**Julia Kovrigin**  **CTP 103**

# Lab 5: Local Area Networks (40 points) PC Version

Objectives:

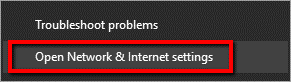
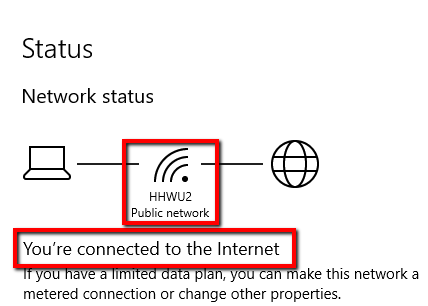
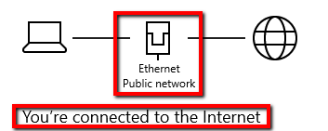
* View network settings and network traffic
* Use the command prompt to view network status and connections

##### Section I. View Network Settings – 18 points

*You must do this lab on your own computer. For essay questions, if you copy and paste answers, you will earn a zero for the question.* All answers are 1 point unless indicated otherwise.

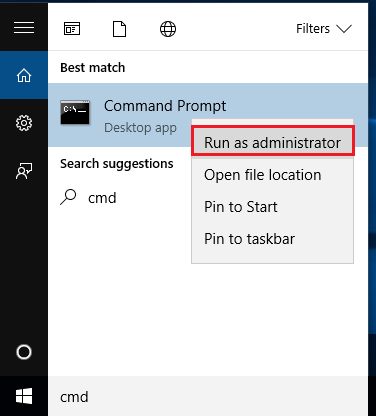
Note: you will be creating several screenshots in this lab. [Click here](https://youtu.be/2O932t8-k2A) to learn how to use the Snipping Tool.

#### Network and sharing Center – Graphical User Interface (GUI)

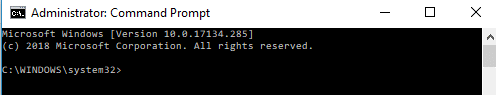
1. Enter your name and section number at the top of the document
2. Open the **Network and Sharing Center**: right click on the Network icon on the task bar (image on right) and select **Open Network and Internet settings.**
3. Select Status (if necessary) and scroll down and click on **View your network properties.** Verify that you are connected to the Internet either wirelessly or through Ethernet (wired).
4. Scroll down and click **View your network properties.** If you are connected via an Ethernet connection, you will find the properties for Ethernet. If you are connected via Wi-Fi, you will scroll to find the properties for the Wi-Fi connection. Note: the active adapter will show “Operational” under “Status”.
   1. Identify the following settings (**1 point each**):
      1. Connection-specific DNS Suffix (this will be your router name): fios-router.home
      2. Physical Address (this is the MAC address) 9c:b6:d0:ea:5d:6d
      3. IPv4 IP address: 192.168.1.185/24
      4. Subnet mask: 255.255.255.0
      5. Default Gateway: 192.168.1.1
      6. DHCP server IP Address: 192.168.1.1
   2. Define the following terms (**2 points each**):
      1. MAC Address: Mac address is the NCIs address, it is a unique address used to identify devices on LAN. This is the address that is programmed by the manufacturer in device hardware. It cannot be changed.
      2. Subnet Mask: Is a 32-bit number that masks an IP address, and divides the IP address into network address and host address.
      3. Default Gateway (be sure to include what it does): serves as an access point or IP router that a network computer uses to send information to a computer in another network or the internet.
      4. DHCP server (be sure to include what it does): Is a Dynamic Host Configuration Protocol, is a network management protocol use on UPD/IP networks. The server assigns an IP address and other network configurations to each device.
      5. DNS (be sure to include what it does): Domain Name Server. There are several of these servers around the world. They store all the domain names and corresponding IP addresses. When a router send the domain name to the DNS, the DNS find the corresponding IP address and sends that information back to the asking router. That is how we get to get to the correct websites.

