Data Communications Laboratory
Introduction to Wireshark

Your Name: Jai Carey

Your Student ID: 45188416

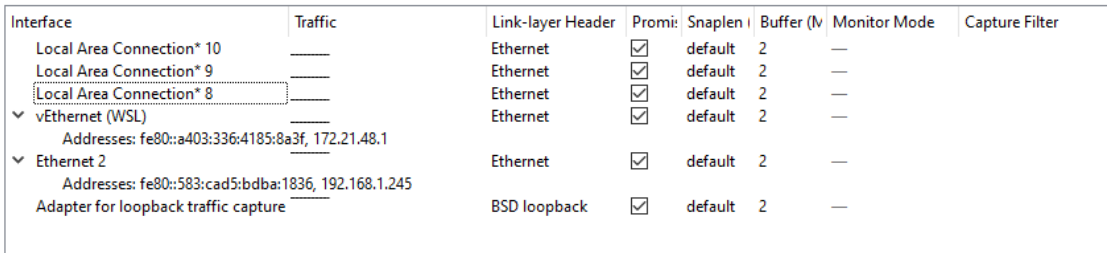
Documentation Task 1.

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.

From Wireshark:

vEthernet (WSL): fe80::a403:336:4185, 172.21.48.1

Ethernet 2: fe80::583:cad5:bdba, 192.168.1.245



Documentation Task 2.

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

From 'ipconfig /all':

IPv4 Address. . . . . : 192.168.1.245

MAC address. . . . . : 00-D8-61-37-31-DB

Documentation Task 3.

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

There is a total of 24 packets
12 Packets are HTTP GET requests to the destination IP address (sent from me)
12 packets were received

1730	7.760729	192.168.1.245	204.93.207.22	HTTP	397	GET / HTTP/1.1
1786	8.039712	204.93.207.22	192.168.1.245	HTTP/X…	368	HTTP/1.1 200 OK
1826	8.099050	192.168.1.245	204.93.207.22	HTTP	342	GET /css/main.css HTTP/1.1
1910	8.384743	204.93.207.22	192.168.1.245	HTTP	409	HTTP/1.1 200 OK (text/css)
1912	8.385020	192.168.1.245	204.93.207.22	HTTP	360	GET /img/ntf_logo_121x88.png HTTP/1.1
1913	8.385169	192.168.1.245	204.93.207.22	HTTP	370	GET /img/antipixel_valid_css_80x15.gif HTTP/1.1
1958	8.614029	192.168.1.245	204.93.207.22	HTTP	358	GET /css/anti-ns4.css HTTP/1.1
1967	8.622948	192.168.1.245	204.93.207.22	HTTP	374	GET /img/antipixel_valid_xhtml10_80x15.gif HTTP/1.1
1972	8.624554	192.168.1.245	204.93.207.22	HTTP	361	GET /img/ipv6_ready_80x15.png HTTP/1.1
1988	8.662097	204.93.207.22	192.168.1.245	HTTP	777	HTTP/1.1 200 OK (PNG)
1990	8.670106	204.93.207.22	192.168.1.245	HTTP	787	HTTP/1.1 200 OK (GIF89a)
2050	8.887788	204.93.207.22	192.168.1.245	HTTP	458	HTTP/1.1 200 OK (text/css)
2058	8.894009	192.168.1.245	204.93.207.22	HTTP	350	GET /css/highcontrast.css HTTP/1.1
2059	8.894618	192.168.1.245	204.93.207.22	HTTP	343	GET /css/mills.css HTTP/1.1
2060	8.895930	192.168.1.245	204.93.207.22	HTTP	347	GET /css/printable.css HTTP/1.1
2067	8.909539	204.93.207.22	192.168.1.245	HTTP	813	HTTP/1.1 200 OK (GIF89a)
2068	8.911751	204.93.207.22	192.168.1.245	HTTP	609	HTTP/1.1 200 OK (PNG)
2142	9.168615	204.93.207.22	192.168.1.245	HTTP	236	HTTP/1.1 200 OK (text/css)
2145	9.179318	204.93.207.22	192.168.1.245	HTTP	715	HTTP/1.1 200 OK (text/css)
2146	9.183290	204.93.207.22	192.168.1.245	HTTP	620	HTTP/1.1 200 OK (text/css)
2150	9.187554	192.168.1.245	204.93.207.22	HTTP	368	GET /img/apple-touch-icon-iphone.png HTTP/1.1
2151	9.187903	192.168.1.245	204.93.207.22	HTTP	348	GET /favicon.ico HTTP/1.1
2278	9.460650	204.93.207.22	192.168.1.245	HTTP	249	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
2297	9.477161	204.93.207.22	192.168.1.245	HTTP	670	HTTP/1.1 200 OK (PNG)

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.*

The grey highlighted row is the main source code for the web page. That packet includes an HTML file which includes all of the content and general structure of the web page.

2 rows below show another HTTP GET request for the css of the web page, these are the styles of the webpage and make the make the HTML prettier.

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

From Lecture 1 Part 2:
(Ethernet (IP (TCP (HTTP (Request)))))

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?

The packet is 446 bytes in length.

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

My 48-bit MAC address is (00:d8:61:37:31:db)

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.]

The 48-bit destination MAC address is (e4:c3:2a:98:3b:74)
This could be the MAC address of the router between the webserver, or a switch, or a load balancer, or any similar networking device on the server side.

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

The hexadecimal for the Type Field is 08 00

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.*

The ASCII "G" from "GET:" is only 1 byte (47 in hex). There are 2 hex values per byte, and usually, an ASCII is 1 byte in length.

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 source address is (e4:c3:2a:98:3b:74)

In the response message, the source is the website, we are the destination
As we are receiving the packet, we cannot be source.

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

The destination address is (00:d8:61:37:31:db)

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

The hexadecimal for the Type Field is 08 00

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?

Yes, this is contained within the packet.

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?

They are the same as in the lecture.