WireShark Lab 6

Jennifer Hurst

- Clear your browser history, and visit: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html (your browser should display the US Bill of Rights)
- • Using Wireshark, capture the packets. Remember to start, then visit webpage, and then stop.
- • We are going to analyze Ethernet frames.
- • (*For each of these questions, take a screenshot of Wireshark, and attach it to your answer*) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- • Include a terminal screenshot showing your computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Lab will NOT be graded if either of these two is missing.

Questions:

1. What is the MAC address from your computer?

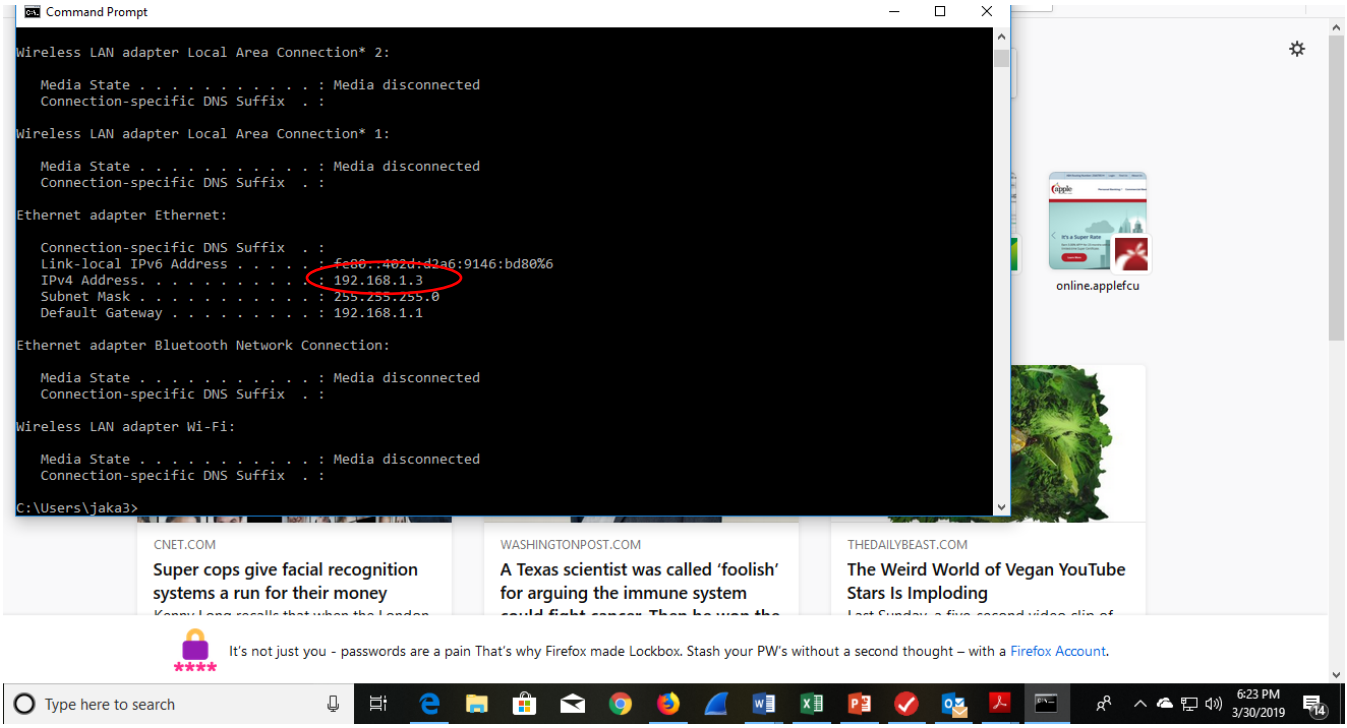
2. What is the destination MAC address?

