hints: the answer is *no*) Whats device has this as its Ethernet address?

Answer: The value of the Ethernet source address is...

`2wire_7f:0c:21 (00:18:3f:7f:0c:21).`

This is not the address of my computer nor gaia.cs.umass.edu, but this is the address of my router.

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

Answer: The destination address seen in the Ethernet frame is...

```
Destination : Intelcor_44:46:1c (40:25:c2:44:46;1c)
    Address: Intelcor_44:46:1c (40:25:c2:44:46:1c)
```

Yes, it is the address of my computer,

8. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean without the flag field?

   Answer: The hexadecimal value for the 2 byte Frame type is `0x0800`.

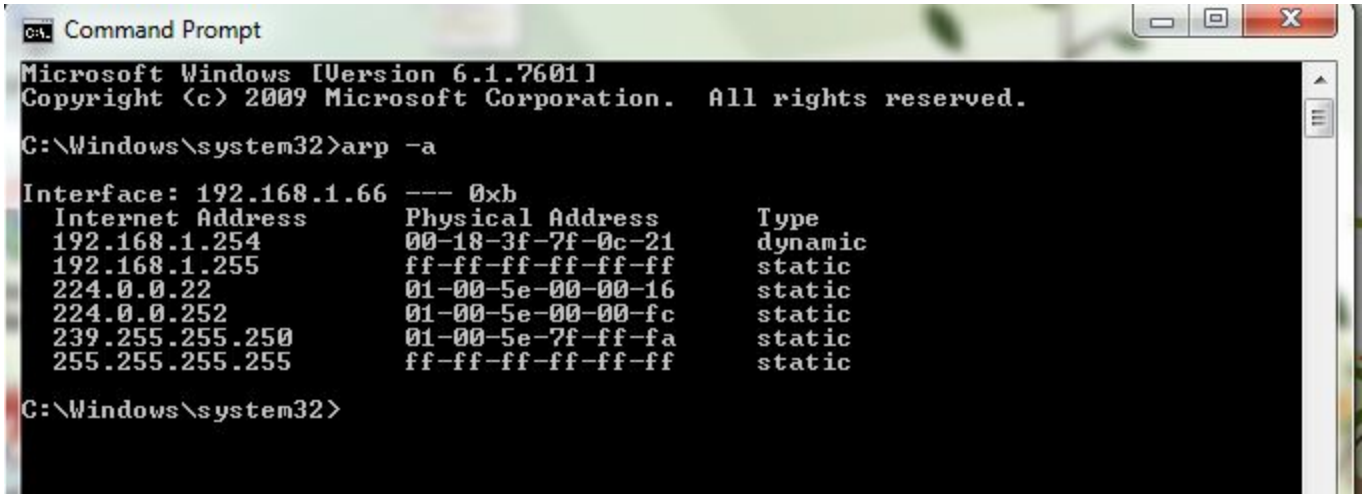
9. How many bytes from the very start of the Ethernet frame does the ASCII “O” in the “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

   Answer: From the start, there are 382 bytes of ASCII “O” in the OK appeared.

10. What is the hexadecimal value of the CRC field in this Ethernet frame?

    Answer: The is no hexadecimal value of CRC field shown in this Ethernet frame.

