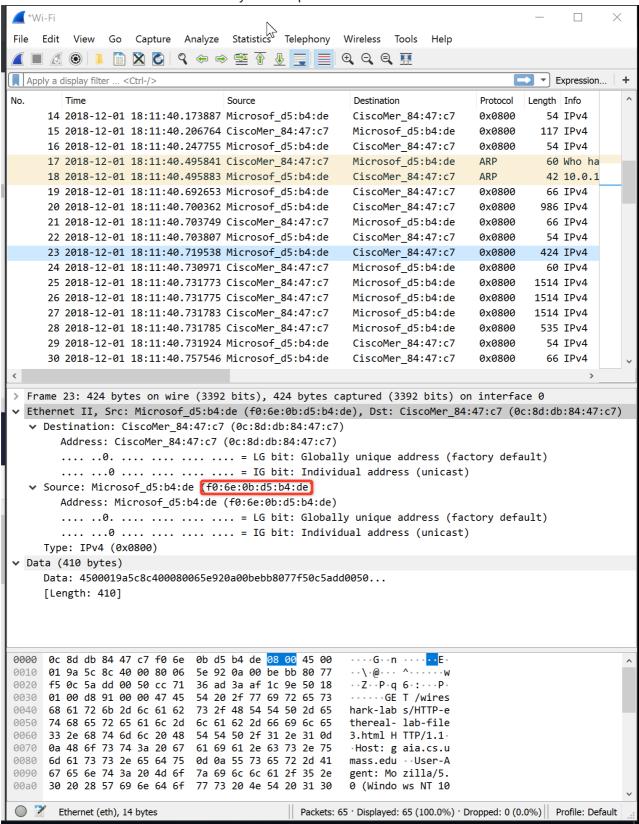Joel Benjamin Castillo (jc5383)

CS6843 - Computer Networking

Prof. Rafail Portnoy
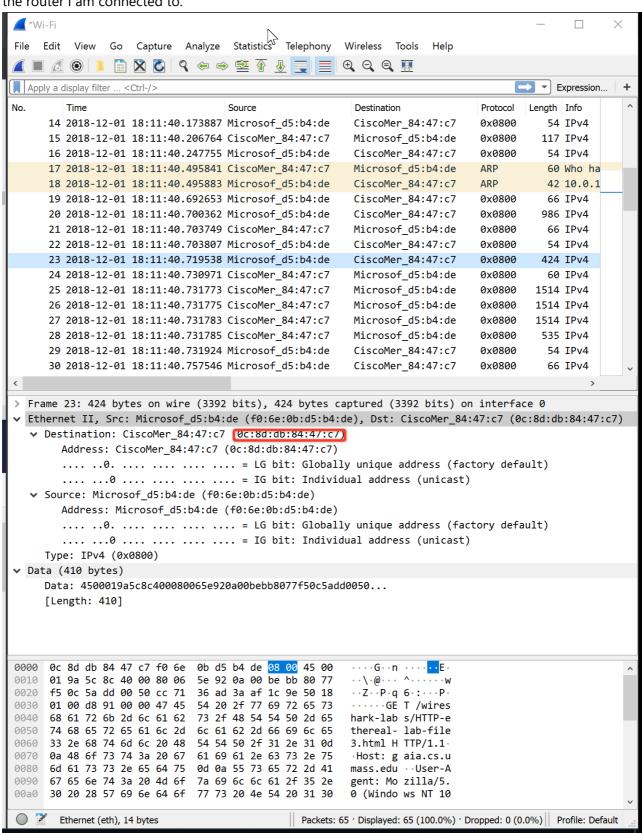
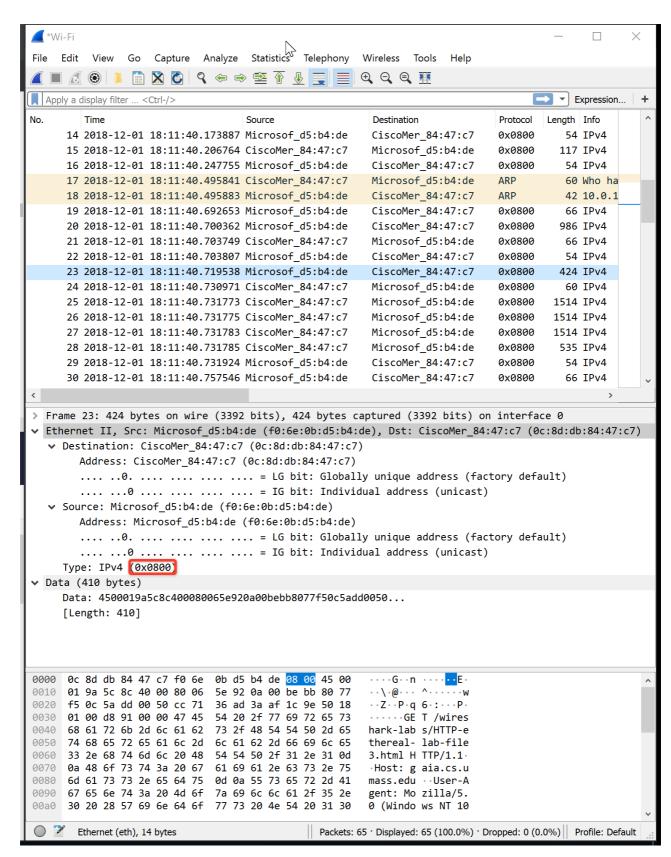**Wireshark Lab - Ethernet**

