

Data Communications Laboratory Introduction to Wireshark

Your Name: James Cummins

Your Student ID: 44816944

Documentation Task 1.

What interfaces are available on your computer? What do they appear to be? Do they all have the same IP address? Record this in your documentation.

According to the Oracle documentation, an interface is a point of interconnection between a computer and a private or public network. This in laymen's terms is the physical or virtual medium in which my computer, a closed system, 'communicates' or 'connects' to another information technology system. It could be a wifi card, or it could be a Ethernet network interface controller.

Wireshark displays two interfaces currently – the VirtualBox and the Ethernet cable.

They cannot share the same IP address as this is designed to be a unique identifying address.

Documentation Task 2.

Record the IP address and MAC (Ethernet) address for the Ethernet interface of the computer you are using

IP address: 10.6.19.63

MAC address: 00-68-EB-A3-07-0A

Documentation Task 3.

1. How many HTTP packets were received by your machine?

22

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|-----------|--------|---|
| 71 | 3.744809 | 10.6.19.63 | 64.142.54.22 | HTTP | 510 | GET / HTTP/1.1 |
| 105 | 4.232603 | 10.6.19.63 | 64.142.54.22 | HTTP | 379 | GET /css/main.css HTTP/1.1 |
| 110 | 4.233905 | 10.6.19.63 | 64.142.54.22 | HTTP | 436 | GET /img/ntf_logo_121x88.png HTTP/1.1 |
| 111 | 4.233951 | 10.6.19.63 | 64.142.54.22 | HTTP | 437 | GET /img/ipv6_ready_80x15.png HTTP/1.1 |
| 113 | 4.284100 | 64.142.54.22 | 10.6.19.63 | HTTP/X... | 1135 | HTTP/1.1 200 OK |
| 114 | 4.284630 | 10.6.19.63 | 64.142.54.22 | HTTP | 387 | GET /css/highcontrast.css HTTP/1.1 |
| 118 | 4.302233 | 10.6.19.63 | 64.142.54.22 | HTTP | 380 | GET /css/mills.css HTTP/1.1 |
| 130 | 4.546426 | 64.142.54.22 | 10.6.19.63 | HTTP | 389 | HTTP/1.1 200 OK (text/css) |
| 135 | 4.547588 | 10.6.19.63 | 64.142.54.22 | HTTP | 384 | GET /css/printable.css HTTP/1.1 |
| 136 | 4.547596 | 64.142.54.22 | 10.6.19.63 | HTTP | 609 | HTTP/1.1 200 OK (PNG) |
| 137 | 4.548487 | 10.6.19.63 | 64.142.54.22 | HTTP | 450 | GET /img/antipixel_valid_xhtml10_80x15.gif HTTP/1.1 |
| 141 | 4.598186 | 64.142.54.22 | 10.6.19.63 | HTTP | 1432 | HTTP/1.1 200 OK (text/css) |
| 142 | 4.599248 | 10.6.19.63 | 64.142.54.22 | HTTP | 395 | GET /css/anti-ns4.css HTTP/1.1 |
| 148 | 4.621478 | 64.142.54.22 | 10.6.19.63 | HTTP | 747 | HTTP/1.1 200 OK (PNG) |
| 149 | 4.621940 | 10.6.19.63 | 64.142.54.22 | HTTP | 446 | GET /img/antipixel_valid_css_80x15.gif HTTP/1.1 |
| 151 | 4.622709 | 64.142.54.22 | 10.6.19.63 | HTTP | 216 | HTTP/1.1 200 OK (text/css) |
| 161 | 4.862208 | 64.142.54.22 | 10.6.19.63 | HTTP | 820 | HTTP/1.1 200 OK (GIF89a) |
| 162 | 4.866769 | 64.142.54.22 | 10.6.19.63 | HTTP | 620 | HTTP/1.1 200 OK (text/css) |
| 166 | 4.918867 | 64.142.54.22 | 10.6.19.63 | HTTP | 458 | HTTP/1.1 200 OK (text/css) |
| 168 | 4.941875 | 64.142.54.22 | 10.6.19.63 | HTTP | 787 | HTTP/1.1 200 OK (GIF89a) |
| 169 | 4.945024 | 10.6.19.63 | 64.142.54.22 | HTTP | 467 | GET /favicon.ico HTTP/1.1 |
| 179 | 5.258280 | 64.142.54.22 | 10.6.19.63 | HTTP | 224 | HTTP/1.1 200 OK (image/x-icon) |

