Vanessa Ulloa

Daniel Kushner

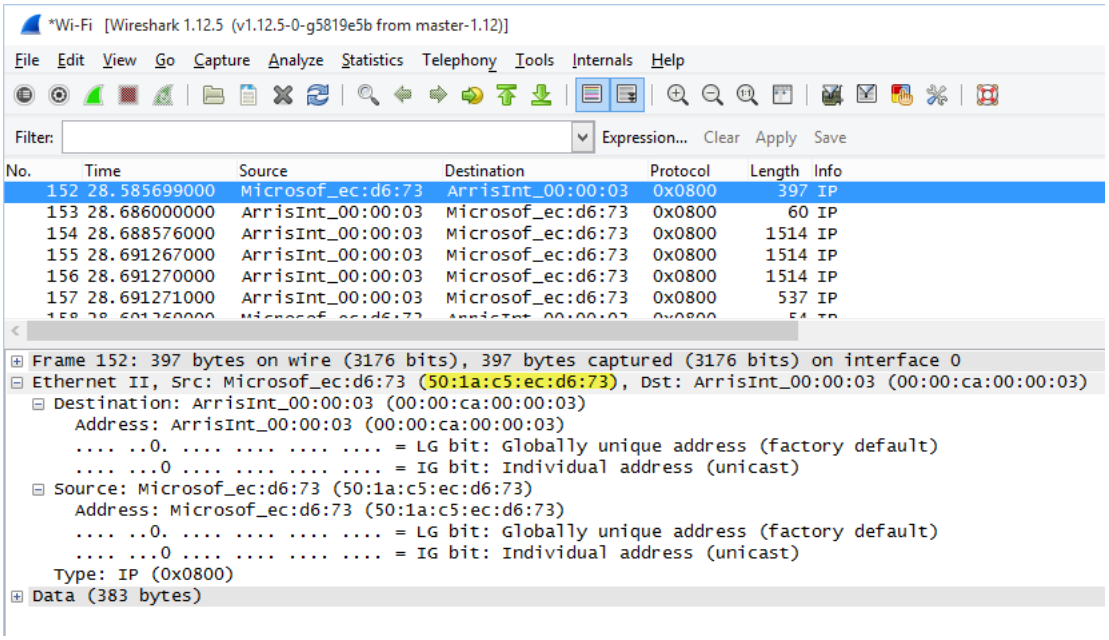
CST 311

16 June 2015

Lab 8

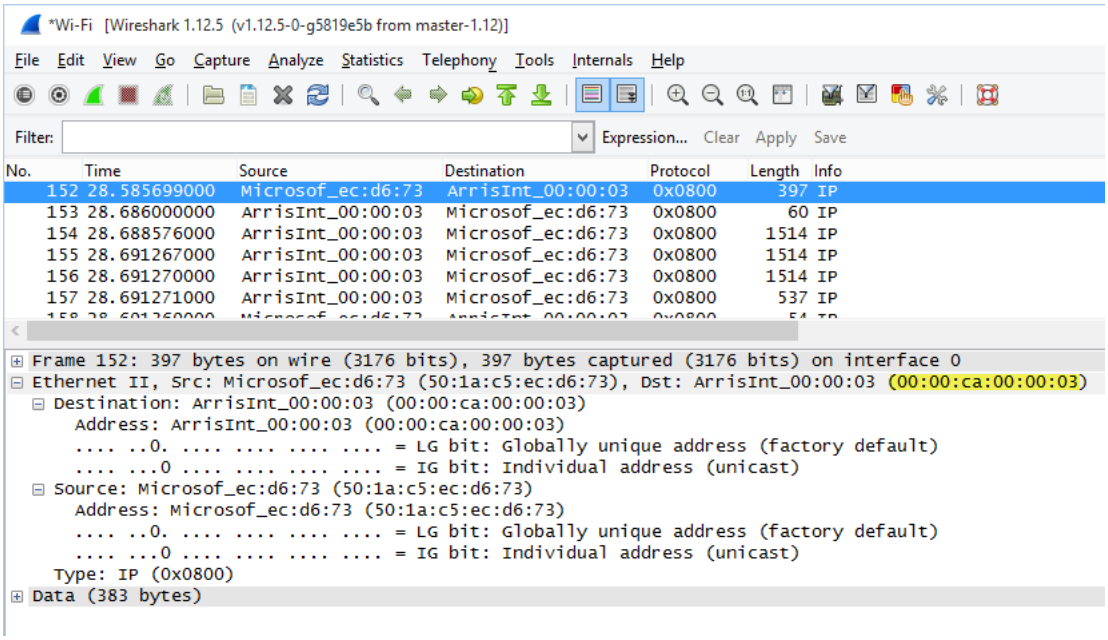
Capturing and analyzing Ethernet frames

