

WireShark Lab 6

Jennifer Hurst

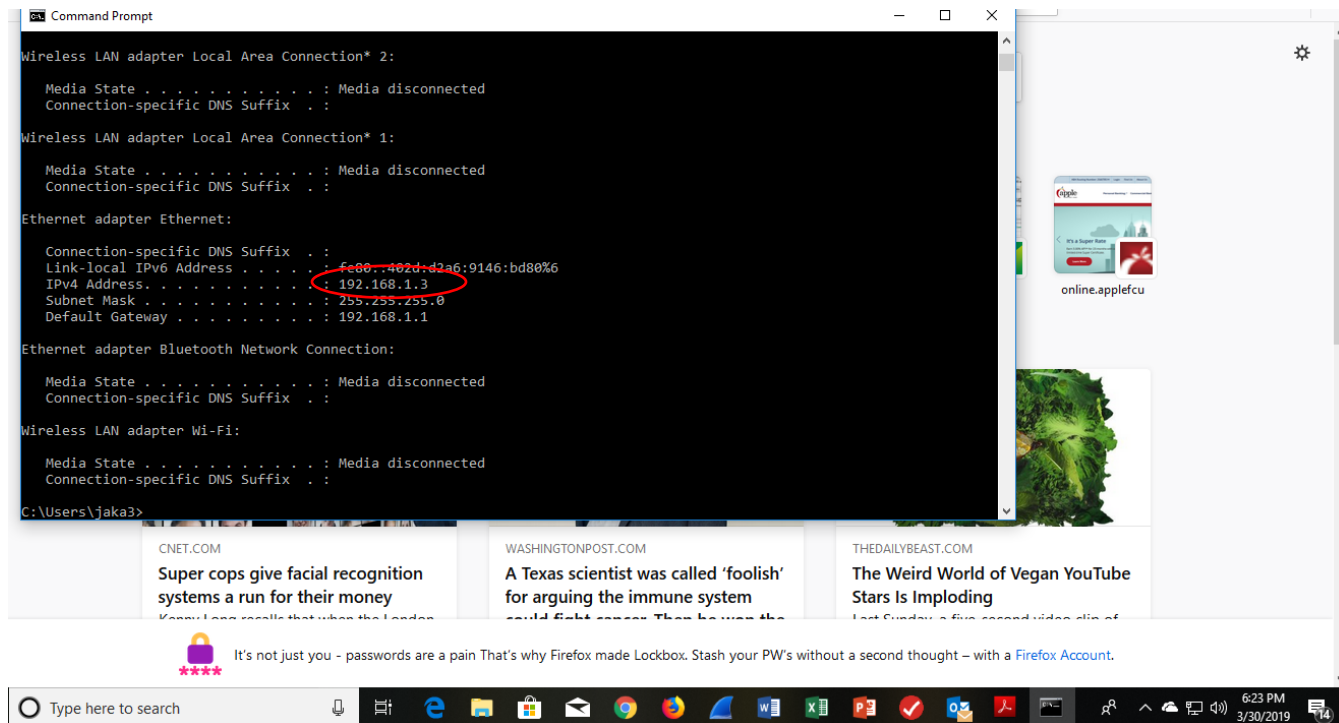
- Clear your browser history, and visit: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html> (your browser should display the US Bill of Rights)
- • Using Wireshark, capture the packets. Remember to start, then visit webpage, and then stop.
- • We are going to analyze Ethernet frames.
- • *(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:

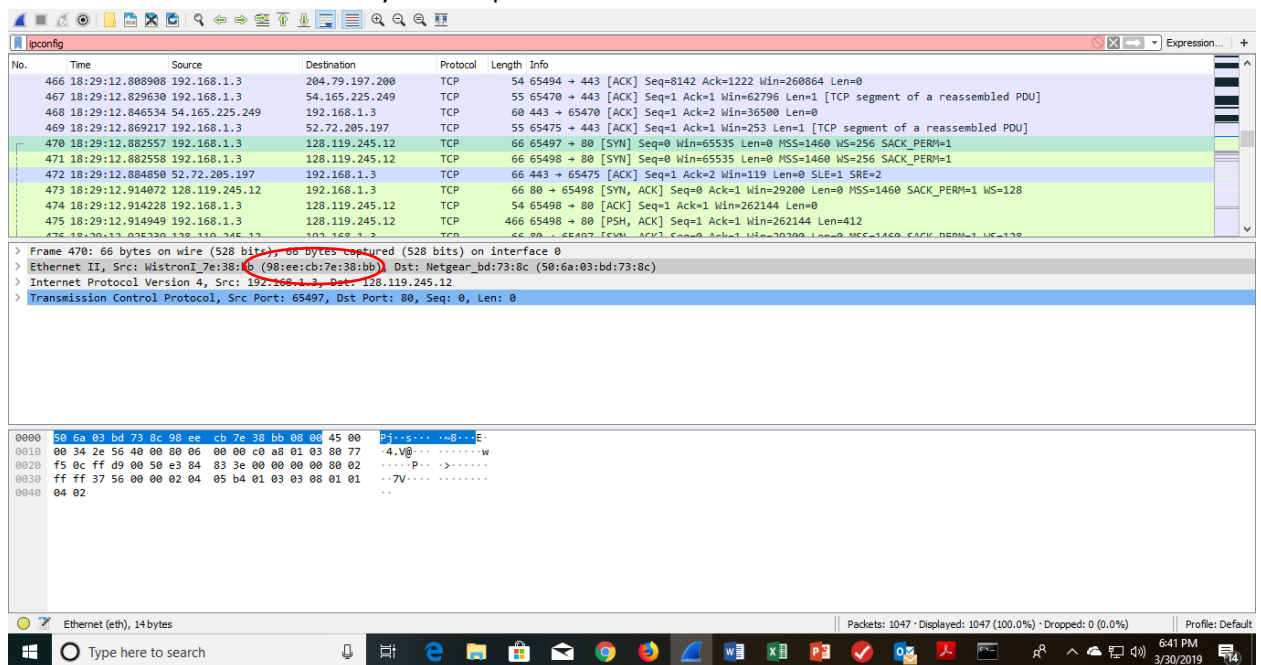
1. What is the MAC address from your computer?
2. What is the destination MAC address?
3. What device has the MAC address shown in the destination?
4. Explain the relationship between the destination MAC address and the destination IP address.
5. Using the terminal (cmd in Windows, Terminal in mac), 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

Wireshark packet capture showing a list of network packets. Packet 470 is selected, and its details pane shows Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The destination MAC address 50:6a:03:bd:73:8c is circled in the Ethernet II section.

No.	Time	Source	Destination	Protocol	Length	Info
466	18:29:12.808908	192.168.1.3	204.79.197.200	TCP	54	65494 → 443 [ACK] Seq=8142 Ack=1222 Win=260864 Len=0
467	18:29:12.829630	192.168.1.3	54.165.225.249	TCP	55	65470 → 443 [ACK] Seq=1 Ack=1 Win=62796 Len=1 [TCP segment of a reassembled PDU]
468	18:29:12.846534	54.165.225.249	192.168.1.3	TCP	60	443 → 65470 [ACK] Seq=1 Ack=2 Win=36500 Len=0
469	18:29:12.869217	192.168.1.3	52.72.205.197	TCP	55	65475 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
470	18:29:12.882557	192.168.1.3	128.119.245.12	TCP	66	65497 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
471	18:29:12.882558	192.168.1.3	128.119.245.12	TCP	66	65498 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
472	18:29:12.884850	52.72.205.197	192.168.1.3	TCP	66	443 → 65475 [ACK] Seq=1 Ack=2 Win=119 Len=0 SLE=1 SRE=2
473	18:29:12.914072	128.119.245.12	192.168.1.3	TCP	66	80 → 65498 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
474	18:29:12.914228	192.168.1.3	128.119.245.12	TCP	54	65498 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
475	18:29:12.914949	192.168.1.3	128.119.245.12	TCP	466	65498 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=412

Details pane for Packet 470:

- Frame 470: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 65497, Dst Port: 80, Seq: 0, Len: 0

Hex dump and ASCII view of the packet data:

```

0000  50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 00 00 45 00  p[...].w...E
0010  00 34 2e 56 40 00 00 06 00 00 c0 a8 01 03 80 77  .4.V.....w
0020  f5 0c ff d9 00 50 e3 84 83 3e 00 00 00 00 80 02  ..P.....
0030  ff ff 37 56 00 00 02 04 05 b4 01 03 03 08 01 01  ..7V.....
0040  04 02  ..

```

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

Wireshark packet capture showing a list of network packets. Packet 470 is selected, and its details pane shows Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The destination MAC address 50:6a:03:bd:73:8c is circled in the Ethernet II section.