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



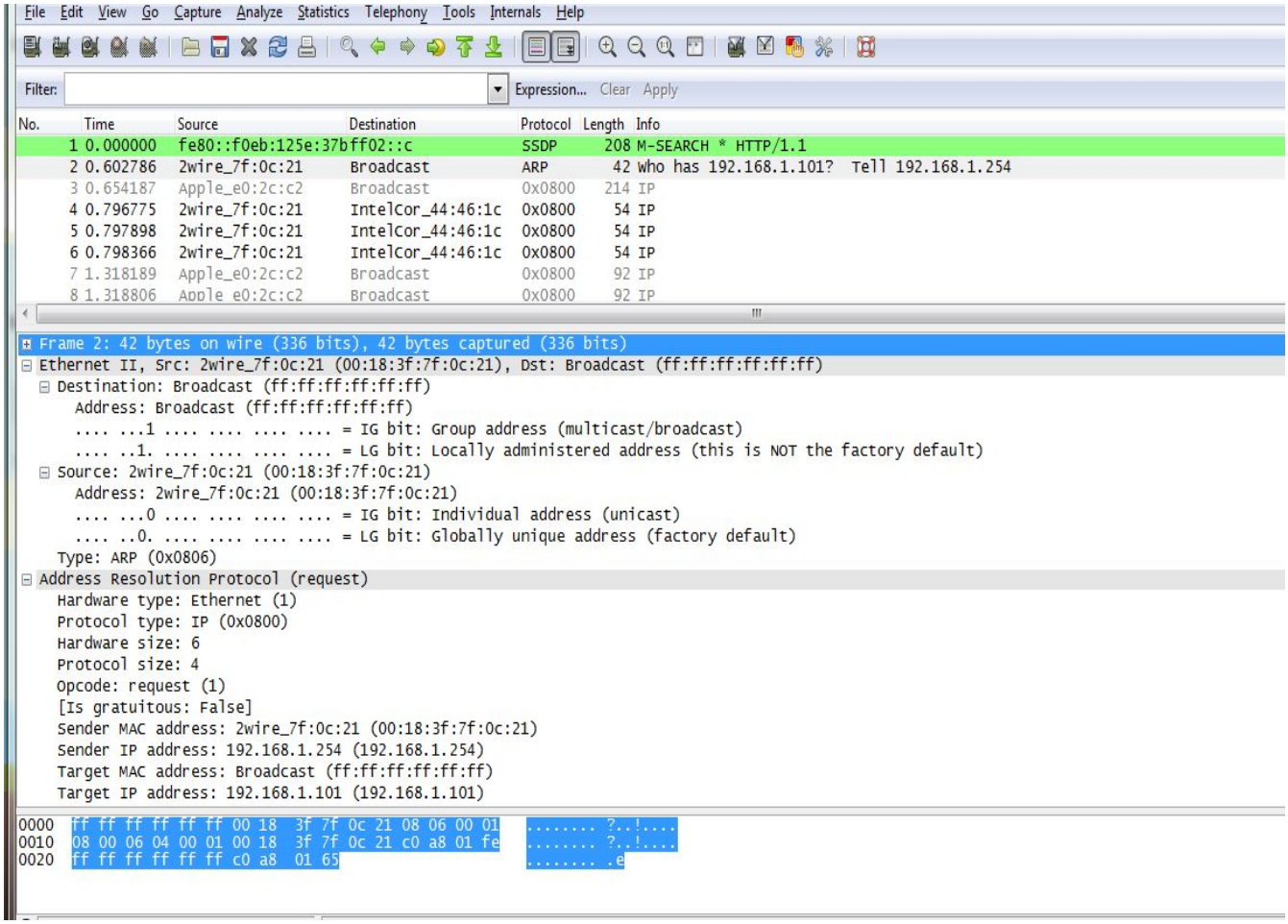
```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>arp -a

Interface: 192.168.1.66 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.254         00-18-3f-7f-0c-21     dynamic
  192.168.1.255         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:\Windows\system32>
```

Answer: Here are the contents of my computer’s ARP cache; the Internet Addresses, Physical addresses that contains the Medium Access Control, and the Type which indicates what type of Protocol.



ARP Message

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

Answer: The hexadecimal value for the source is...

`2wire_7f:0c:21 (00:18:3f:7f:0c:21)`

The hexadecimal value for the destination is...

`Destination:Broadcast (ff:ff:ff:ff:ff:ff)`

13. Give the hexadecimal value for the two-byte Ethernet frame type field. What do bit(s) whose value is 1 mean without the flag field?

Answer: The hexadecimal value for the 2 byte Ethernet frame type field is...

`Type: ARP (0x0806)`

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

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

Answer: There are 42 bytes of ARP opcode from the beginning of the Ethernet.

b. What is the value of the *upcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Answer: The value of the opcode field within the ARP-payload part of the Ethernet fram in which an ARP request is...

```
Opcode: request 1
```