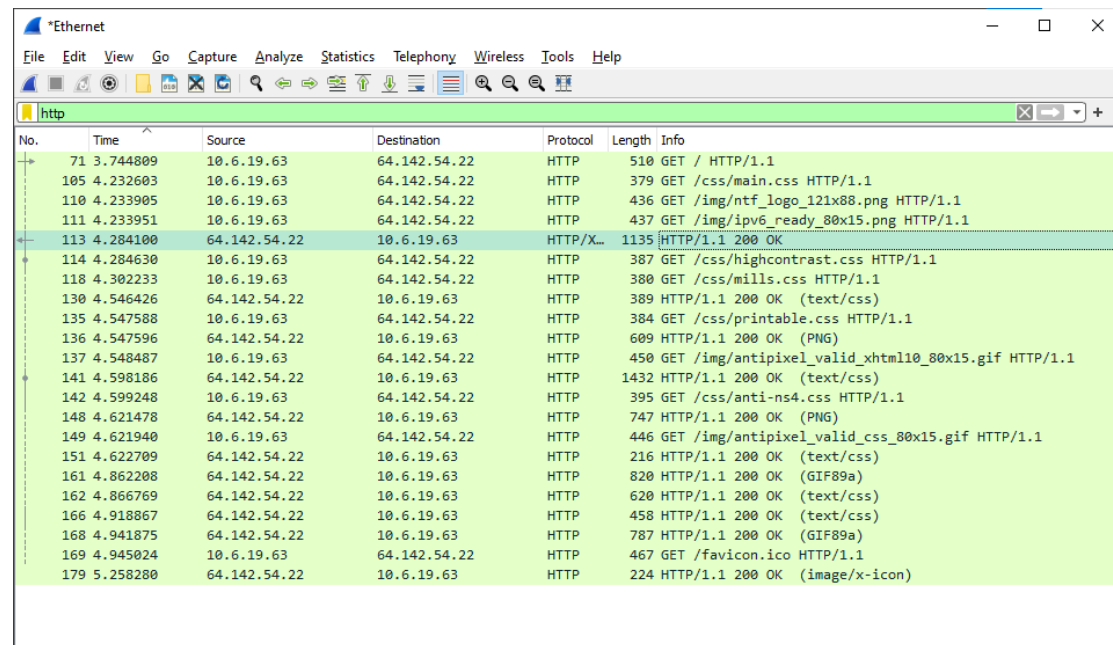
2. Which one contains the main source code for the web page? Could you tell this from the main capture window? How? *Hint: make sure the HTTP section is selected in the packet in the middle pane.*

HTTP/1.1 200 OK\r\n

I inferred this by sorting the packages by time and then looking at the first response that didn't start with GET (client to server communication), because

HTML is normally (always?) the first file that goes across from the server to the client. Likewise, OK indicates a success from the server to the client.