#### Windows command line interface

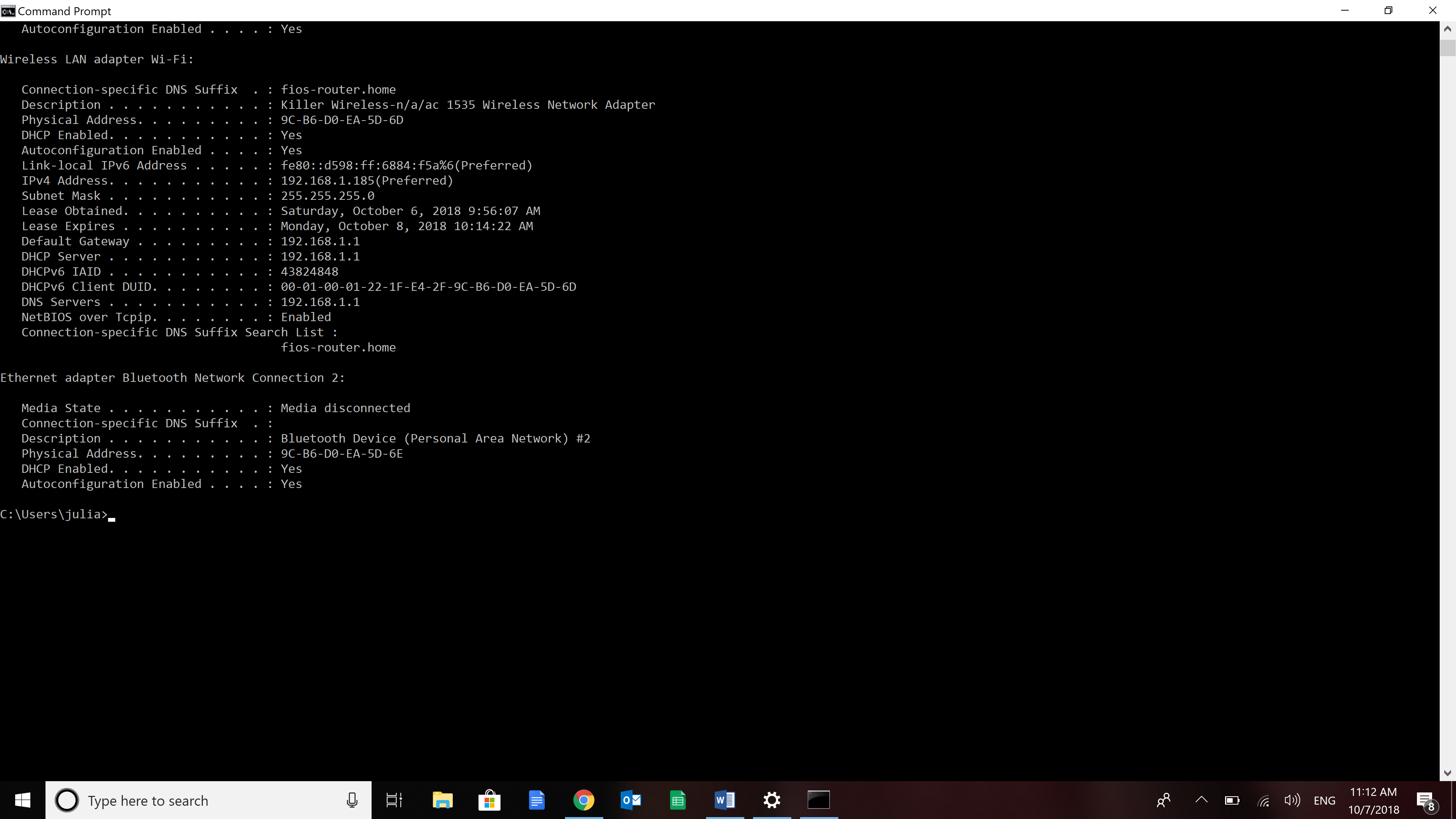
1. Open the Command prompt:
   1. Click on the **Start Button** in the bottom left corner of the screen
   2. Type **cmd**
   3. Right-click on **Command Prompt**; select **Run as administrator**



* 1. You will see this message: “Do you want to allow this app to make changes to your device?” Select **Yes**
  2. The window will look like this:



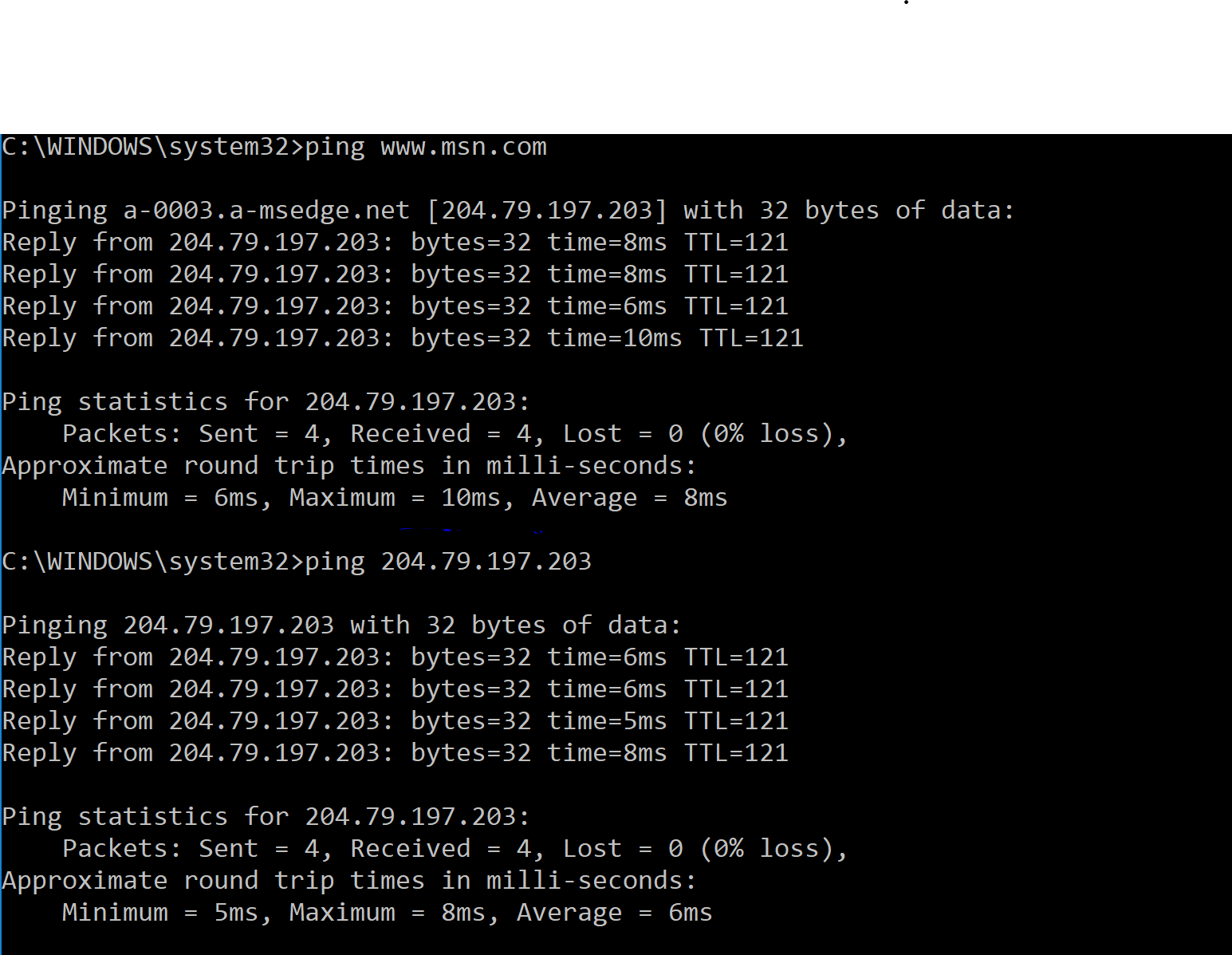
1. To view network settings type: **ipconfig /all** and press **Enter**. (Note: there is a space between ipconfig and /all.)
2. **Scroll** up in the Command Prompt window until you see the settings for the adapter you reported on in item 4-a-3) above.
3. Paste a screen shot of the Command Prompt window (right-click outside the center box and paste the screen shot) showing this information (crop if necessary). (Make sure your screenshot is the width of the paper – resize from the corner.) (**2 points**)



