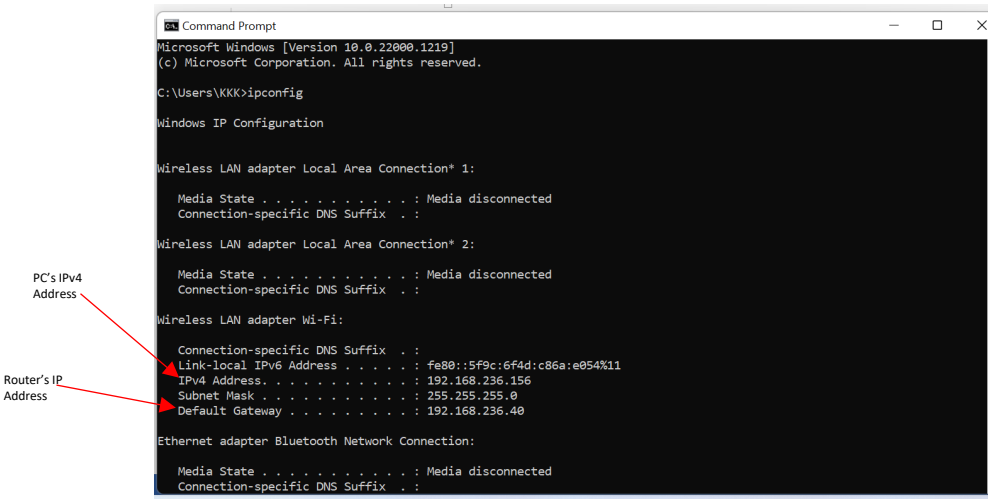
CS 4404 – Written Assignment 4 Instructions

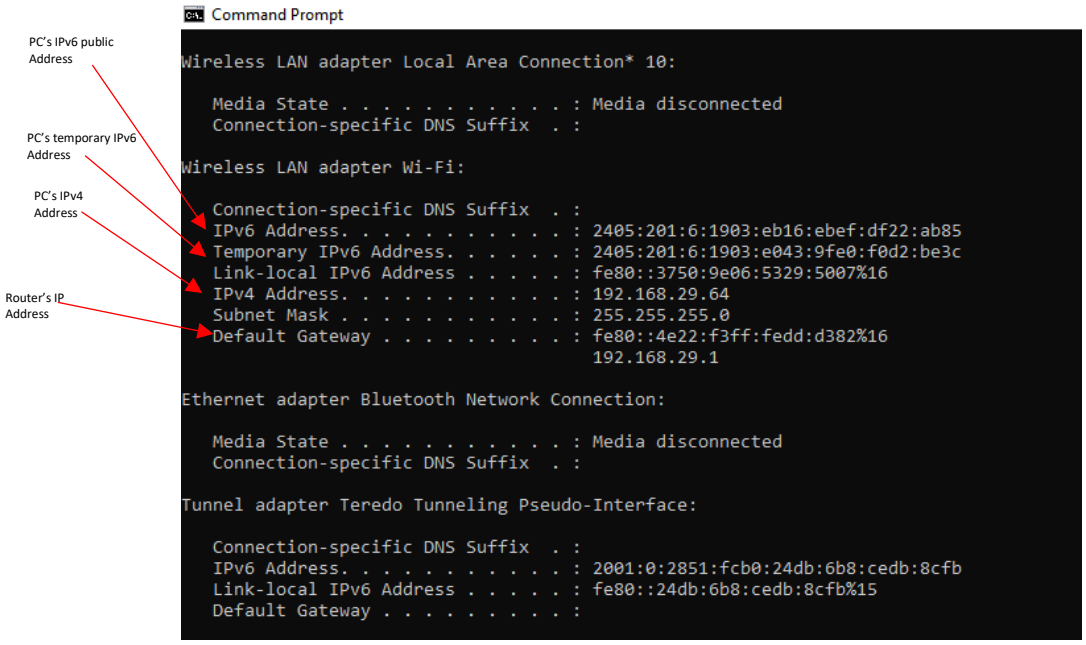
Follow the instructions below to help you carry out the assignment:

I. Before you begin, note down the IP address of your PC and that of the website you are browsing to. To get your PC's IP address, simply open the command prompt in Windows OS and type the following command: **ipconfig.** To access your PC's IP address on other OS platforms (MacOS and Linux) please follow the link: https://geekflare.com/find-ip-address-of-windows-linux-mac-and-website/

II. Above command will display the IP configuration on your PC. Note the IP address on your active network card which can be of either *Ethernet adapter Ethernet* or *Wireless LAN adapter Local Area Connection* or *Wireless LAN adapter Wi-Fi* or *Ethernet adapter Bluetooth Network Connection* or whichever type of internet connection is supported by your PC (the below screenshot shows the *Wireless LAN adapter Local Area Connection* type). You will also notice several parameters including subnet mask, default gateway IP (usually a router acting as your gateway), and so on.