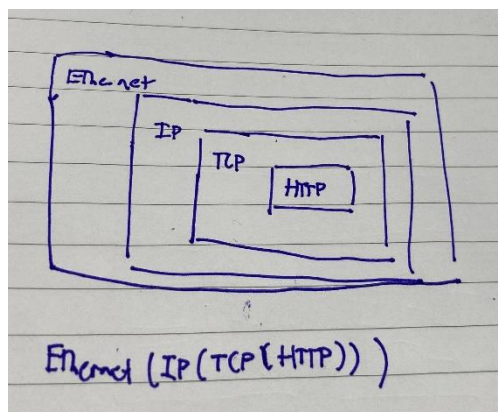
Similarly, the length was longer.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|-----------|--------|---|
| 71 | 3.744809 | 10.6.19.63 | 64.142.54.22 | HTTP | 510 | GET / HTTP/1.1 |
| 105 | 4.232603 | 10.6.19.63 | 64.142.54.22 | HTTP | 379 | GET /css/main.css HTTP/1.1 |
| 110 | 4.233905 | 10.6.19.63 | 64.142.54.22 | HTTP | 436 | GET /img/ntf_logo_121x88.png HTTP/1.1 |
| 111 | 4.233951 | 10.6.19.63 | 64.142.54.22 | HTTP | 437 | GET /img/ipv6_ready_80x15.png HTTP/1.1 |
| 113 | 4.284100 | 64.142.54.22 | 10.6.19.63 | HTTP/X... | 1135 | HTTP/1.1 200 OK |
| 114 | 4.284630 | 10.6.19.63 | 64.142.54.22 | HTTP | 387 | GET /css/highcontrast.css HTTP/1.1 |
| 118 | 4.302233 | 10.6.19.63 | 64.142.54.22 | HTTP | 380 | GET /css/mills.css HTTP/1.1 |
| 130 | 4.546426 | 64.142.54.22 | 10.6.19.63 | HTTP | 389 | HTTP/1.1 200 OK (text/css) |
| 135 | 4.547588 | 10.6.19.63 | 64.142.54.22 | HTTP | 384 | GET /css/printable.css HTTP/1.1 |
| 136 | 4.547596 | 64.142.54.22 | 10.6.19.63 | HTTP | 609 | HTTP/1.1 200 OK (PNG) |
| 137 | 4.548487 | 10.6.19.63 | 64.142.54.22 | HTTP | 450 | GET /img/antipixel_valid_xhtml10_80x15.gif HTTP/1.1 |
| 141 | 4.598186 | 64.142.54.22 | 10.6.19.63 | HTTP | 1432 | HTTP/1.1 200 OK (text/css) |
| 142 | 4.599248 | 10.6.19.63 | 64.142.54.22 | HTTP | 395 | GET /css/anti-ns4.css HTTP/1.1 |
| 148 | 4.621478 | 64.142.54.22 | 10.6.19.63 | HTTP | 747 | HTTP/1.1 200 OK (PNG) |
| 149 | 4.621940 | 10.6.19.63 | 64.142.54.22 | HTTP | 446 | GET /img/antipixel_valid_css_80x15.gif HTTP/1.1 |
| 151 | 4.622709 | 64.142.54.22 | 10.6.19.63 | HTTP | 216 | HTTP/1.1 200 OK (text/css) |
| 161 | 4.862208 | 64.142.54.22 | 10.6.19.63 | HTTP | 820 | HTTP/1.1 200 OK (GIF89a) |
| 162 | 4.866769 | 64.142.54.22 | 10.6.19.63 | HTTP | 620 | HTTP/1.1 200 OK (text/css) |
| 166 | 4.918867 | 64.142.54.22 | 10.6.19.63 | HTTP | 458 | HTTP/1.1 200 OK (text/css) |
| 168 | 4.941875 | 64.142.54.22 | 10.6.19.63 | HTTP | 787 | HTTP/1.1 200 OK (GIF89a) |
| 169 | 4.945024 | 10.6.19.63 | 64.142.54.22 | HTTP | 467 | GET /favicon.ico HTTP/1.1 |
| 179 | 5.258280 | 64.142.54.22 | 10.6.19.63 | HTTP | 224 | HTTP/1.1 200 OK (image/x-icon) |

Documentation Task 4.

1. Draw a diagram showing (in outline, don't worry about details such as how many bytes are used and fields in each packet) how the the IP, TCP and HTTP packets are contained within the Ethernet frame



Documentation Task 5.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message.

1. How many bytes long is the packet?

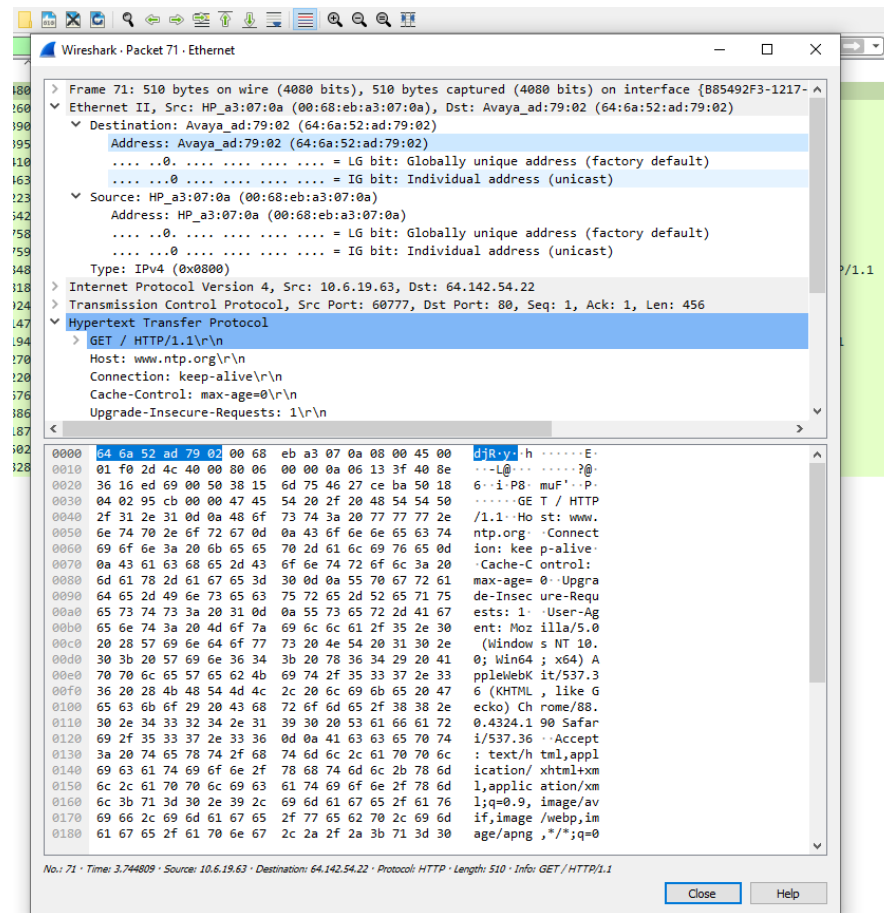
510 bytes

2. What is the 48-bit MAC address of your computer?

00-68-EB-A3-07-0A

3. 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.]