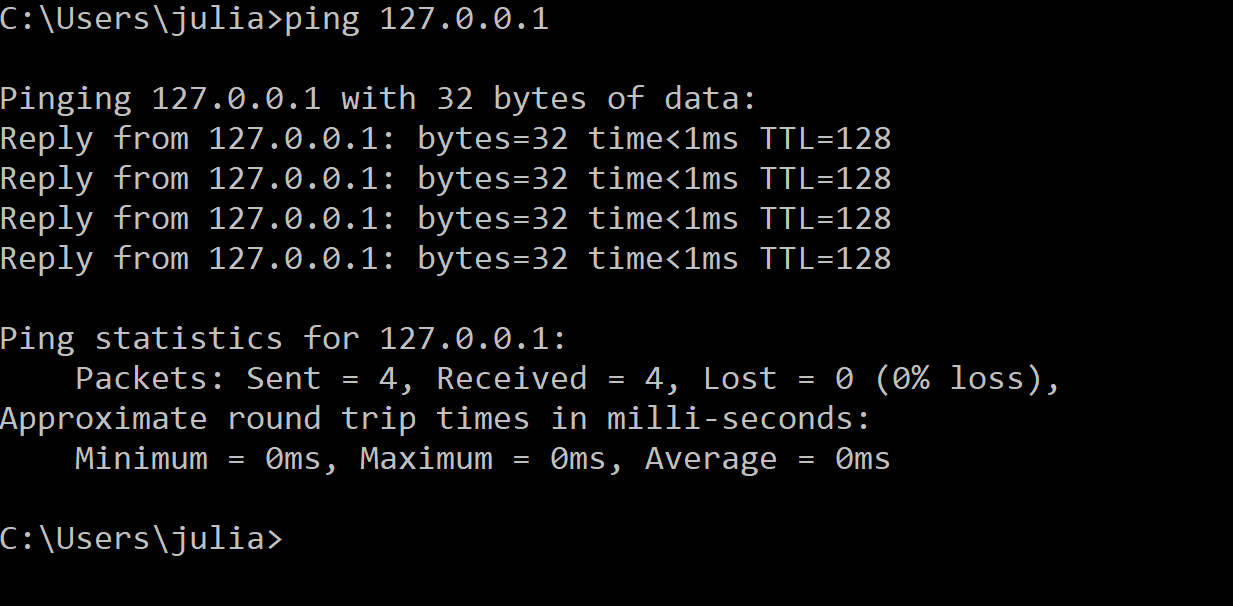
1. Notice that these settings are the same in both the graphical user interface (GUI) in the Windows network properties and in the command line interface (CLI) using the Command Prompt.