Ethernet Frames

1. What is the 48-bit Ethernet address of your computer? `f0:6e:0b:d5:b4:de`
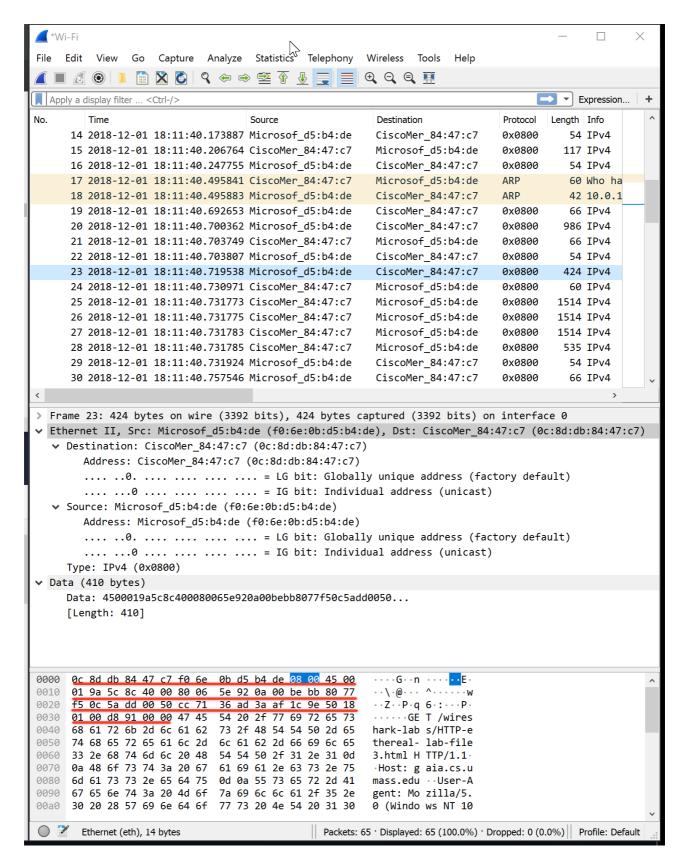
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.] `0c:8d:db:84:47:c7` This is the Ethernet address of the router I am connected to.

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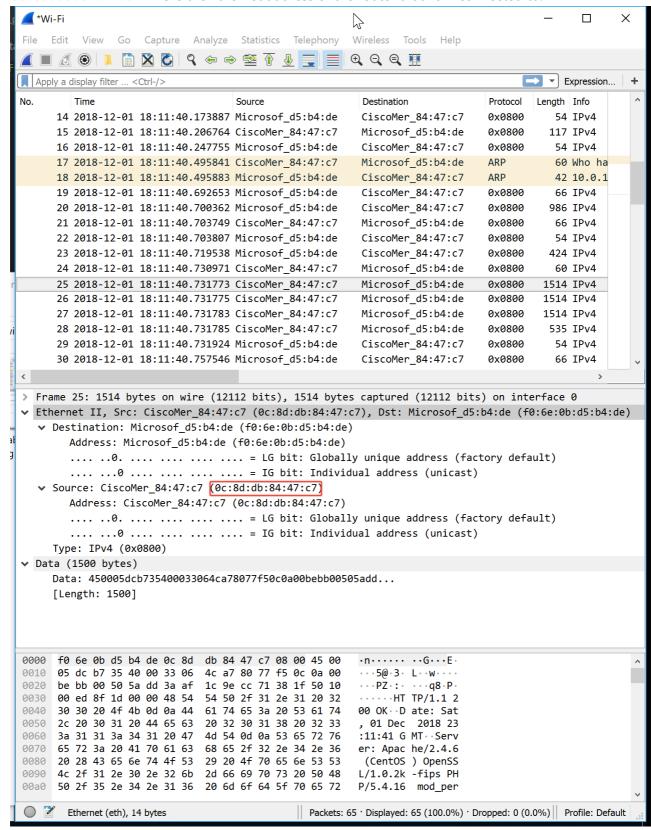
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? 54 bytes

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?