No.	Time	Source	Destination	Protocol	Length	Info
466	18:29:12.808908	192.168.1.3	204.79.197.200	TCP	54	65494 → 443 [ACK] Seq=8142 Ack=1222 Win=260864 Len=0
467	18:29:12.829630	192.168.1.3	54.165.225.249	TCP	55	65470 → 443 [ACK] Seq=1 Ack=1 Win=62796 Len=1 [TCP segment of a reassembled PDU]
468	18:29:12.846534	54.165.225.249	192.168.1.3	TCP	60	443 → 65470 [ACK] Seq=1 Ack=2 Win=36500 Len=0
469	18:29:12.869217	192.168.1.3	52.72.205.197	TCP	55	65475 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
470	18:29:12.882557	192.168.1.3	128.119.245.12	TCP	66	65497 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
471	18:29:12.882558	192.168.1.3	128.119.245.12	TCP	66	65498 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
472	18:29:12.884850	52.72.205.197	192.168.1.3	TCP	66	443 → 65475 [ACK] Seq=1 Ack=2 Win=119 Len=0 SLE=1 SRE=2
473	18:29:12.914072	128.119.245.12	192.168.1.3	TCP	66	80 → 65498 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
474	18:29:12.914228	192.168.1.3	128.119.245.12	TCP	54	65498 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
475	18:29:12.914949	192.168.1.3	128.119.245.12	TCP	466	65498 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=412

Details pane for Packet 470:

- Frame 470: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 65497, Dst Port: 80, Seq: 0, Len: 0

Hex dump and ASCII view of the packet data:

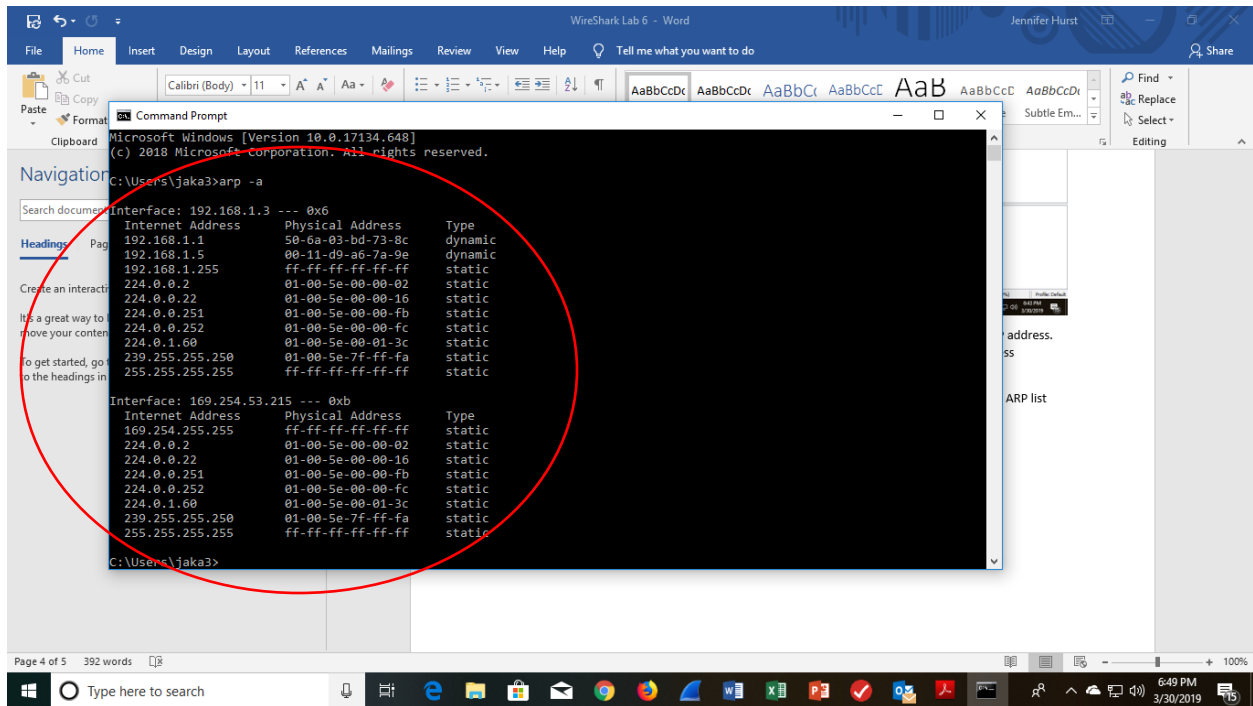
```

0000  50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 00 00 45 00  p[...].w...E
0010  00 34 2e 56 40 00 00 06 00 00 c0 a8 01 03 80 77  .4.V.....w
0020  f5 0c ff d9 00 50 e3 84 83 3e 00 00 00 00 80 02  ..P.....
0030  ff ff 37 56 00 00 02 04 05 b4 01 03 03 08 01 01  ..7V.....
0040  04 02  ..

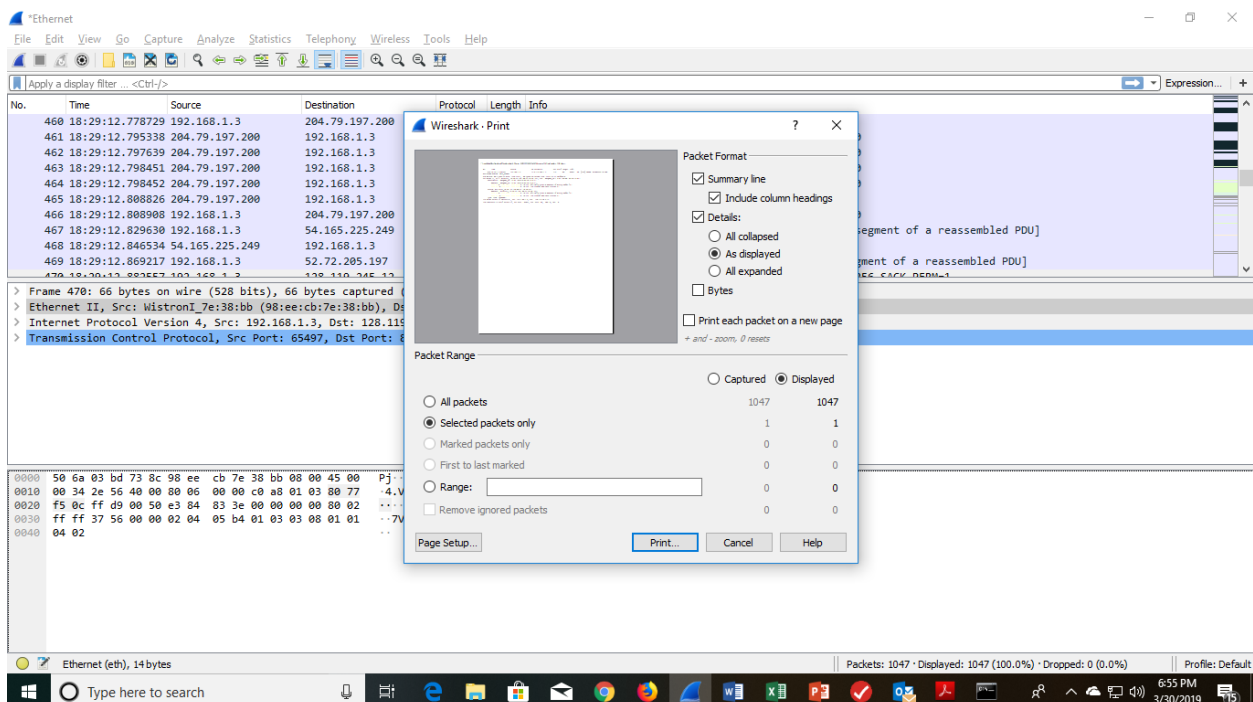
```

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)

0000 50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 08 00 45 00 Pj...s...w8...E-
0010 01 c4 2e e8 40 00 80 06 00 00 c0 a8 01 03 80 77 ...@.....w
0020 f5 0c e0 02 00 50 5d 16 49 27 ea 8b 37 04 50 18 ...03...7:P-
0030 04 00 38 e6 00 00 47 45 54 20 2f 77 69 72 65 73 8...GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d s.html H TTP/1.
0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a User-agent: Moz
0080 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window
0090 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 s NT 10.0; Win64
00a0 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b ; x64) AppleWebK
00b0 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c it/537.3.6 (KHTML
00c0 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 , like Gecko) Ch
00d0 72 6f 6d 65 2f 36 34 2e 30 2e 33 32 38 32 2e 31 rome/64.0.3282.1
00e0 34 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 40 Safari/537.36
00f0 20 45 64 67 65 2f 31 37 2e 31 37 31 33 34 0d 0a Edge/17.17134...
0100 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a Accept-L language:

Close Help Profile: Default

here to search

1:19 PM 3/31/2019