##### Section II. Use the command Line to view network status and connections – 12 points

1. **Ping**: this command is used to see if a device with an IP address is available.
   1. Open the Administrator Command Prompt
   2. You will use the ping command to find the IP address for www.msn.com. Type: **ping** **www.msn.com** and press **Enter.** What is the IP address of www.msn.com? (**1 point**) 204.79.197.203
   3. Now try pinging the **IP address** for www.msn.com. Note you can ping either the IP address, or the Domain Name URL address.
   4. Using the Snipping Tool, take a screenshot of both ping commands (pinging the Domain Name URL address and the IP address). Paste the results below. (Make sure your screenshot is the width of the paper – resize from the corner.) (**2 points**)

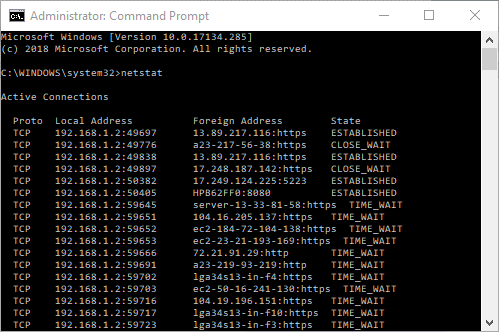


1. **Loopback Address**: 127.0.0.1 is a special IP address called the **loopback address**. It lets you communicate with your system. If you were unable to access the network, you can ping this address to make sure that your system is working properly. That will help you determine if the problem is with your computer or somewhere else on the network.
   1. In the Administrator Command Prompt window, type **ping** **127.0.0.1** and press **Enter**. You should see this result in Windows.
   2. Using the Snipping Tool, take a screenshot of the ping of the loopback address. Paste it below. (Make sure your screenshot is the width of the paper – resize from the corner.) (**2 points**)



1. **Hostname**: this command tells you the host name of your computer.
   1. In the Administrator Command Prompt window, type **hostname** and press **Enter.** What is your host name? (**1 point**) SER-JUL01
2. **Tracert**: this command traces the path from one networked node to another, identifying all intermediate hops (gateways) along the way. (**1 point each**)
   1. In the Administrator Command Prompt window, type **tracert** **facebook.com** and press **Enter** Be patient, this can take a few minutes.
   2. What is the site IP address? (Hint: the screen says “Tracing route to facebook.com” then shows the IP address in brackets) 31.13.69.228
   3. How many hops did it take? 8
   4. Use tracert to find the path to your gateway device. You will need the IP address of your Default Gateway from Section I. Type **tracert** **[IP address of your gateway]** (be sure to **YOUR** gateway address in place of [IP address of your gateway]. For example, if I entered 192.168.1.1 as the Default Gateway in Section I, my tracert command would be **tracert 192.168.1.1.**) How may hops did it take? 1
   5. What do you think is the reason it took that number of hops? 1 hop on local network-because it’s on the same network. And it only takes one hop to access my router. Eight hops to reach Facebook, because it had to go through eight routers to reach Facebook server.
3. **Netstat** is a common command line TCP/IP networking utility available in most versions of Windows, Linux, Unix and other operating systems. It provides information and statistics about protocols in use and current TCP/IP network connections. Below is an example output for Windows. The same information appears in the Mac output with a few more columns. Look for the following columns.

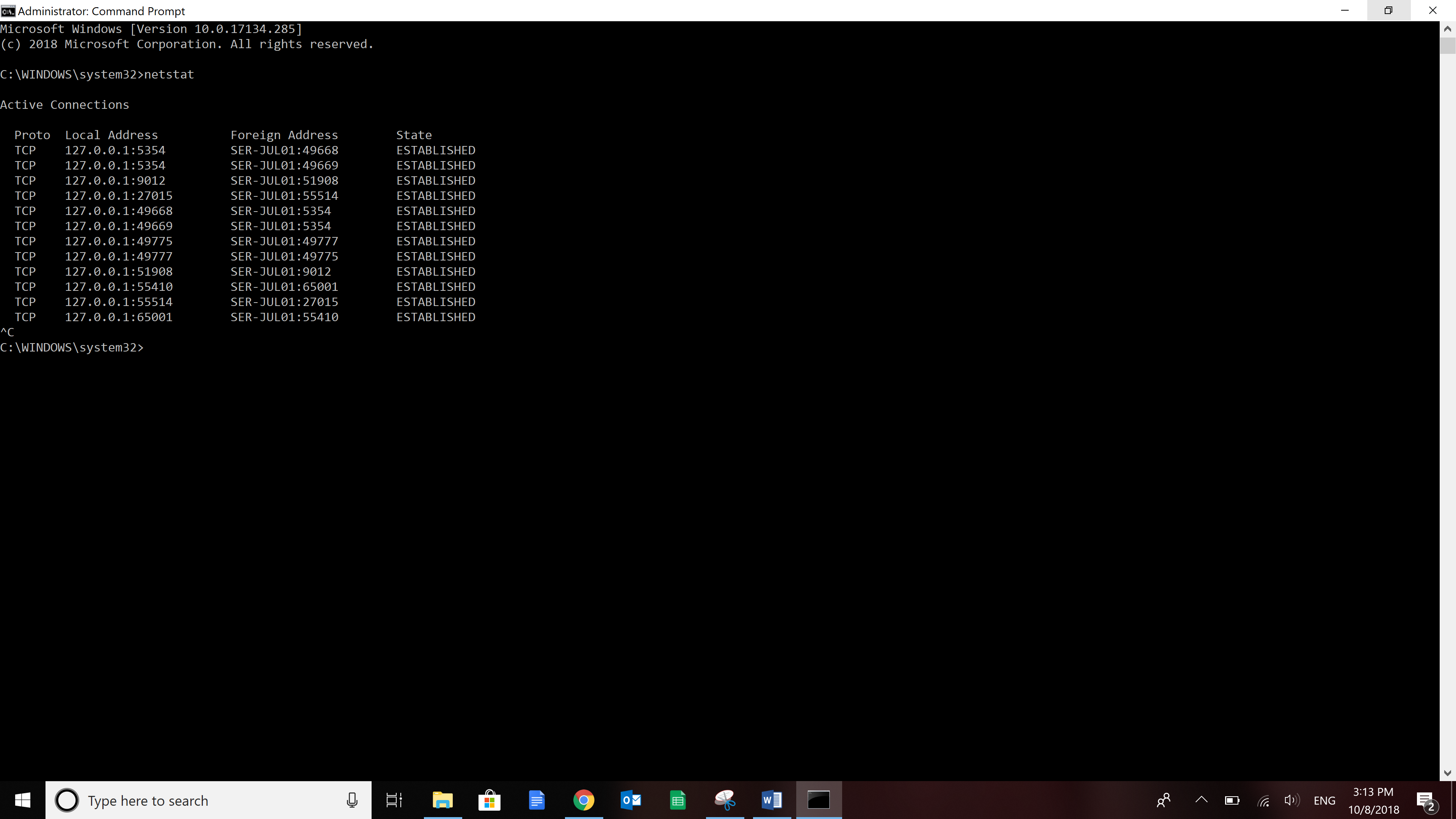
* **Proto** represents the name of the protocol (TCP or UDP).
* **Local Address** shows the IP addresses of the local computer and the port being used.
* **Foreign address** represents the IP address and the port number of the remote computer.