`0c:8d:db:84:47:c7` This is the Ethernet address of the router that I am connected to.

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

`f0:6e:0b:d5:b4:de` Yes, this is the Ethernet address of my network adapter.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? `0x0800` - IP

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? `67 bytes`

ARP

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

```
≥ Windows PowerShell

~ $ arp -a

Interface: 10.0.190.187 --- 0x4
  Internet Address        Physical Address      Type
  10.128.128.128          0c-8d-db-84-47-c7     dynamic
  10.255.255.255          ff-ff-ff-ff-ff-ff     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
  239.255.255.250         01-00-5e-7f-ff-fa     static
  239.255.255.253         01-00-5e-7f-ff-fd     static
  255.255.255.255         ff-ff-ff-ff-ff-ff     static

Interface: 10.0.0.1 --- 0x5
  Internet Address        Physical Address      Type
  10.0.0.255              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
  239.255.255.250         01-00-5e-7f-ff-fa     static
  239.255.255.253         01-00-5e-7f-ff-fd     static

Interface: 169.254.250.98 --- 0x8
  Internet Address        Physical Address      Type
  169.254.255.255         ff-ff-ff-ff-ff-ff     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
  239.255.255.250         01-00-5e-7f-ff-fa     static
  239.255.255.253         01-00-5e-7f-ff-fd     static
  255.255.255.255         ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x1c
  Internet Address        Physical Address      Type
  192.168.56.255          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
  239.255.255.250         01-00-5e-7f-ff-fa     static
  239.255.255.253         01-00-5e-7f-ff-fd     static
  255.255.255.255         ff-ff-ff-ff-ff-ff     static

~ $
```
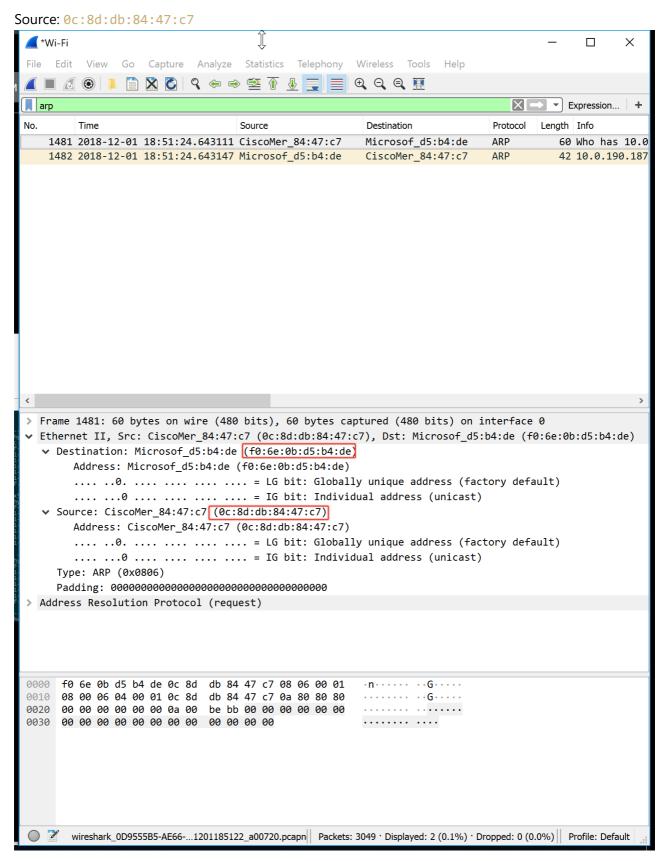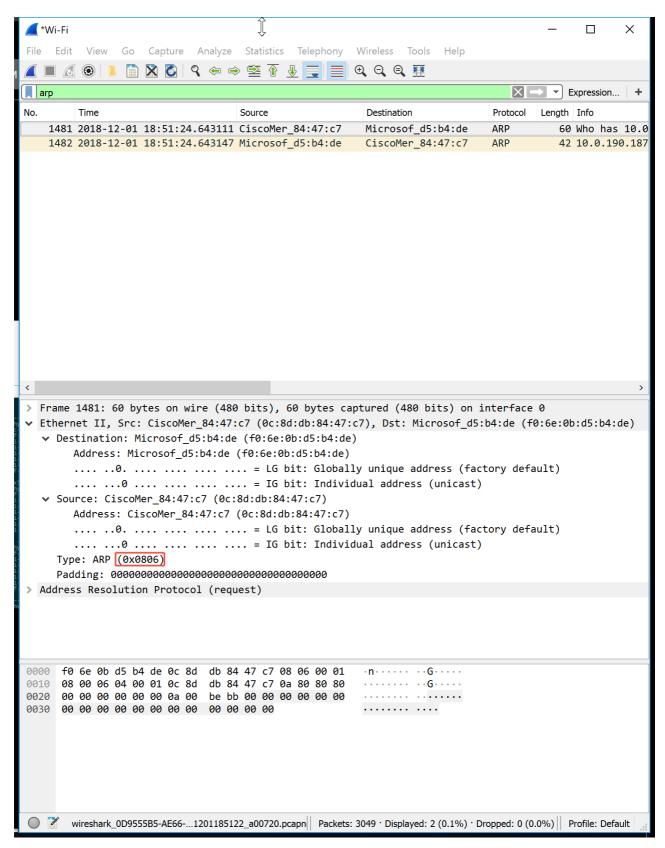
IP Address, MAC (Ethernet Address), ARP Entry Type - Static is manually configured and is permanent, Dynamic means the entry is created using the ARP protocol.