No – not sure, presumably whatever is next in the network relay – perhaps the mq switch that the network is connected to or the ISP. 64-6A-52-AD-79-02



4. What is the hexadecimal (shown by 0xnnnn) value for the two-byte “Type field” in the Ethernet header?

0x0800

5. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? *Hint: count the number of bytes in the raw packet pane at the bottom of the Wireshark window.*

54 bytes

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

6. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu? What device has this as its Ethernet address?

The hexadecimal value is 64-6A-52-AD-7D-02

Gaia.cs.umass.edu

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

00-68-EB-A3-07-0A

Yep

8. What is the hexadecimal value for the two-byte “Type field” in the Ethernet header?

0x0800

9. Is the OK in the HTTP message actually contained in the HTTP packet shown to you by Wireshark when you filter for HTTP packets? If not, where is it?

*Ethernet

Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|-----------|--------|----------------------|
| 71 | 3.744809 | 10.6.19.63 | 64.142.54.22 | HTTP | 510 | GET / HTTP/1.1 |
| 105 | 4.232603 | 10.6.19.63 | 64.142.54.22 | HTTP | 379 | GET /css/main.css HT |
| 110 | 4.233905 | 10.6.19.63 | 64.142.54.22 | HTTP | 436 | GET /img/ntf_logo_12 |
| 111 | 4.233951 | 10.6.19.63 | 64.142.54.22 | HTTP | 437 | GET /img/ipv6_ready_ |
| 113 | 4.284100 | 64.142.54.22 | 10.6.19.63 | HTTP/X... | 1135 | HTTP/1.1 200 OK |
| 114 | 4.284630 | 10.6.19.63 | 64.142.54.22 | HTTP | 387 | GET /css/highcontras |
| 118 | 4.302233 | 10.6.19.63 | 64.142.54.22 | HTTP | 380 | GET /css/mills.css H |

Destination Port: 60777
 [Stream index: 1]
 [TCP Segment Len: 1081]
 Sequence Number: 10118 (relative sequence number)
 Sequence Number (raw): 1177024063
 [Next Sequence Number: 11199 (relative sequence number)]
 Acknowledgment Number: 457 (relative ack number)
 Acknowledgment number (raw): 940928829
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x018 (PSH, ACK)
 Window: 1026
 [Calculated window size: 65664]
 [Window size scaling factor: 64]
 Checksum: 0xa18b [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > [SEQ/ACK analysis]
 > [Timestamps]
 TCP payload (1081 bytes)
 TCP segment data (1081 bytes)
 [8 Reassembled TCP Segments (11198 bytes): #74(1429), #75(1448), #83(1460), #84(1460), #85(1424)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 Response Version: HTTP/1.1
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK

Date: Thu, 04 Mar 2021 02:45:24 GMT\r\n
 Server: Apache\r\n
 Transfer-Encoding: chunked\r\n
 Content-Type: text/html\r\n
 \r\n

| | | |
|----|---|---------------------------------|
| 00 | 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d | HTTP/1.1 200 OK |
| 10 | 0a 44 61 74 65 3a 20 54 68 75 2c 20 30 34 20 4d | Date: Thu, 04 Mar 2021 02:45:24 |
| 20 | 61 72 20 32 30 32 31 20 30 32 3a 34 35 3a 32 34 | GMT |
| 30 | 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 | Se rver: Ap |
| 40 | 61 63 68 65 0d 0a 54 72 61 6e 73 66 65 72 2d 45 | ache |
| 50 | 6e 63 6f 64 69 6e 67 3a 20 63 68 75 6e 6b 65 64 | ncoding: chunked |
| 60 | 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 | Content-Type: |
| 70 | 74 65 78 74 2f 68 74 6d 6c 0d 0a 0d 0a 32 36 32 | text/html |
| 80 | 61 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e | version |

ame (1135 bytes) Reassembled TCP (11198 bytes) De-chunked entity body (11053 bytes)

Looks like it

10. Compare any Ethernet packet you have captured to the structure shown in lectures. Are they the same or, if there are differences, what are they?

Largely the same as far as I can tell.