Note: In some cases, there is a possibility of it showing the IPv4 addresses along with the public IPv6 address as well as the temporary IPv6 addresses as shown in the below example screenshot:

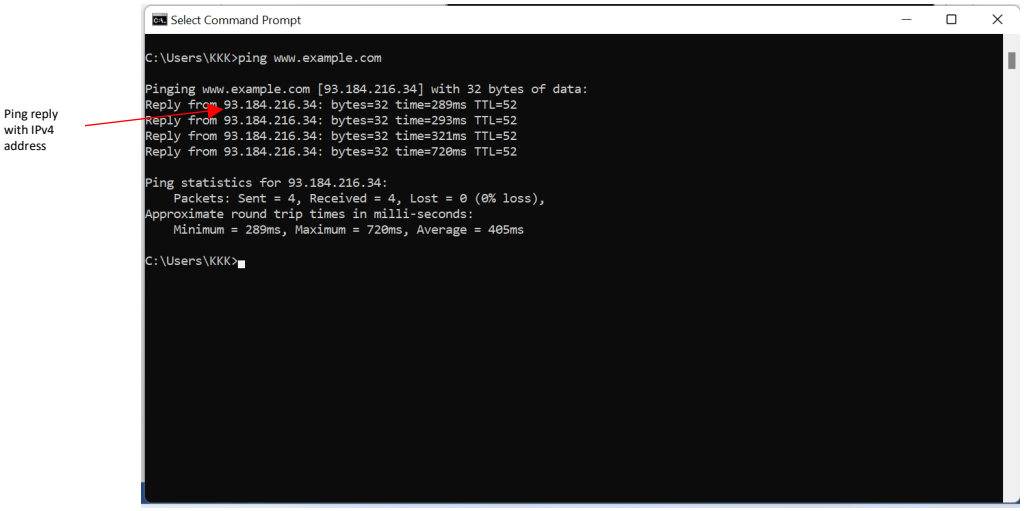


- In such cases, make a note of these IPv6 public and temporary addresses as well because, in the later steps, the commands might have to be modified accordingly.
- The following two readings will help you understand why and when an IPv4 or IPv6's public or temporary addresses exist or are used:
    - https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6
    - https://www.networkacademy.io/ccna/ipv6/ipv6-on-windows

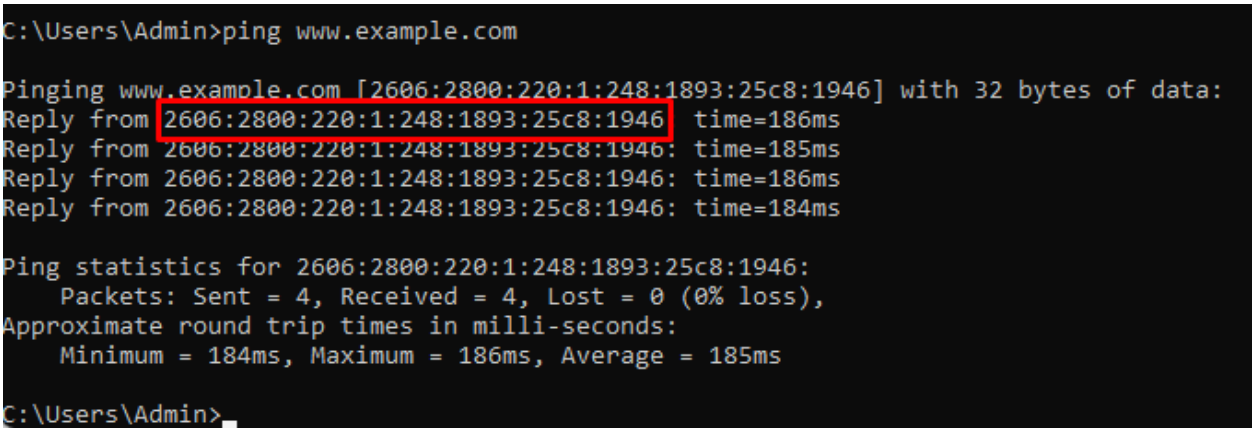
III. To get the IP address of a website, simply run a ping test to that website address.

a. In the command prompt, type the following command: ping www.example.com

b. Notice the ping reply comes with the IP address of the website (see the below screenshot). Note the website IP address.



- For those who see the reply ping from the website's IPv6 address like the below sample screenshot should make a note of the same:



IV. We shall be using an unsecured website (unsecured *http* as against secure *https*) for the first demonstration to see how information exchange with unsecured websites behaves. The IP addresses collected in (II) and (III) above will be used to verify results in Wireshark.

V. Open your preferred web browser and clear the web browser cache (visit the https://its.uiowa.edu/support/article/719 link for instructions on how to clear the web browser cache). It is advised that you clear the web browser cache each time you want to carry out this process.

VI. Close the web browser and all other open windows.

VII. Launch Wireshark.

VIII. Once the Wireshark is open and running, it will display all network interfaces on your computer. Please choose the appropriate interface (WiFi for the wireless interface or Local LAN for the wired interface). Please pay close attention to the interface and choose only the interface with network activity (indicated by the graph lines in front of the interface).

IX. Double-click on the chosen network interface (card). Network capture begins automatically. Notice that there may or may not be any activity recorded/displayed by Wireshark.

X. Relaunch the web browser and browse to http://www.example.com/ (you are expected to only browse to the website. Do not carry out any other activities on the website).