|  |  |  |  |
| --- | --- | --- | --- |
| **Proto** | **Local Address** | **Foreign Address** | **State** |
| TCP | 192.168.1.2:49697 | 13.89.217.116:https | ESTABLISHED |

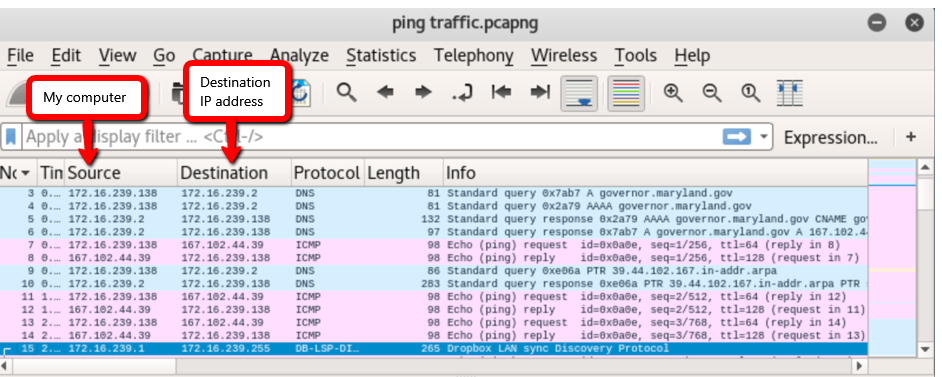
Looking at the first connection, we see that the local computer with an IP Address of 192.168.1.2 has initiated a connection to IP address 13.89.217.116 and it is a secure connection (https) The connection state is ESTABLISHED, and the local computer used port 49697 to initiate the connection.

* 1. Open the command prompt in administrator mode and type: **netstat** and press **Enter**. After you have around 10 results, press CTRL+c to interrupt the responses.
  2. Scroll up to the top of the window and paste a screenshot of the window below. (**2 points**)



##### Section III. View network traffic – 10 Points

#### Capturing Packets

1. Using an application such as Wireshark, we can capture packets of data traveling from and to our computer and look at the information in the packets. This can be helpful for network troubleshooting, analysis, protecting from threats, or software development. (You can download Wireshark for no charge from [www.Wireshark.org](http://www.Wireshark.org). Note: you do not need to download the program for this part of the lab.)
2. Here is a capture of ping traffic (using the Command Line) pinging the IP address 167.102.44.39.  
   

My system: 172.16.239.138

My DNS server: 172.16.239.2

The website queried: 167.102.44.39

Frame 3: My system asks my local DNS if it knows the IPV4 address of the IP address

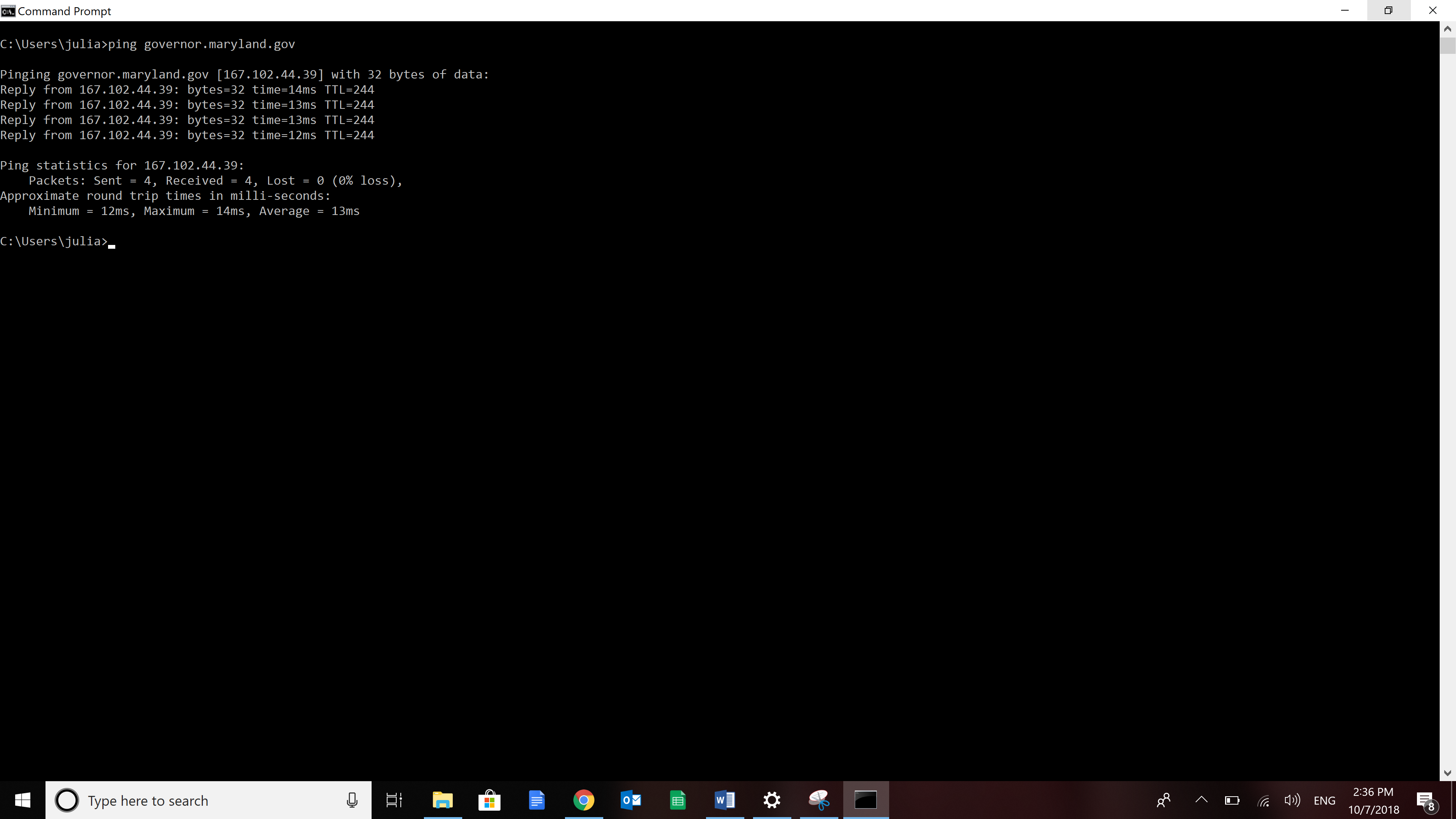
Frame 4: My system asks my local DNS if it knows the IPV6 address of the IP address

Frame 5: My local DNS responds that it does not have a IPVP6 address

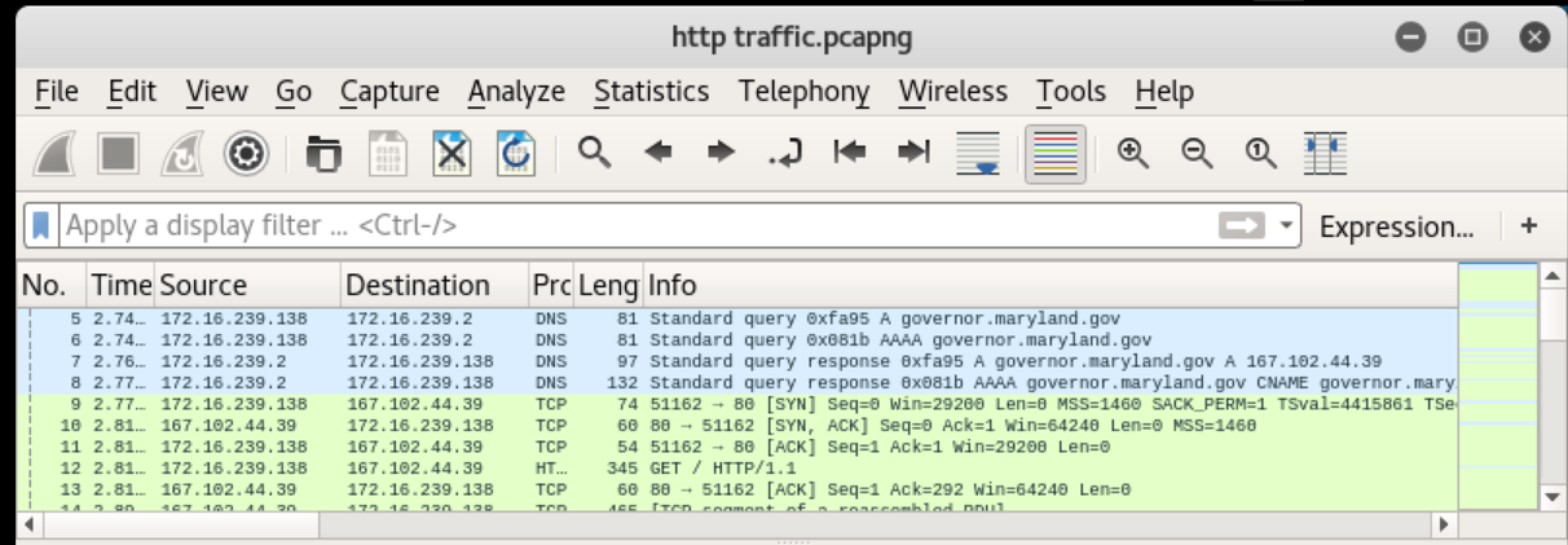
Frame 6: My local DNS responds that the IPV4 address is 167.102.44.39