3. What device has the MAC address shown in the destination?

4. Explain the relationship between the destination MAC address and the destination IP address.

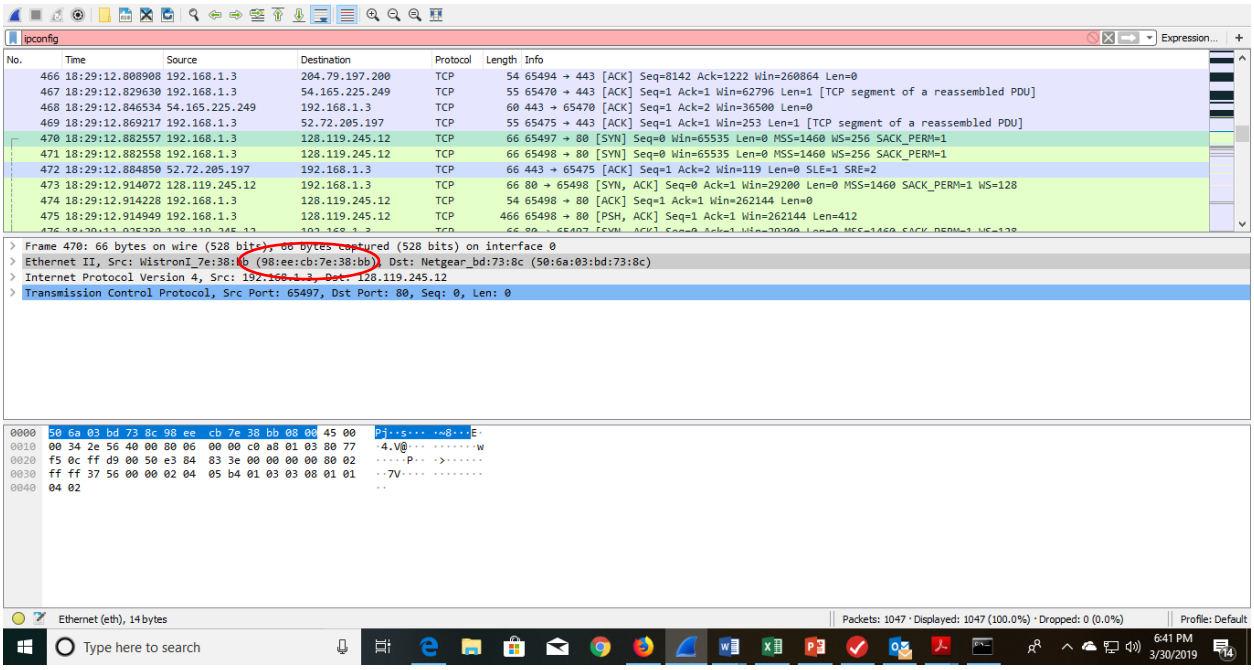
5. Using the terminal (cmd in Windows, Terminal in mac), run a command to display your full ARP list table. (Find out what the command is, and print a full screen shot of your result.)

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**
   My IP address is 192.168.1.3

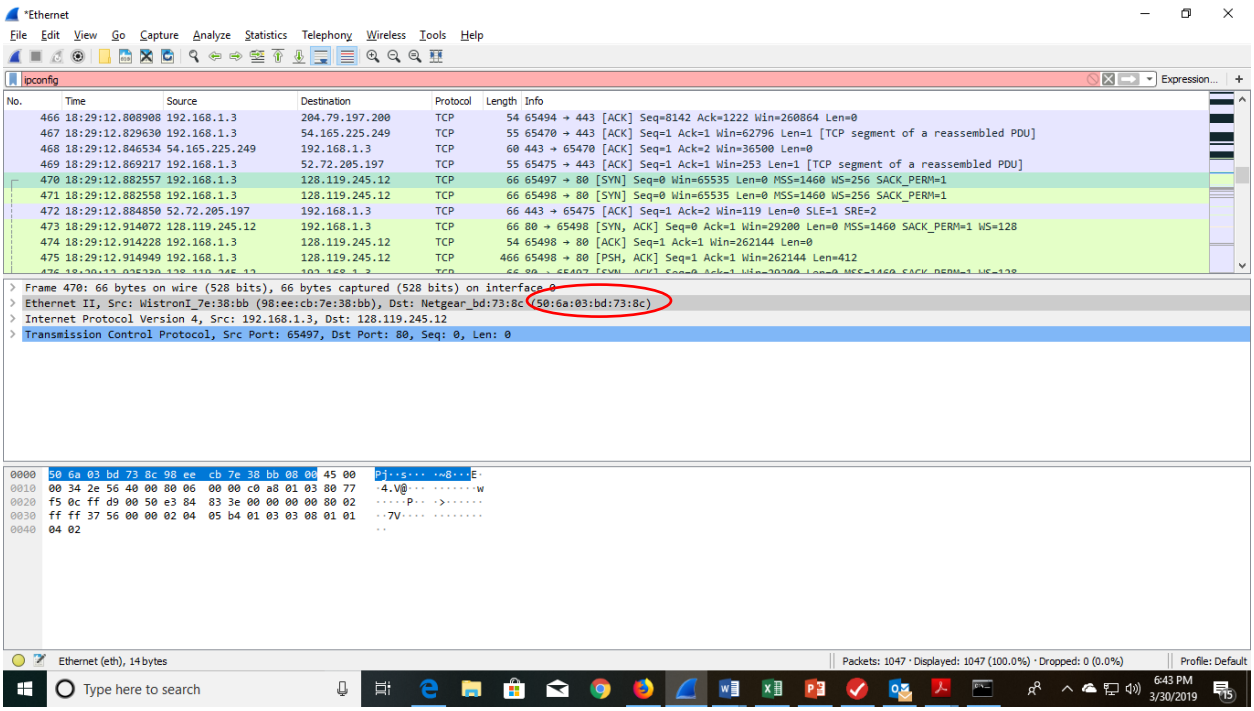


Questions:

