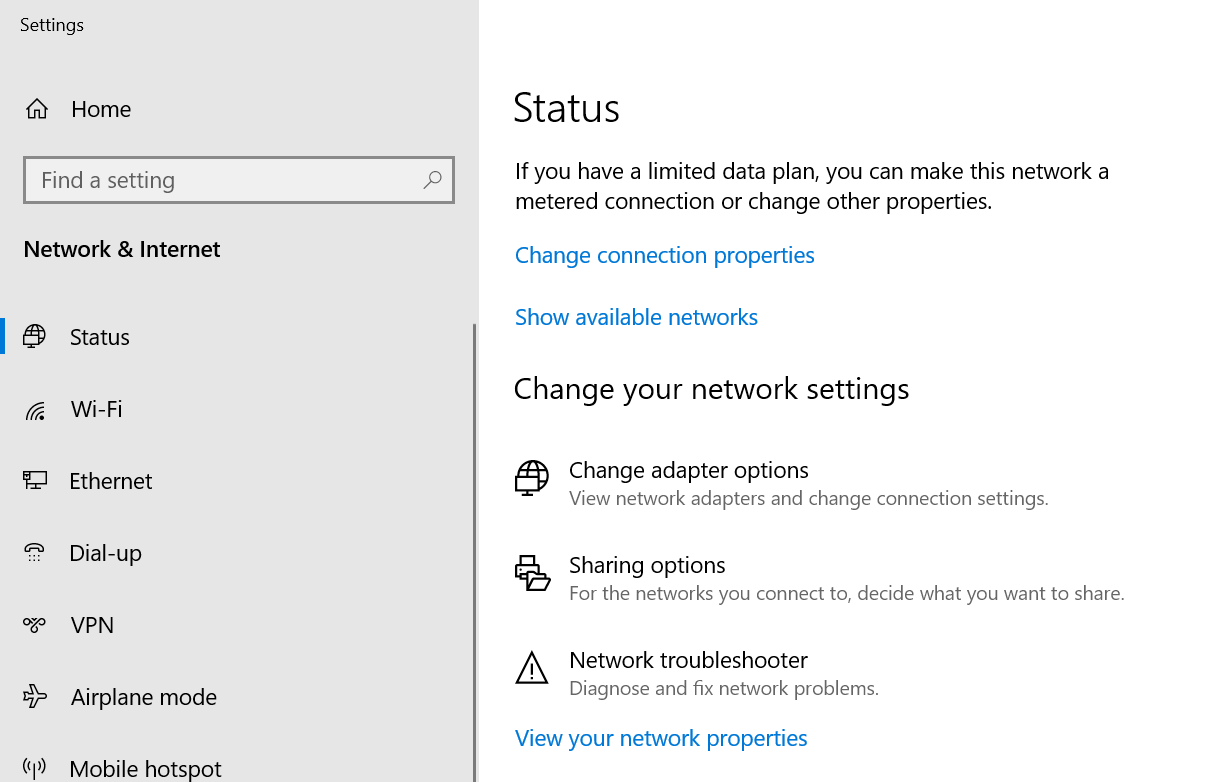
**IT 250 Fundamentals of Information Assurance and Security**

**Assignment 4 - Wireshark**

**Objective:** Get familiar with Wireshark and use it to capture and analyze network traffic packets.

Record the network addresses and gateway to your network on your machine. On Windows 10, the easiest way to do this is to open Network & Internet Settings, and click on the “View your network properties” link as shown below:



If you are using a Mac, go to Network Preferences, select the Wi-Fi network, and then click “Advanced” and use the tabs to find the following information. (3 pts):

Device IPv4 address: **192.168.4.57/22**

Subnet mask: **255.255.252.0**

Device MAC address: **34:98:b5:a3:13:88**

DNS Server address: **206.225.75.226, 206.225.75.225**

DHCP Server address: **192.168.4.1**

Default gateway address: **192.168.4.1**

Question 1: Why does a device need both IP and MAC addresses (3 pts)?

**IP addresses and MAC addresses both serve different roles when it comes to being on a device. Each device needs both because MAC addresses are how devices can be identified within local network communication, and IP addresses is used globally.**