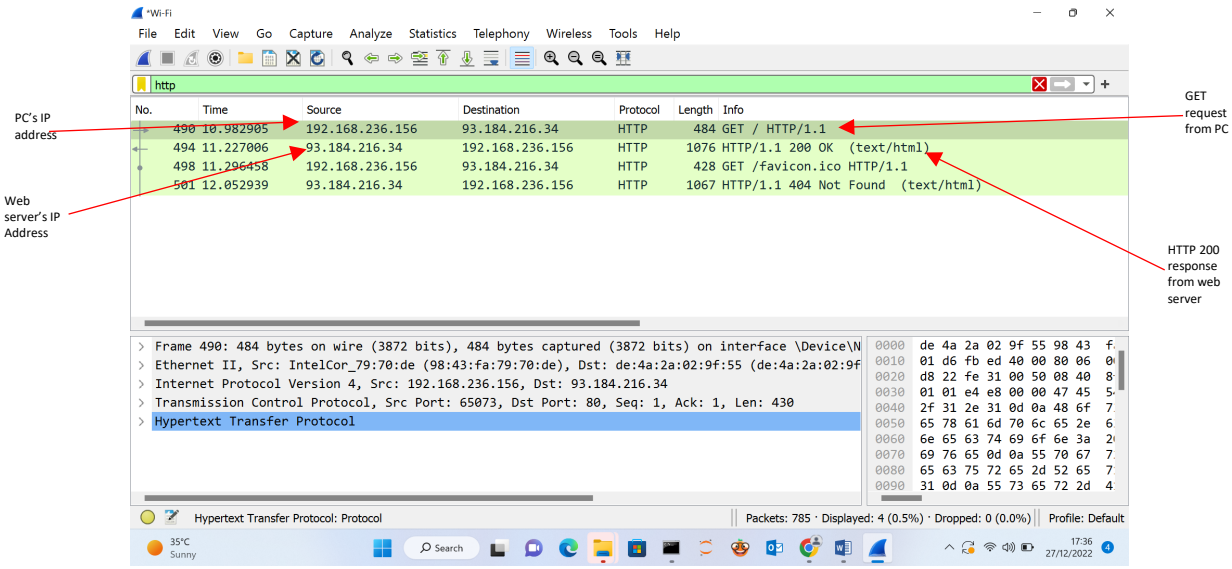
XI. Now ping www.example.com by using the command: ping www.example.com

XII. Once the ping is complete, head back to the Wireshark interface to stop and save the capture. Explore the data packets captured as listed in the packet list pane. Notice that different types of protocols were captured (DNS, TCP, TLS, HTTP, and so on). Notice the total number of packets captured at the bottom right corner of the Wireshark interface.

XIII. We shall now filter for HTTP packets. In the Filter Toolbar, type http (lower case) and hit enter or click on the arrow button at the right end of the Filter Toolbar. This will display only HTTP packets.

XIV. Notice that the IP addresses displayed contain that of your PC and the website. Also notice the HTTP protocol in action: the GET request sent to the web server requesting for service, the OK response from the web server, and the web content sent (see the below screenshot). For more on HTTP status codes, please visit: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

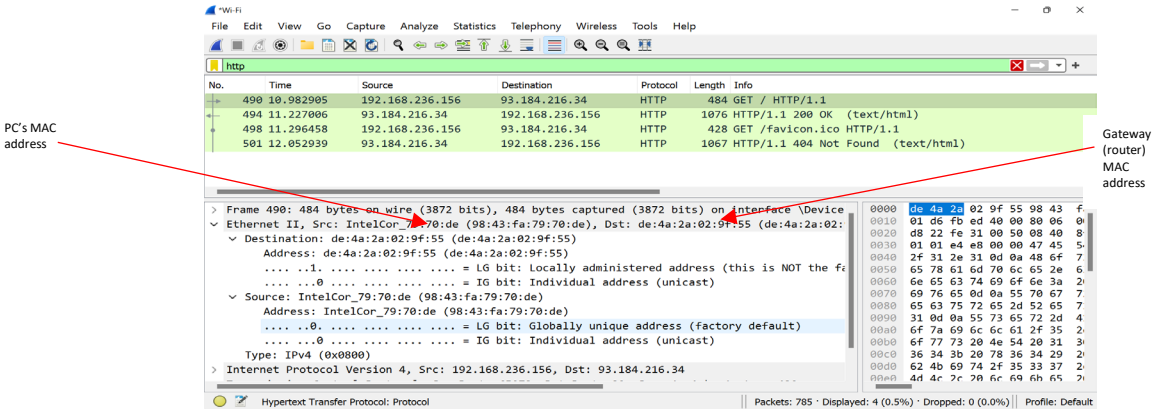
XV. Let us now explore elements in the Packet Details Pane.



XVI. Click on the first GET request sent (should usually be the first displayed in the pane. Look at the Packet List Pane, typically, for major sections of information can be seen, namely (see the above screenshot):

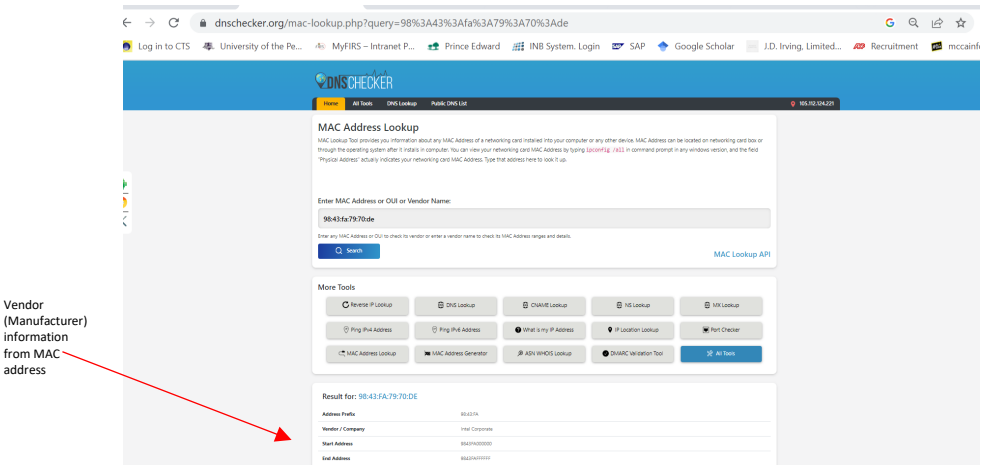
a. **Frame**: Expanding this first section gives you physical layer details about the packet. We will not be reviewing this section.
b. **Ethernet**: Expanding this second section gives the data-link layer (layer 2) information about the packet.
c. **Internet Protocol**: Expanding this section gives layer 3 information about the packet.
d. **Transmission Control Protocol**: Expanding this section gives TCP information about the packet.
e. **Hypertext Transfer Protocol**: Expanding this section gives HTTP information about the packet

XVII. Click on the arrow in front of the **Ethernet** to expand it. You will see several layer-2 information including the MAC address of your PC (**Src: xx:xx:xx:xx:xx**) - the SOURCE MAC address and the MAC address of your gateway/router (**Dst: xx:xx:xx:xx:xx**) - the DESTINATION MAC address (see the below screenshot).

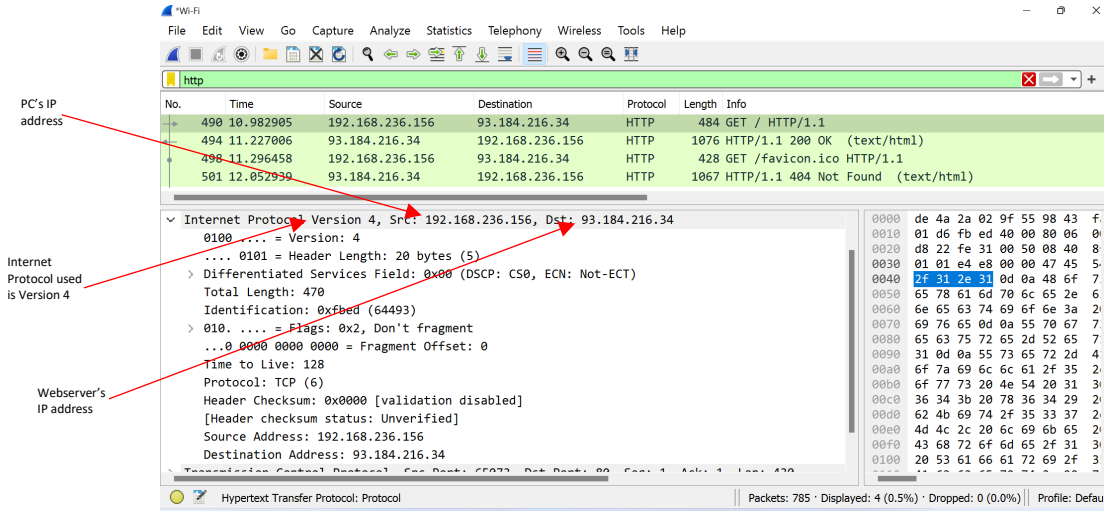


XVIII. The first 3 sets of hexadecimal digits in the MAC address represent the vendor/manufacturer. To look up manufacturer information of a networking device using its MAC (physical) address, you can use any MAC address lookup website. For instance: https://dnschecker.org/mac-lookup.php?query=98%3A43%3Afa%3A79%3A70%3Ade

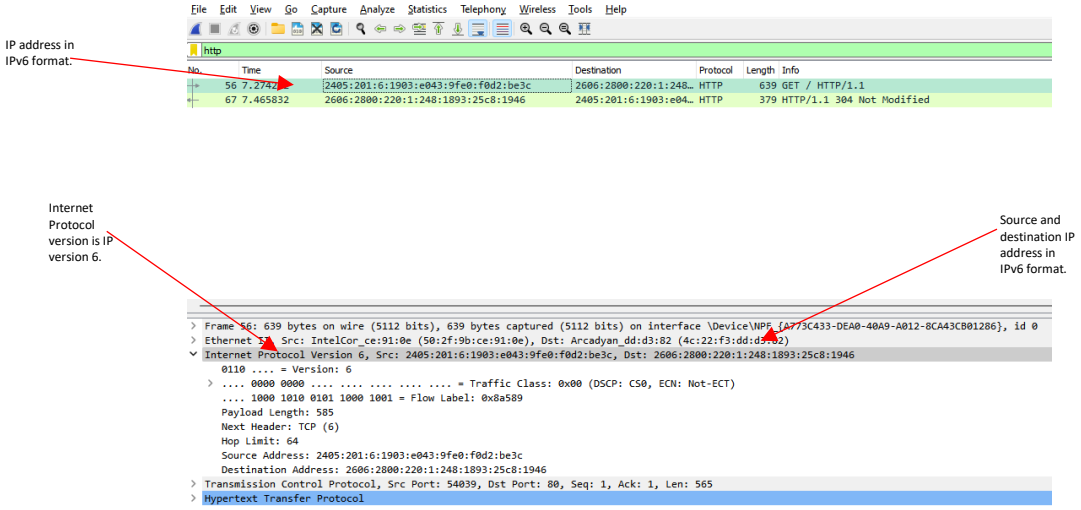
Type in the entire MAC address (as it appears) and click on the search button. It will give you several information including: Vendor/Company name, Company Address, and MAC address range (start and end address). See the below screenshot.



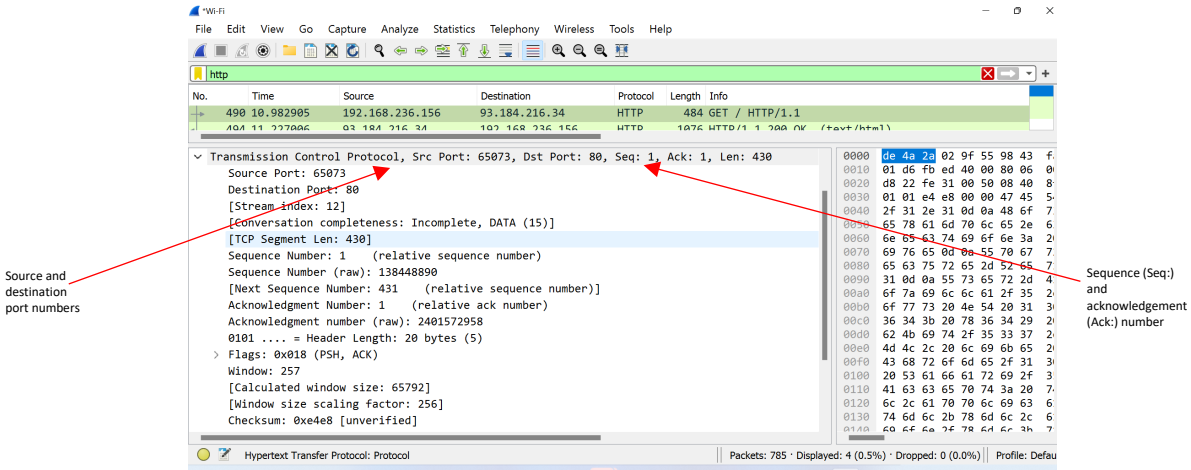
XIX. Next, click on the arrow in front of **Internet Protocol** to expand it. Notice the first line shows you that this is IPv4 (or IPv6 depending on your network connection as explained in steps II and III) and then gives you the IP address of your PC (**Src: X.X.X.X**) and the IP address of the webserver (**Dst: X.X.X.X**). You can crosscheck your PC IP address with the one you got from the command prompt. Other relevant information which may be seen includes flags, Time-To-Live, and header checksum information (see the below screenshot).



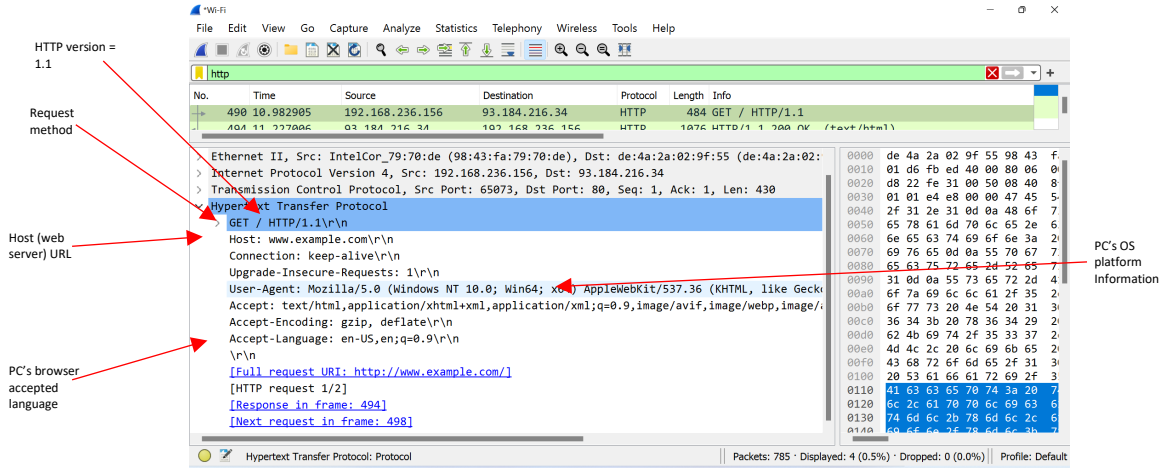
- Depending on your PC/network device/connected network, your IP address may be purely IPv6. In this case, you will notice the Internet protocol version is IPv6, and all displayed IP addresses are in IPv6 format as shown below:



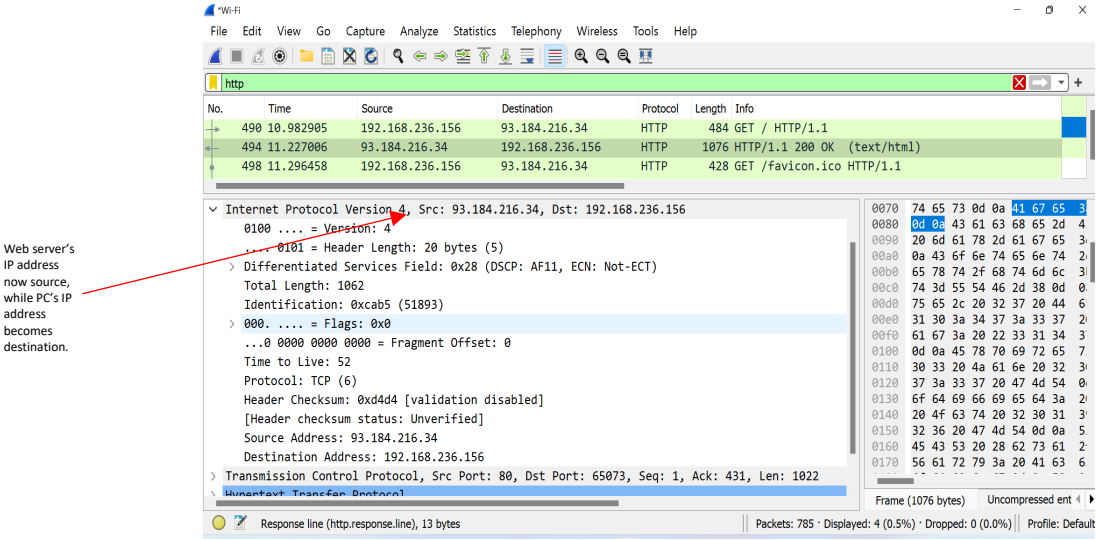
XX. Next, click on the arrow in front of **the Transmission Control Protocol.** Notice the first line gives information about what TCP port numbers are used (source and destination port numbers). It also gives the Sequence number (Seq:) and acknowledgment number (Ack:). Other visible information includes TCP Segment length (TCP Segment Len:), Sequence number, Acknowledgement number, Flags, Checksum information, and TCP payload size (see the below screenshot).



XXI. Next, click on the arrow in front of **the Hypertext Transfer Protocol**. Here, several information is displayed including the HTTP version, the Request method, the request version, the Host (webserver) URL, and User agent information, which gives information as per your PC's OS platform. In the below screenshot, it is Windows NT 10.0, Win64, x64 (Windows 10 OS and 64-bit PC). It also gives information as to what language your PC browser is configured (**Accept-Language**) for among other information. See the below screenshot:



XXII. We have explored an HTTP data packet sent from your PC to the server. Now let us examine the response from the webserver to PC. Click on the next line with the HTTP response (see the below screenshot). The source IP should be the web server IP, while the destination IP should be your PC IP address.

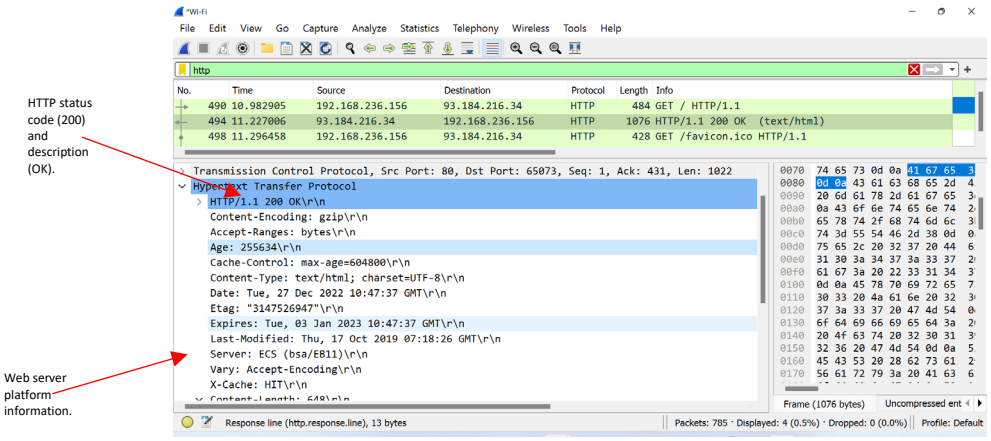


XXIII. Notice that the IP address information under Internet Protocol (in the Packet Details Pane) has changed, with Source IP as the web server's IO and your PC as the destination IP. Explore and compare packet details information with the first get packet sent by your PC.

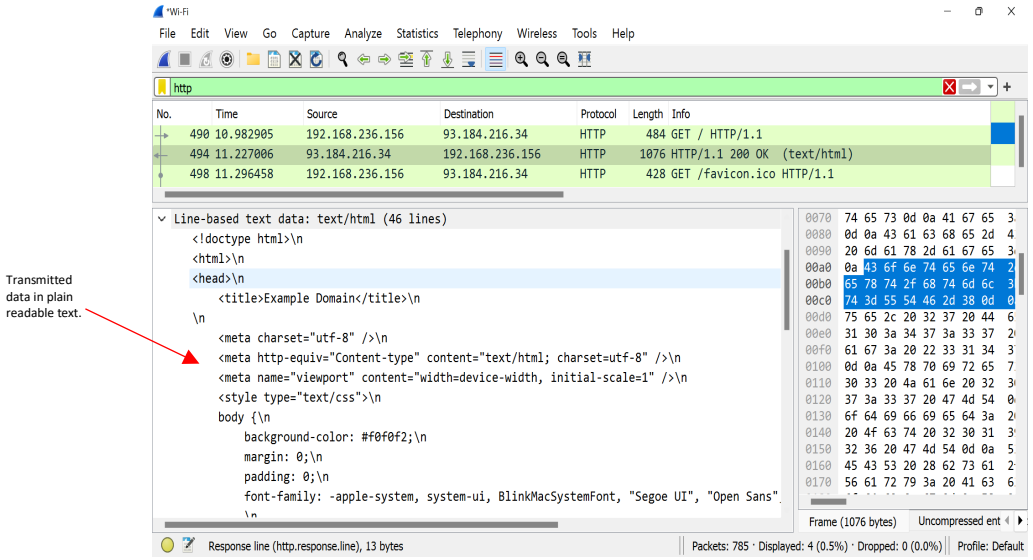
XXIV. Next, navigate to **Hypertext Transfer Protocol** in the packet details pane. Here, you will find several useful information including (see the below screenshot):

a. Status code and code description for the transmission (see this URL for more information on HTTP status codes: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status)

b. Web server platform information and more.



XXV. Scroll down and you will get to the last information entry: **Line-base text data**. Click on the arrow to see the transmitted information in the plain readable text (see the below screenshot). HTTP transmissions are unsecured, since they are transmitted in plain text and can be read by anyone who can intercept the message. This is the reason why it is recommended that HTTPS protocol be used, which encrypts all transmissions before sending them through the public network (Internet). See the below screenshot:



XXVI. To see the TCP 3-way handshake, we need to filter for TCP packets to and from the computer/web server. This can be achieved by executing the desired Wireshark expression command in the filter toolbar. Before you do so, ensure that the current filter on http is cleared (use the red cross near the arrow button shown in the above screenshot) else the new command will act as a sub-filter.

Now, you may use the following command (with appropriate modifications as prescribed in this step): **ip.addr eq 192.168.236.156 and ip.addr eq 93.184.216.34** (or use the command **ip.addr == 192.168.236.156 and ip.addr == 93.184.216.34** for some cases and make sure everything is in lowercase) please note that you may need to type this in rather than copy-and-paste if the command does not work. Here, 192.168.236.156 is my PC address, while 192.168.236.156 is the web server address. If you have only IPv6 addresses, please use the command with the following syntax:

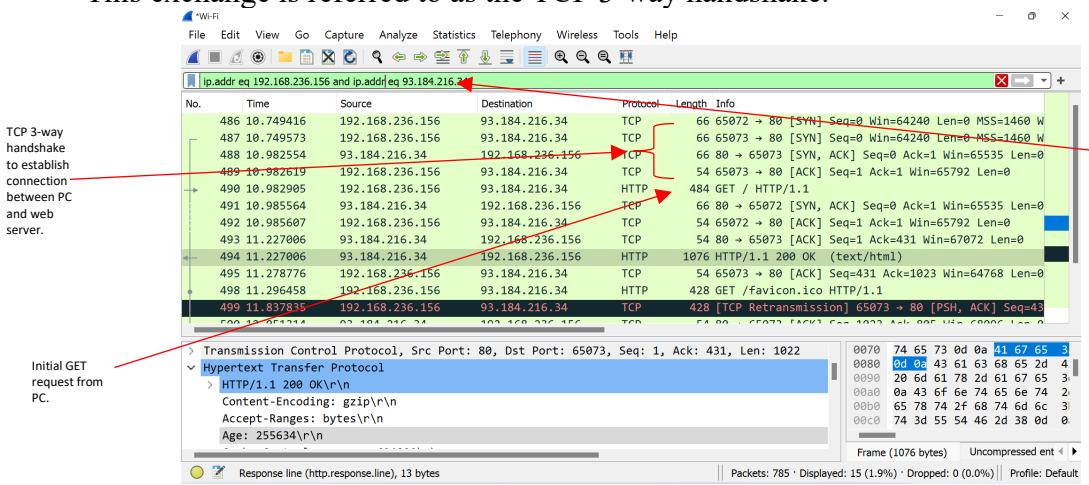
ipv6.addr eq 2405:201:6:1903:e043:9fe0:f0d2:be3c and ipv6.addr eq 2606:2800:220:1:248:1893:25c8:1946 (or use the command **ipv6.addr == 2405:201:6:1903:e043:9fe0:f0d2:be3c and ipv6.addr == 2606:2800:220:1:248:1893:25c8:1946** for some cases and make sure everything is in lowercase) please note that you may need to type this in rather than copy-and-paste if the command does not work. Here, the first IPv6 address represents the source's temporary IPv6 address (try a public IPv6 address if this doesn't work as temporary IPv6 might not be enabled/available), while the second represents the destination's IPv6 address.

For more information on how to write an expression to filter packets in Wireshark, please visit the following website: https://www.hypack.com/File%20Library/Resource%20Library/Technical%20Notes/04_2022/Troubleshooting-Using-Filters-in-Wireshark.pdf

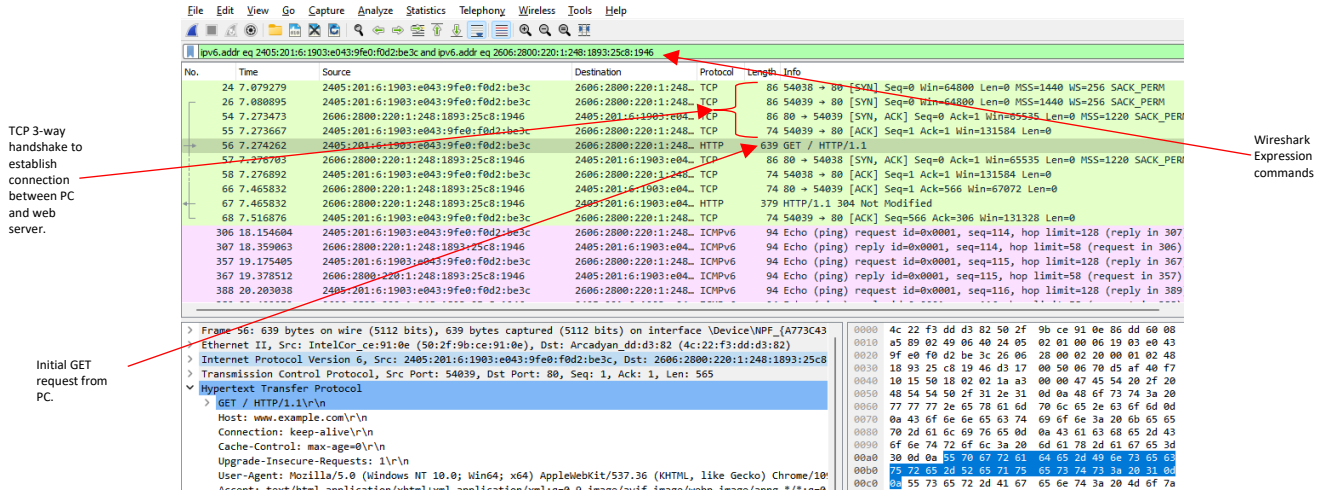
XXVII. In the packet line pane, notice that a TCP 3-way handshake is needed to establish a connection between your PC and the web server before the first GET transmission was made by your PC to the web server (see the below screenshots). The following TCP information was exchanged to establish the connection:

a. SYN, from my PC to the server
b. SYN, ACK from the server to my PC
c. Ack, from my PC to the server.

This exchange is referred to as the TCP 3-way handshake.



- Refer to the below screenshot for the IPv6 one:



XXVIII. For more information on HTTP traffic analysis, please visit the following website https://linuxhint.com/http_wireshark/

Submit a paper that is double-spaced using 12-point Times New Roman font. The paper must be well-written. Check all content for grammar and spelling.
For this assignment, your peers will be evaluating your work using the Written Assignment Unit 4 Rubric.

References:

- Bermudez, C. (2022, April). *Troubleshooting using filters in wireshark*. HYPACK. https://www.hypack.com/File%20Library/Resource%20Library/Technical%20Notes/04_2022/Troubleshooting-Using-Filters-in-Wireshark.pdf
- *Example Domain*. (n.d.). Example. https://www.example.com/
- Ghosh, B. (n.d.). *HTTP analysis using Wireshark*. Linux Hint. https://linuxhint.com/http_wireshark/
- *How to clear the cache and cookies in your web browser*. (2022, April 27). Information Technology Services. https://its.uiowa.edu/support/article/719
- *HTTP response status codes*. (2022, September 15). MDN Web Docs. https://developer.mozilla.org/en-US/docs/Web/HTTP/Status
- *IPv4 vs IPv6 - Understanding the differences*. (n.d.). NetworkAcademy.io. https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6
- *IPv6 on Windows*. (n.d.). NetworkAcademy.io. https://www.networkacademy.io/ccna/ipv6/ipv6-on-windows
- *MAC address lookup*. (n.d.). DNS Checker. https://dnschecker.org/mac-lookup.php
- Nair, A. (2022, October 29). *How to find IP address of Windows, Linux, Mac and website?* Geekflare. https://geekflare.com/find-ip-address-of-windows-linux-mac-and-website/