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



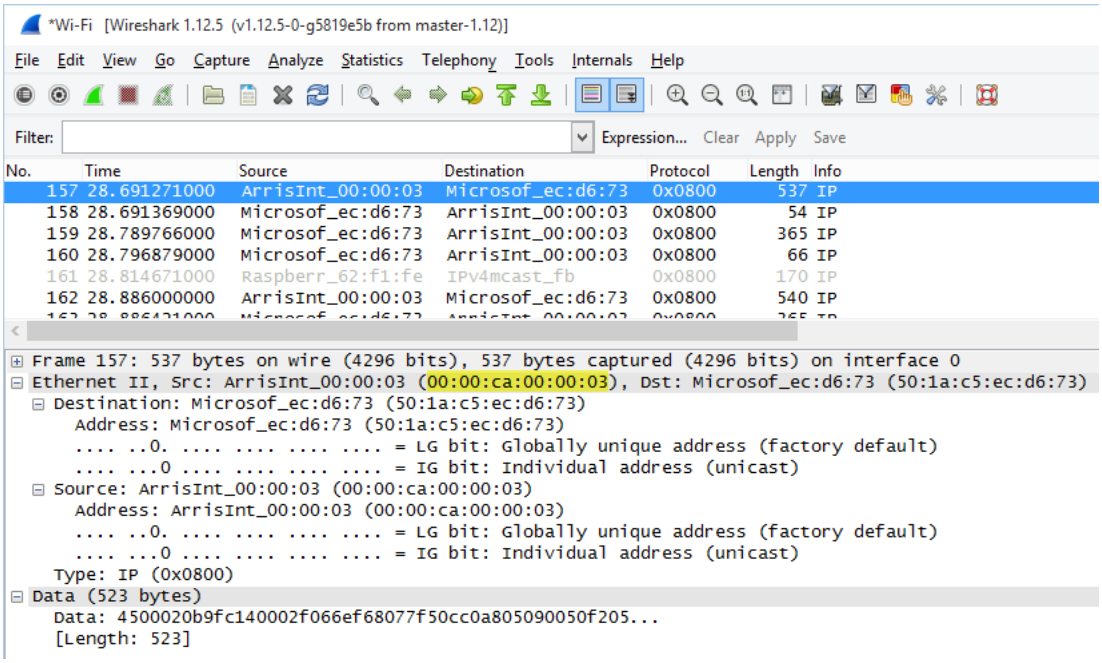
   a. 50:1a:c5:ec:d6:73

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.]