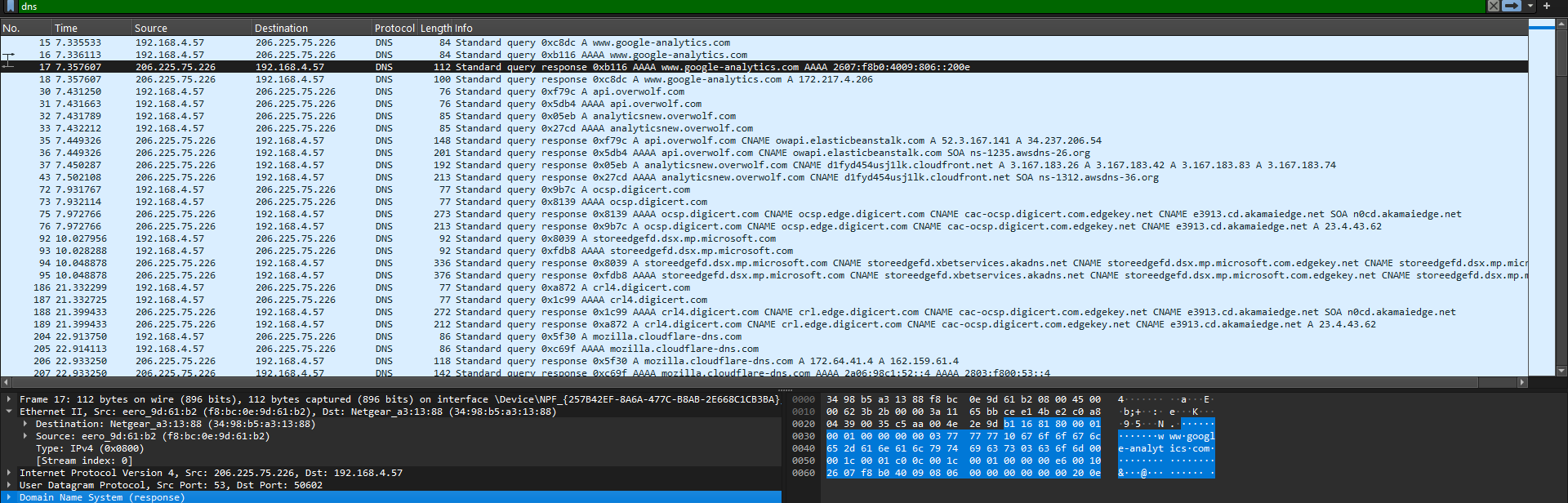
Download and install Wireshark from <https://www.wireshark.org/#download>. Once you have read the tutorial, carry out the steps outlined in the rest of the document.

Watch [this video](https://www.youtube.com/watch?v=lb1Dw0elw0Q) to familiarize yourself with Wireshark and how to use it. You may also go through Wireshark tutorial available at <https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>

Note 1: You may include Wireshark screen shots for the questions below. Please ensure that the screen shots are large enough to be viewed in the document.

Note 2: Try to minimize all other network activity while you do this assignment. This way, the capture set that contains the packets that you need to inspect is not polluted by unwanted packets.

1. **Domain Name Service (DNS)**
2. Start up the Wireshark packet sniffer (but don’t yet begin packet capture). Enter “dns” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured DNS messages will be displayed later in the packet-listing window. Start packet capture.
3. Open the Firefox browser. Type [www.google.com](http://www.google.com) and press enter. You should see some activity in the Wireshark window. Stop Wireshark capture by clicking on the red square icon.
4. Find the DNS query and response packets in the Wireshark window, and insert a screenshot containing both the request and response here (3 pts).



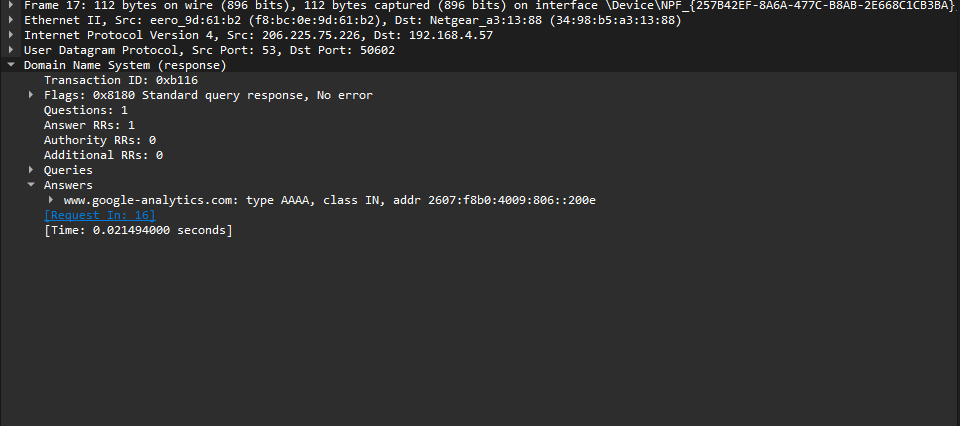
Question 2: To which server (IP address) did your device send the above DNS request to? Explain (3 pts)?

**192.168.4.57**

Question 3: What transport protocol does DNS use? What is the DNS server port number (3 pts)?

**It uses UDP, and the source port is 53, and the destination port is 50602**

Question 4: What is the purpose of the DNS request and response? Insert a screen shot of the “answer” contained in the DNS response (3 pts).



1. **Ping and ICMP**
2. Clear the previous capture filter and type “icmp” as the new filter.
3. Open a command prompt/terminal window, type “ping [www.yahoo.com](http://www.yahoo.com)” without the quotes and press enter.
4. You should see ICMP packets in the Wireshark window.

Question 4: What is the purpose of the ping tool? Why do you need this tool (3 pts)?

**The ping tool allows network devices to be tested for reachability, and how long it may take for data to travel between the source and destination. It is important to have this tool because it helps with network connectivity testing, troubleshooting, and error checks for firewalls.**

Question 5: What protocol does the ping tool use? Explain (3 pts)?

**The ping tool uses ICMP. This protocol is used for error reporting and network diagnostics. TCP and UDP are not used for those types of events.**

1. **ARP**
2. Clear the previous capture filter and enter “arp” as the new filter. Start a new Wireshark packet capture.
3. Ping your default gateway and ensure that you get responses back from it. Open a command line prompt as administrator. In the command prompt, type the command “arp -a” without the quotes. This will display the ARP table. Locate the gateway’s IP address in the table returned by the command, and the corresponding MAC address.
4. Now, type the command “arp -d gateway-ip-address” (replace “gateway-ip-address” with the actual IP address of the gateway). This will delete the gateway’s row from the ARP table.
5. Once the command completes, ping the default gateway again. After the responses are received, stop the Wireshark capture. You should see some activity in the Wireshark window.
6. Locate the ARP request and response for the gateway and insert a screenshot of the request and response here (3 pts).

Question 6: What is the purpose of the ARP protocol? What does the ARP response contain (3 pts)?

**The ARP protocol includes a map of the MAC and IP address layers within a local network. This allows devices to communicate over wifi. It contains the senders MAC address and IP address, as well as the receivers MAC and IP address.**

1. **The Basic HTTP GET/response interaction**
2. Use Firefox for this part.
3. Clear the previous capture filter and enter “http” as the new filter. Start a new Wireshark packet capture.
4. Enter the following to your browser: <http://web.simmons.edu/~grovesd/comm244/notes/week2/links>.
5. Your browser should display a very simple page with some text and an image. You should see some activity in the Wireshark window. Stop Wireshark packet capture when the web page has loaded.

Question 7: How many HTTP GET requests were sent by your browser? What are these requests trying to “get” (3 pts)?

**There were 2 HTTP GET requests sent by my browser. Looking at the requests, they say GET /~grovesd/com244/notes/week2/links. HTTP/1.1 which is the link that was entered into the browser. The second request included GET /favicon.ico HTTP/1.1, which represents the website that was searched.**

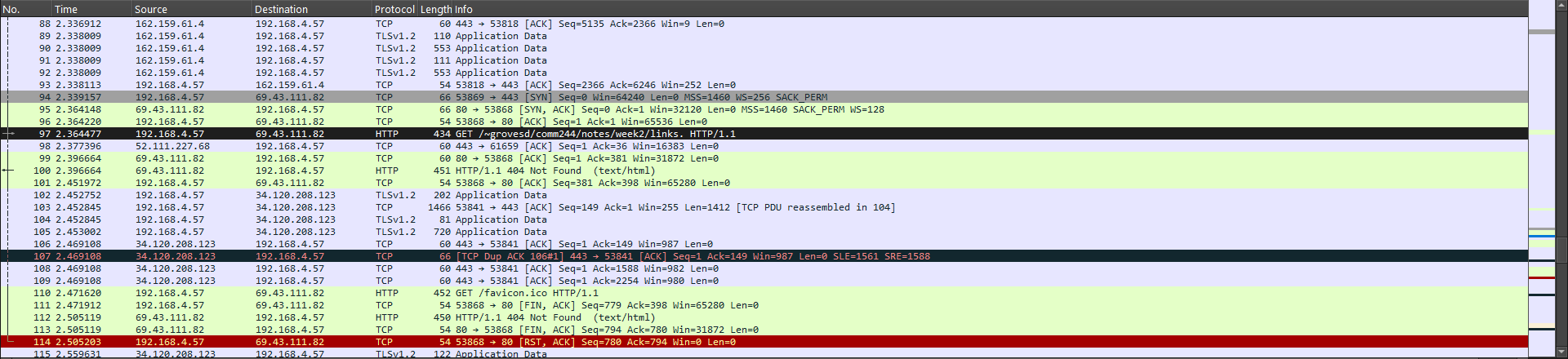
Question 8: What is the data contained in the HTTP response to the first GET request (3 pts)?

**The hypertext transfer protocol includes HTTP/1.1 404 Not Found\r\n, which is the response version, and status code. The line-based txt data is text/html (7 lines).**

Question 9: What transport protocol does HTTP use? What is the server port number (3 pts)?

**It uses TCP, and the server port number is 53868(Source) 80(Destination)**

Click on the first GET request to select it. Clear the capture filter to show “non-HTTP” packets captured before this packet. Insert a screenshot of the connection packets from your device to the server to send the GET request and insert it here (3 pts).



Question 10: How many unique connections were opened for the transfer of the page with the image to your browser (Hint: each connection will have a unique port number for the sender) (3 pts)?

**6**