Pings requests and replies begin

* 1. IP address 172.16.239.138 is the local computer. But who is 167.102.44.39 (hint: look at Info column for packets 3-6)? (**2 points**) It’s the IPV4 address. It’s the IP Address for governor.maryland.gov
  2. What is the ICMP protocol? (**2 points**) (do a Google search – do NOT copy and paste) a protocol used by devices to communicate error reporting messages.
  3. Use the ping command in the Administrator Command Prompt window to confirm. Type **ping governor.maryland.gov.** Paste a copy of your Command Prompt window below. (**2 points**) (Make sure your screenshot is the width of the paper.)



1. This is a capture of http traffic using a browser to visit the IP address 167.102.44.39



My system: 172.16.239.138

My DNS server: 172.16.239.2

The website queried: 167.102.44.39

Frame 5: My system asks my local DNS if it knows the IPV4 address of governor.maryland.gov

Frame 6: My system asks my local DNS if it knows the IPV6 address of governor.maryland.gov

Frame 7: My local DNS responds that the IPV4 address is 167.102.44.39

Frame 8: My local DNS responds that it does not have a IPVP6 address

Frame 9: My system begins the three-way handshake with the website by sending a SYN packet

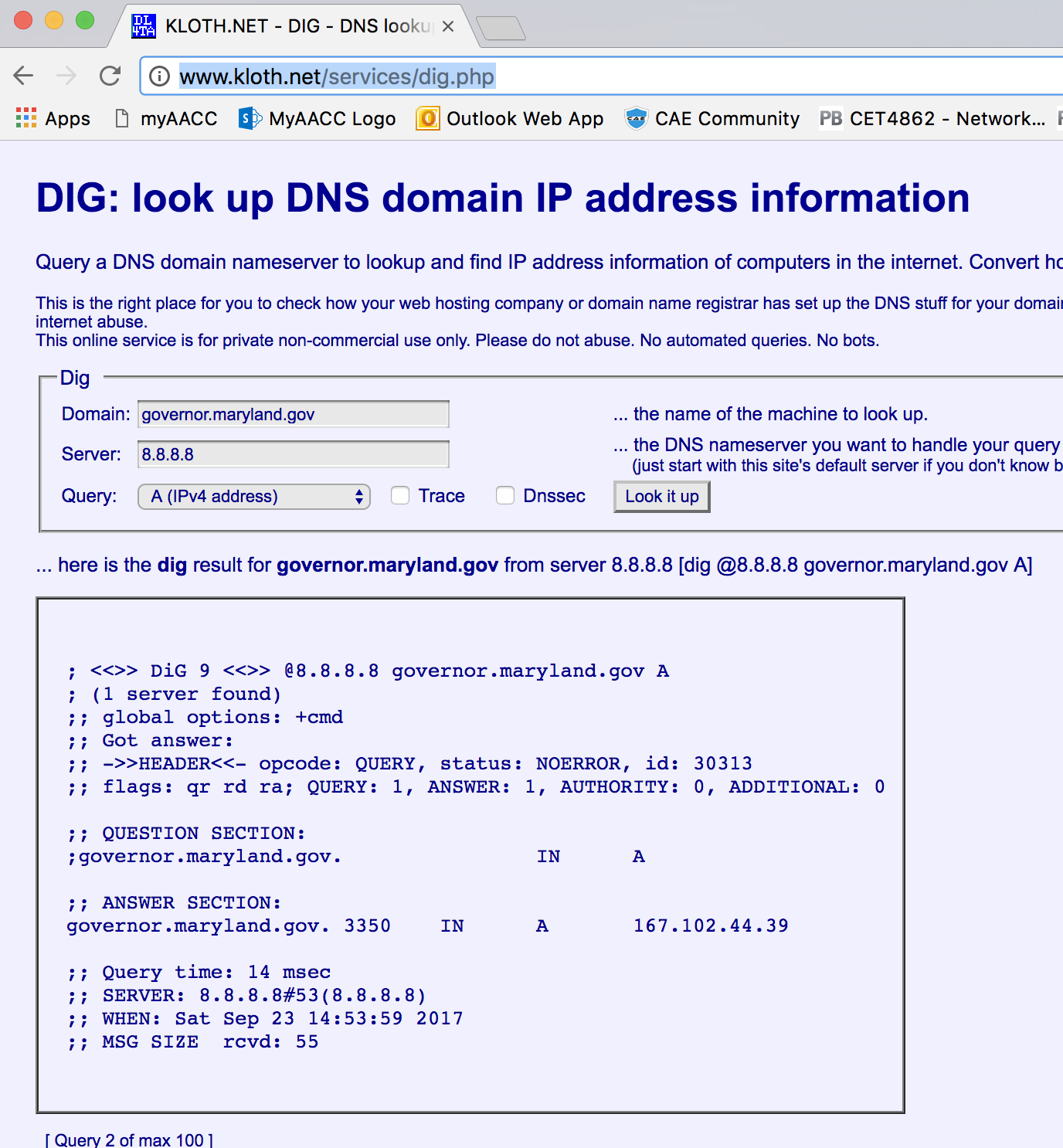
Frame 10: The website acknowledges my request to interact by sending a SYN ACK packet

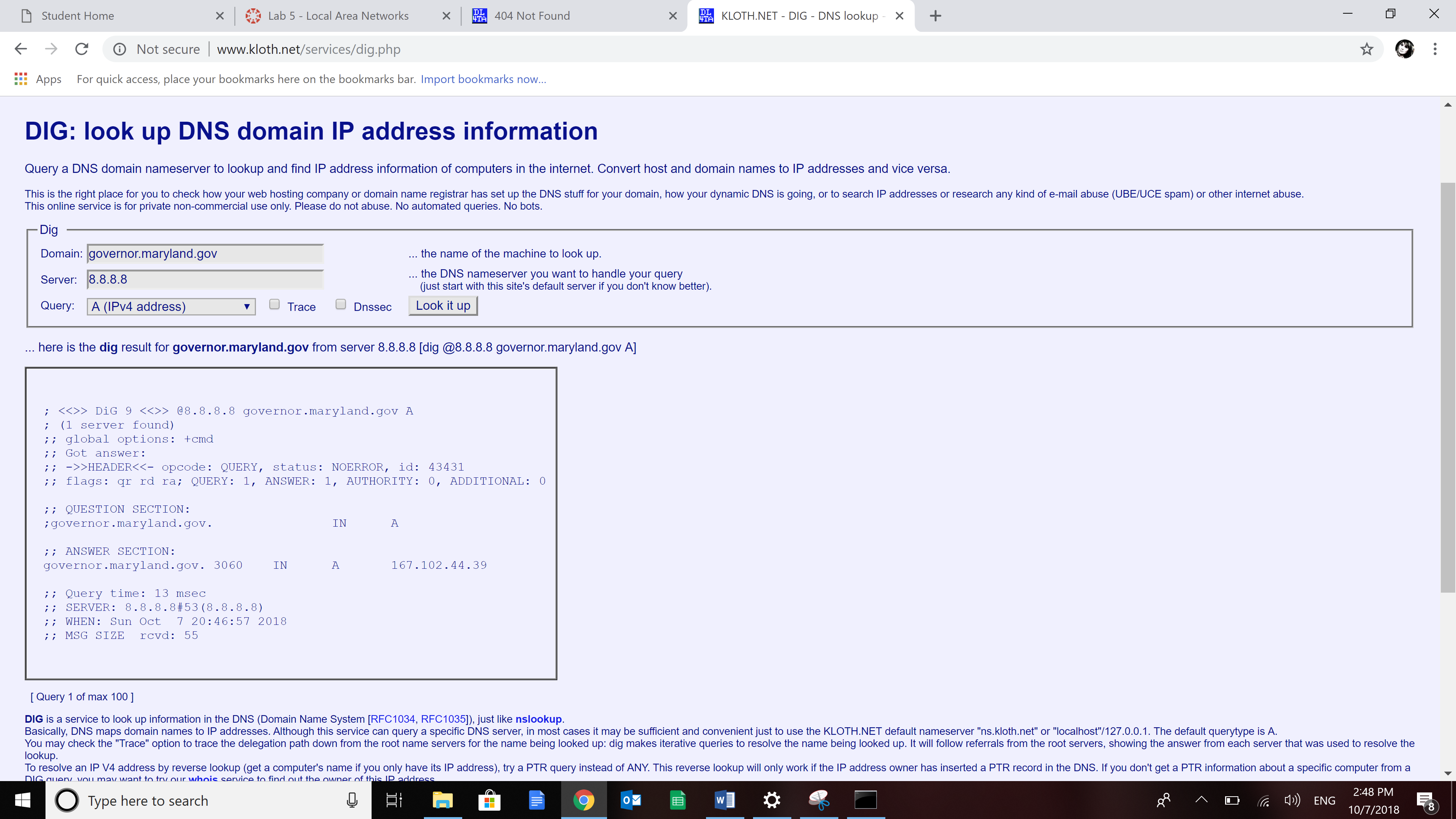
Frame 11: My system completes the three-way handshake with an ACK packet

Frame 12: My system requests the webpage with an HTTP GET request

* 1. What is a three-way handshake? (do a Google search – do NOT copy and paste) (**2 points**) Three-way communication between client and DNS server of synchronization and acknowledgement messages to establish connection before exchanging information.

#### Validating IP Addresses

1. A way to validate an IP address is a certain domain is to use the DIG utility to query DNS servers. There are several web based lookup tools. We will use <http://www.kloth.net/services/dig.php> to validate governor.maryland.gov.   
     
   By default, the Server field is “localhost” implying it will query your local DNS server. We want to change this to 8.8.8.8, which is a public DNS server Google hosts.
2. Using 8.8.8.8 server, “dig” the domain governor.maryland.gov to verify the IP address (click Look it up). Paste the screenshot of the results below. (**2 points**) (Make sure your screenshot is the width of the paper.)



##### Submission Instructions

1. Make sure you have entered your name and section number at the top of the document.
2. Save the document as **LastName\_Lab5.docx**, replacing YourLastName with YOUR last name.
3. Submit the assignment to the Lab 5 dropbox in Canvas by the due date