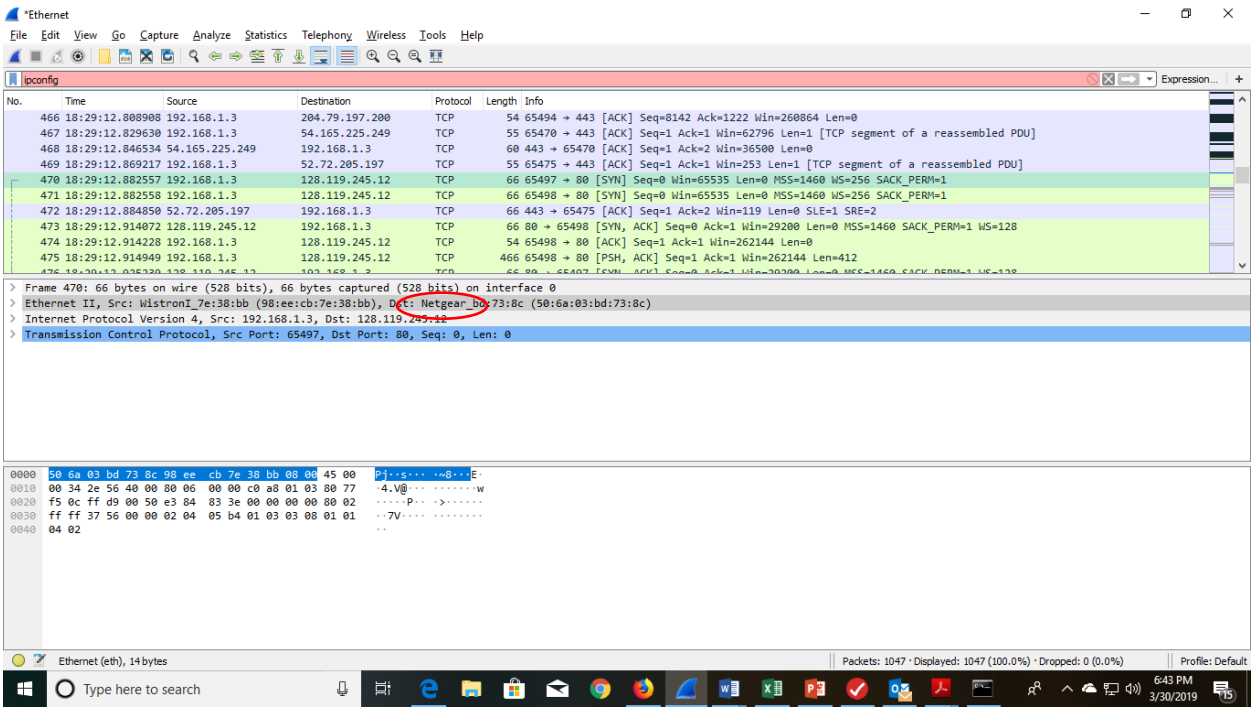
1. What is the MAC address from your computer? 98-EE-CB-7E-38-BB