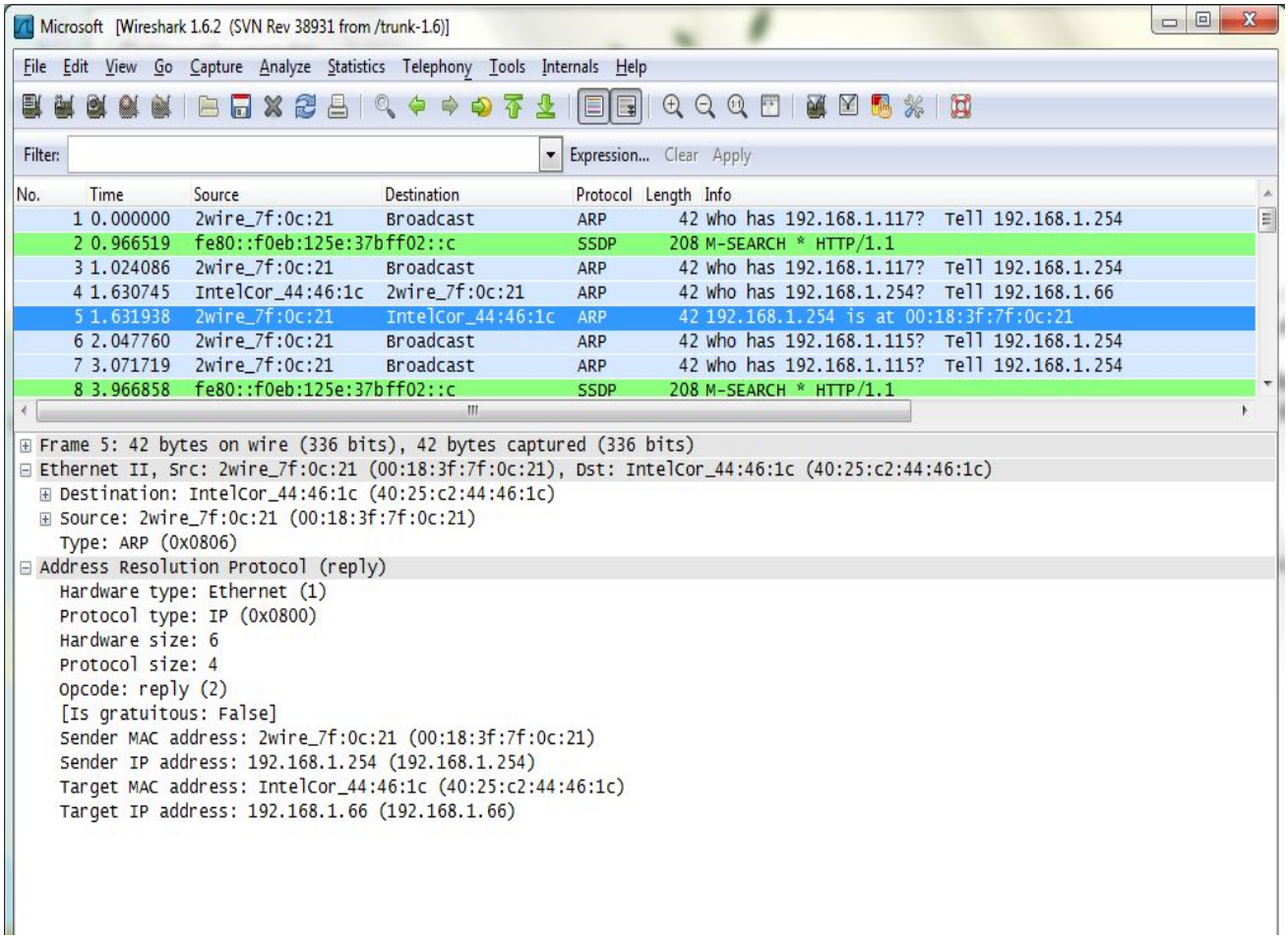
c. Does the ARP message contain the IP address of the sender?

Answer: Yes. The IP address is...

```
Sender IP Address: 192.168.1.254 (192.168.1.254)
```

d. Where in the ARP request does the “question” appear in - the Ethernet address of the machine whose corresponding IP address is being queried?

Answer: It is in the Target MAC address `Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)`”question” the Ethernet address of the machine whose corresponding `Target IP address: 198.168.1.101`



ARP Reply Message

15. Now find the ARP reply that was sent in reponse to the ARP request.

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

Answer: There are 42 bytes of ARP opcode since the beginning of the Ethernet frame.

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?

Answer: The value of the opcode field within the ARP payload part of the Ethernet frame is...

`Opcode: reply (2)`

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?

Answer: It is in the `Sender MAC address` where the “answer” of ARP request appeared - with and Ethernet address of `00:18:3f:7f:0c:21.` and sender IP address: `192:168:1:254.`

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

Answer: The hexadecimal value for the source address is `00:18:3f:7f:0c:21.` The hexadecimal value for the destination address is `40:25:c2:44:46:1c.`

17. 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 corresponds to an ARP request sent by the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated packet 6 - another ARP request.Why is there no ARP reply (sent in response to the ARP resquest in packet 6) in the packet trace?

Answer: It seems to me that the “request” disappeared, and the main reason why is that the MAC address of the sender did not match the destination address. If this is the case, then there will be no ARP “reply”.

Extra Credit

Extra-1. The arp command:

arp-s InetAddr EtherAddr

allows you manually add an entry to 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 address, but the wrong Ethernet address for that remote Ethernet address?

Answer: When you entered the wrong Ethernet address, the router will just discard it and ARP resolve this problem. It’s the ARP’s job to find the right MAC address whenever you send a packet.

Extra-2. What is the default amount of time that an entry remains in your cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

Answer: