**IP ADDRESS VISUALIZATION ACTIVITY**

1. **CAPTURE SOME OF YOUR INTERNET TRAFFIC WITH WIRESHARK**
	1. Open the Wireshark program on your computer:
	2. Click on the interface that matches your computer’s Wi-Fi card:



* 1. After 10 seconds, click on the **** icon to stop the capture.
	2. We can export all of this data by clicking on **File > Export Packet Dissections > As JSON ...**



* 1. You can call this first file **traffic1.json** and save it to the Documents folder.
	2. Note 1: You can control what type of data shows up by making your computer do some things that would require wifi (like surfing to some webpages).
	3. Note 2: Another way to capture data about your traffic would be to write the following command in the Command Prompt:

 **"C:\Program Files\Wireshark\tshark.exe" -i 5 -a duration:15 -T json > traffic1.json**

1. **VISUALIZE THE TRAFFIC**
	1. Go to the following webpage:

<http://lapis-constrictor.glitch.me/>

* 1. Enter the IP address of your computer.

(See below if you don’t know this number.)

* 1. Click on “Choose File”
	2. Locate the .json file that you created previously.

|  |
| --- |
| How to find the IP address of your Computer: |
| * Open a Command Prompt by clicking ⊞ Win and typing **cmd**
* Type the command: **ipconfig**
* Find the wireless adapter that says “Wi-Fi”.
* You will see a “IPv4 Address” with 4 numbers: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_
 |

1. **ANALYZE THE TRAFFIC**
	1. Which IP Address has the most number of packets? \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_
	2. Identify who owns the IP address. Use the command **nslookup \_\_.\_\_.\_\_.\_\_** in the Command Prompt to see who that IP address belongs to: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| How to find the Name Server for an IP Address |
| * Open a Command Prompt by clicking ⊞ Win and typing **cmd**
* Type the command: **nslookup \_\_.\_\_.\_\_.\_\_**

*(fill in the blanks with the IP address you want to look up)* * Example: **nslookup 34.200.100.132**
 |

* 1. Which types of websites will generate the most traffic? Generate 3 different .json files that illustrate that you have tried generating different types of traffic.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Types of Traffic** | **Top IP Address** | **Top IP nameServer** | **# packets** | **dataRate** |
| Example:I was surfing on espn.com | 34.200.100.132 | . . . amazonaws.com | 4300 | 800 Mbps |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **Reflection:**
	1. What conclusion can you make about the type of traffic you generated and the #of packets and datarate?

1. **Extension: IPv4 vs IPv6**
	1. IPv4 Address are made up of 4 numbers that range from 0-255. How many different IP addresses can you make with IPv4?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **192 .** | **168 .** | **0 .** | **255** |
|  | **\_\_\_\_\_\_\_\_\_\_ .** | **\_\_\_\_\_\_\_\_\_\_ .** | **\_\_\_\_\_\_\_\_\_\_ .** | **\_\_\_\_\_\_\_\_\_\_**  |
| *# options* | *256 \** | *256 \** | *256 \** | *256* |
|  | 2^8 \* | 2^8 \* | 2^8 \* | 2^8 |

* 1. IPv6 Addresses are made up of 32 numbers that range from 0-15. How many different IP address can you make with IPv6?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **[ FE80 :** | **CD00 :** | **0000 :** | **0000 :** | **0000 :** | **0000 :** | **211E :** | **729C ]** |
|  | **\_ \_ \_ \_ :** | **\_ \_ \_ \_ :** | **\_ \_ \_ \_ :** | **\_ \_ \_ \_ :** | **\_ \_ \_ \_ :** | **\_ \_ \_ \_ :** | **\_ \_ \_ \_ :** | **\_ \_ \_ \_** |
| *# options* | *16\*16\*16\*16* | *16\*16\*16\*16* | *16\*16\*16\*16* | *16\*16\*16\*16* | *16\*16\*16\*16* | *16\*16\*16\*16* | *16\*16\*16\*16* | *16\*16\*16\*16* |
|  | 2^8 \* | 2^8 \* | 2^8 \* | 2^8 \* | 2^8 \* | 2^8 \* | 2^8 \* | 2^8 \* |

* 1. Which is better: IPv4 or IPv6? Why?