2. What is the destination MAC address? 50:6a:03:bd:73:8c

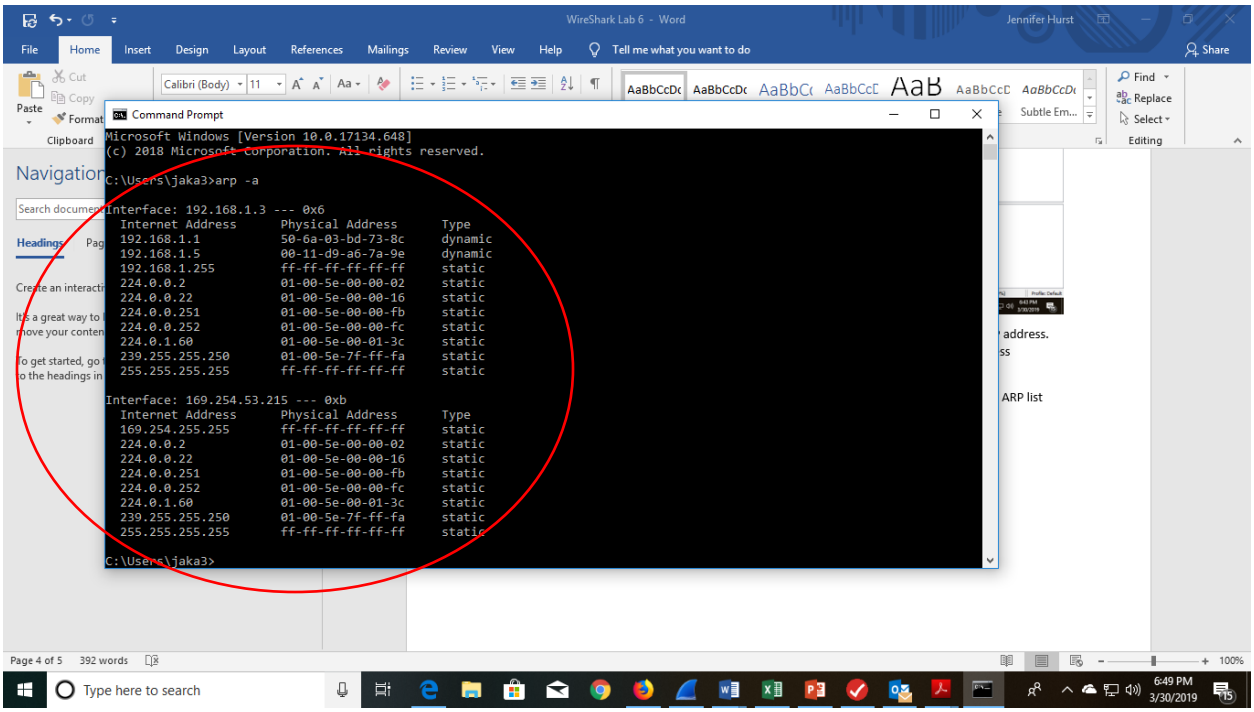


3. What device has the MAC address shown in the destination? Netgear.

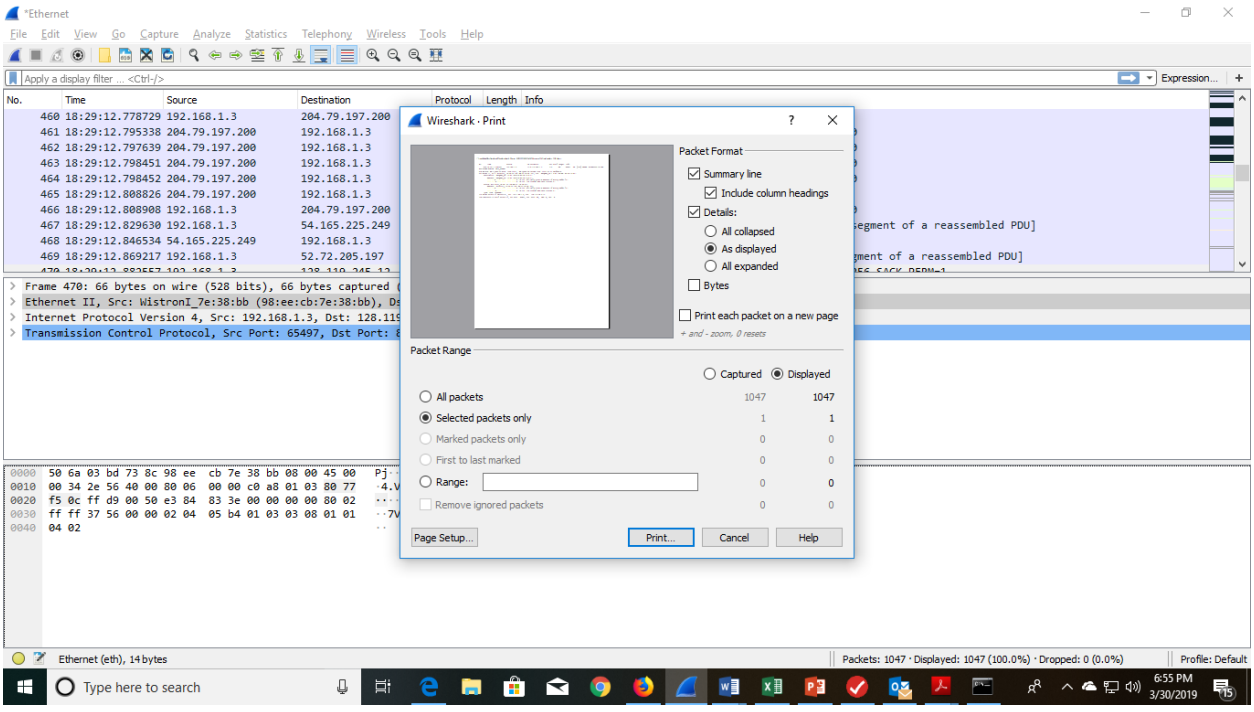


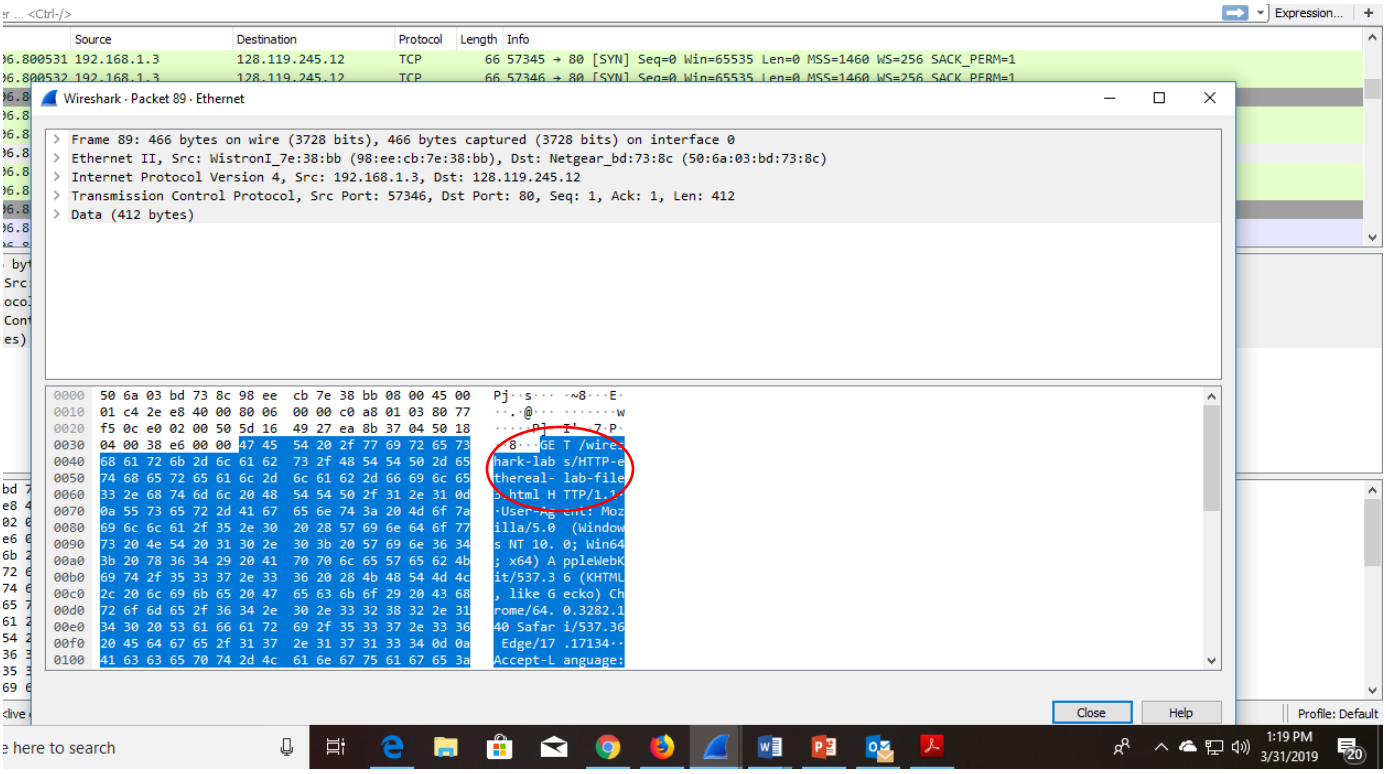
4. Explain the relationship between the destination MAC address and the destination IP address. The ARP cache links the MAC address and the destination IP address. ARP, the address resolution protocol converts an IP address to a MAC address.

5. Using the terminal (cmd in Windows, Terminal in mac), run a command to display your full ARP list table. (Find out what the command is, and print a full screen shot of your result.) Arp -a command



Print screen, final page.




Wireshark · Packet 89 · Ethernet
Frame 89: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface 0
Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd:73:8c (50:6a:03:bd:73:8c)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57346, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
Data (412 bytes)
Close
Help