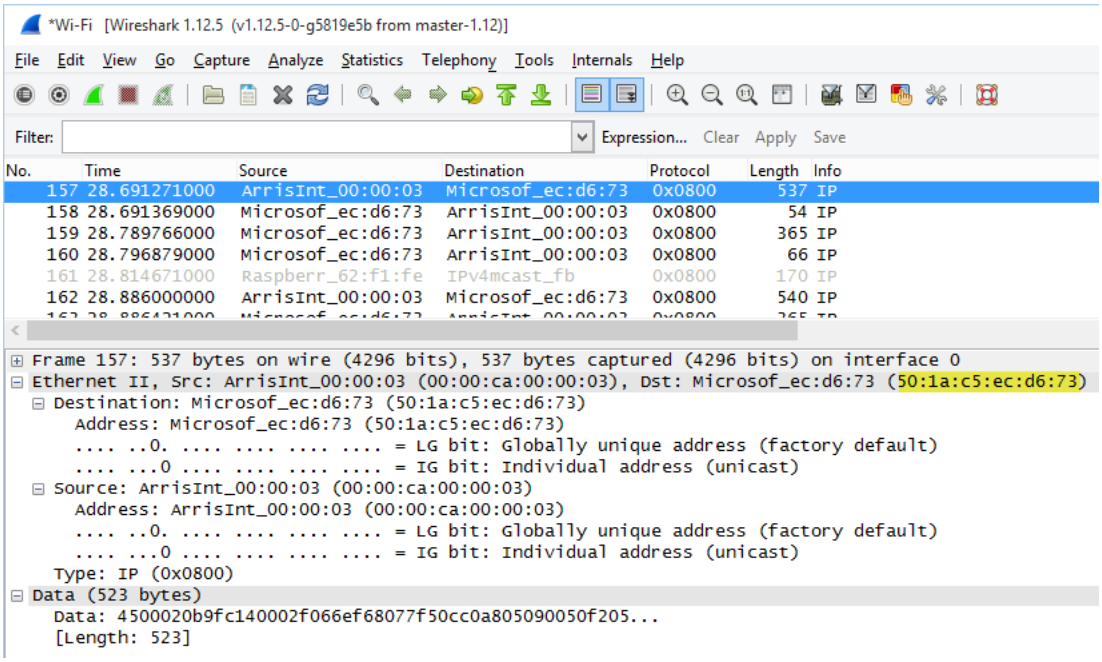
   a. 00:00:ca:00:00:03
   b. Not the same address as gaia.cs.umass.edu but the router instead.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   a. Type field: 0x0800
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?
   a. 54 bytes
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?



a. 00:00:ca:00:03

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

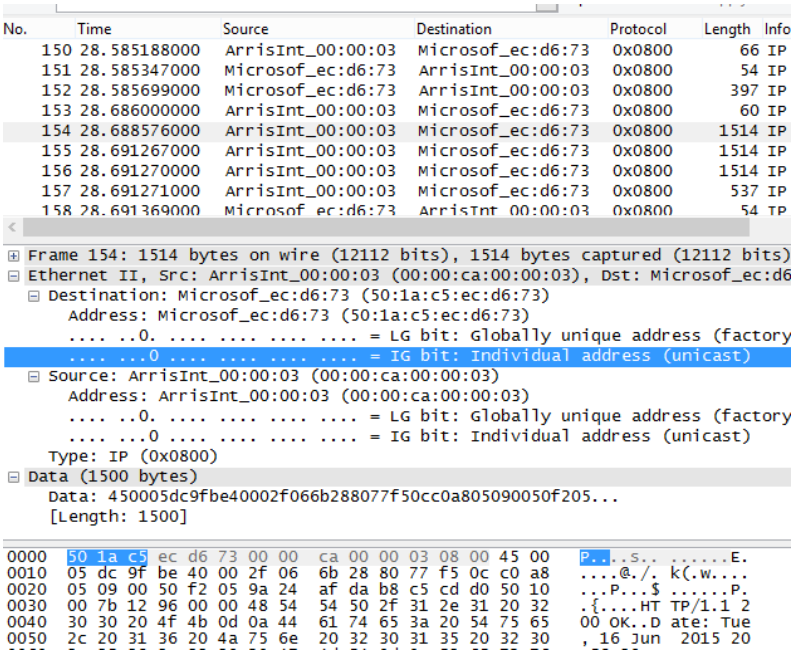


a. 50:1a:c5:ec:d6:73

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

a. 0x0800

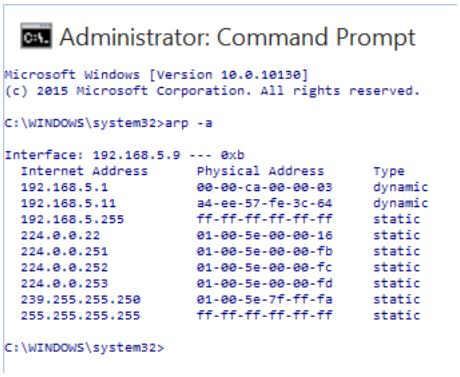
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?