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Destination: f0:6e:0b:d5:b4:de

Source: `0c:8d:db:84:47:c7`

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to? `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? 20 bytes from the beginning of the frame 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? The hex value in the ARP-payload of the request is 0x0001 c) Does the ARP message contain the IP address of the sender? Yes d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried? The field Target MAC Address is set to 00:00:00:00:00:00 to query the machine whose IP address is being queried.

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? 20 byes from the beginning of the 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? `0x0002` - 2

```
*Wi-Fi                                                                        —    □    ✕

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

🔺 ■ 🔺 ◎  📄 🗙 🔄  🔍 ⬅ ➡ 🔼 ⬇ 🔽 ≡  ⊕ ⊖ ⊝ 🔳

🚩 arp                                                                    🗙 ➡ ▼  Expression...  +

No.      Time                          Source                Destination             Protocol   Length   Info
      1481 2018-12-01 18:51:24.643111 CiscoMer_84:47:c7      Microsof_d5:b4:de        ARP            60   Who has 10.0
      1482 2018-12-01 18:51:24.643147 Microsof_d5:b4:de      CiscoMer_84:47:c7        ARP            42   10.0.190.187

>  Frame 1482: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v  Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
     v  Destination: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
           Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
           .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
           .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     v  Source: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
           Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
           .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
           .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        Type: ARP (0x0806)
v  Address Resolution Protocol (reply)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: reply (2)
     Sender MAC address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
     Sender IP address: 10.0.190.187
     Target MAC address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
     Target IP address: 10.128.128.128

0000   0c 8d db 84 47 c7 f0 6e  0b d5 b4 de 08 06 00 01   ····G··n ········
0010   08 00 06 04 00 02 f0 6e  0b d5 b4 de 0a 00 be bb   ·······n ········
0020   0c 8d db 84 47 c7 0a 80  80 80                     ····G··· ··

○ 📝   Opcode (arp.opcode), 2 bytes              ‖ Packets: 3049 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) ‖ Profile: Default
```

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? The answer appears in the `Sender MAC Address` field. Value contains `f0:6e:0b:d5:b4:de`

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message? Destination: `0c:8d:db:84:47:c7`
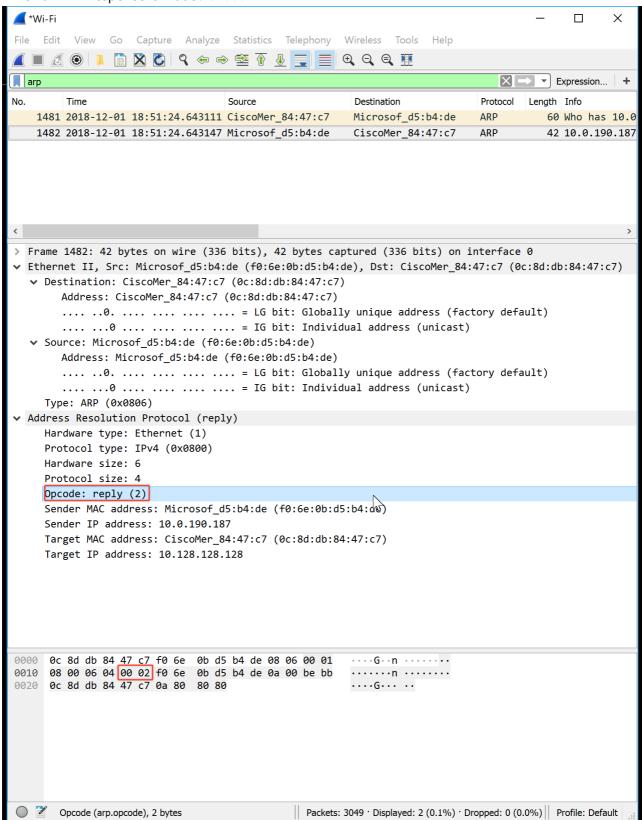
Source: `f0:6e:0b:d5:b4:de`

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 reply because this request came from a different host. It is a broadcast, but the reply will be sent to the sender's MAC address.