   a. 53 bytes

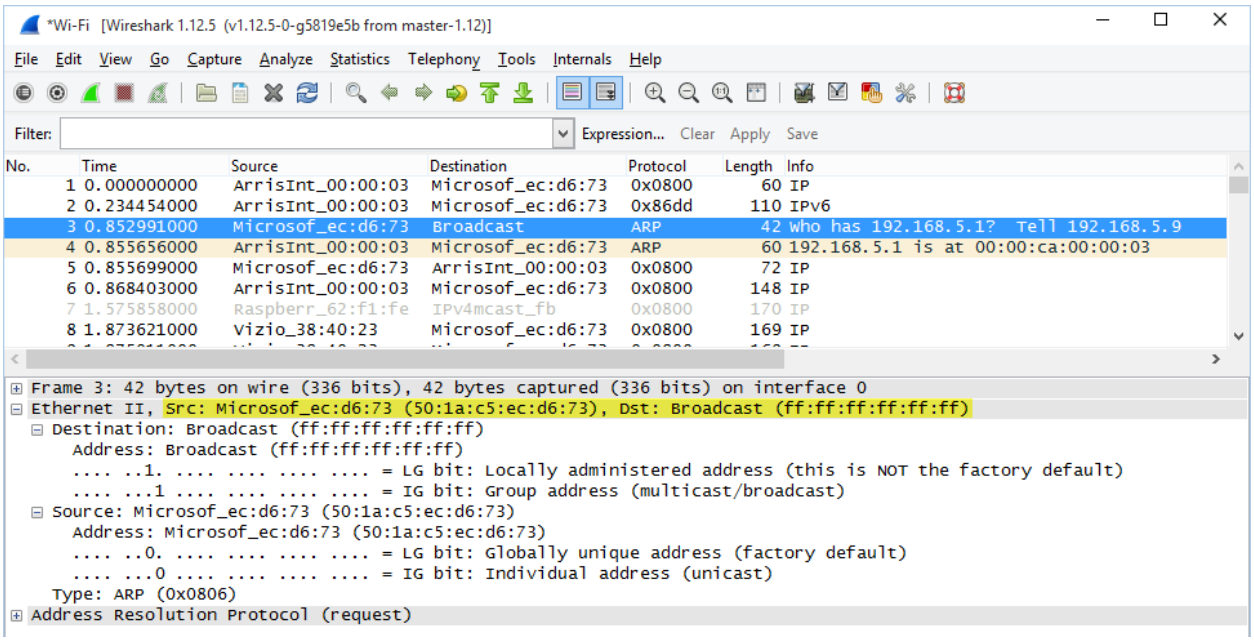
The Address Resolution Protocol

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



   a. Internet address = IP Address, Physical Address = MAC Address, type = protocol type.

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



   a. Source: 50:1a:c5:ec:d6:73
   b. Destination: ff:ff:ff:ff:ff:ff

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
    a. 0x0806, ARP
12. 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 frame does the ARP opcode field begin?
       i. 20 bytes
    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?
       i. 0x0001
    c. Does the ARP message contain the IP address of the sender?
       i. Yes, the Sender IP Address (192.168.5.9)
    d. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
       i. The target MAC address = 00:00:00:00:00:00
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?
       i. 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?
       i. 0x0002

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?
    i. The Sender MAC address with the IP Address

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
    a. Source address: 00:00:ca:00:00:03
    b. Destination address: 50:1a:c5:ec:d6:73
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?
    a. The reply is sent to the machine that sent the request, to the physical address.