**Laboratory Exercise 2 – Wireshark Lab**

Due Date: October 10th, 11:59pm

Points Possible: 100

**1. Overview**

In this lab, students will perform several tasks in generating and analyzing network traffic.

**2. Resources required**

This exercise requires downloading Wireshark onto your computing system (laptop or desktop...NOT for smartphones).

**3. Initial Setup**

For this exercise, you will:

1) Go to the website www.wireshark.org

2) Click "Download\_Get Started Now"

3) When you see "Stable Release (3.2.7)", you will see options to download Wireshark onto your system according to your operating system. For Windows 10 users, choose the "Windows Installer (64-bit) option. For Apple Mac users, choose "macOS Intel 64.bit.dmg". This will initiate the download process.

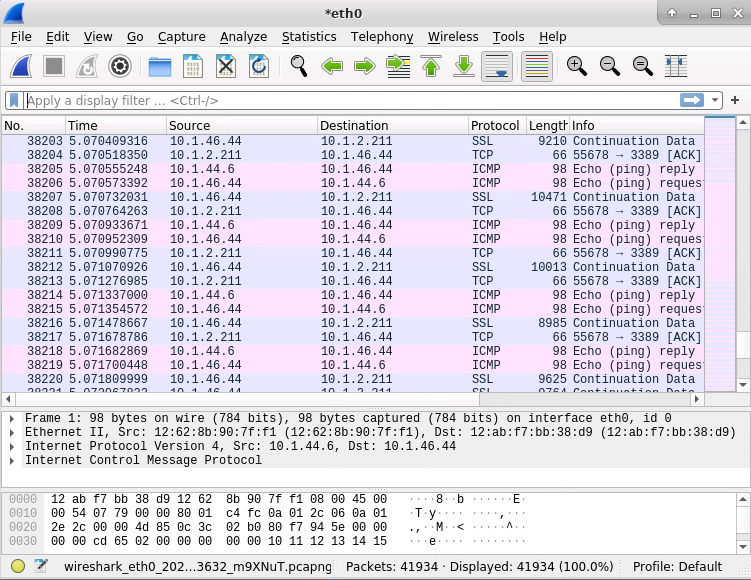
4) Complete the download process...

4) Open and Start Wireshark from where you installed Wireshark on your system...

-You will see the Wireshark Welcome screen. On the Welcome screen you will see a list of interfaces that you can monitor. The first interface you see is usually the primary Ethernet interface, often named "eth0" or "lo0". You will also see an interface called Wifi or WLAN. This is your Wifi interface. Double-click either the Ethernet or Wifi interface...ONLY CHOOSE ONE!!!

-This should have automatically started Wireshark capturing packets. Sometimes, in case no traffic is showing in the Wireshark window, you may have to manually start the packet capture. To manually start packet capture, look at the top left of the Wireshark application. You will see a Blue Fin under "File". Click the Blue Fin. This tells Wireshark to start capturing packets.

-Next you will see several windows with a bunch of data scrolling by. This shows the traffic going to and from your network interface. Do not worry about all of the different colors at this point. Use the picture below as a reference but recognize your system may be slightly different. In the top window, you see a packet-by-packet summary of ALL the traffic that Wireshark sees on the Network Interface card. The middle window is a detailed listed of the structure of a particular packet. If you clicked any line in the top scroll window, you will see this middle window change. The bottom window is the packet viewed in hexadecimal format. Do not worry about this for now but note that if you ever get into reverse engineering (...especially malware), this window will be your best friend. Notice the columns and how all of the data is aligned to a column. Let's go back to the top window, with all the colors. The first column is the frame number in the order received on Wireshark. This is only a number that your Wireshark application tracks. Everyone will have a different frame number. The second column is a local timestamp field. Therefore it is only relevant on YOUR computer. The third column is the source IP address of the received packet. The fourth column is the destination IP address. The fifth column is the higher protocol for the packet. Sometimes you will see the transport layer protocol such as TCP or UDP. Other packets will have the actual application layer protocol such as HTTP or FTP. The sixth column is the length of the entire packet, in bytes. The final column is labeled "Info". This column shows a quick view inside the actual payload of the packet beyond all of the headers.



**4. Tasks**

**-Surf the Web**

-Start your Wireshark capture by clicking the Blue Fin if you have not already done so

-Without going to any websites, just watch the packets go by for about 15-20 seconds.

-Open a web browser and go to a favorite website.

-Observe how the Wireshark window changes in response to your visit to a website.

-After going to a few websites of your choice and watching Wireshark change, STOP

Wireshark. You stop Wireshark by clicking the red stop button next to the blue fin that you clicked to start capture. With Wireshark stopped, you can use the scrollbar in Wireshark and trace the message sequence of your web surfing transactions.

**-Questions**

1) What is your IP address just by looking at Wireshark? (Do the best you can)

2) For the websites that you visited, what are the IP addresses of those websites?

3) What protocols do you see in those web surfing sessions?

4) Can you find the 3-way handshake for when you entered a website into your browser? (\*HINT: Look in the "Info" column for "[SYN] and [SYN ACK]" messages!!!). Once you find it, within a few messages after the handshake, you should see a "GET" message in that "Info" column...What is the text of that "GET" message?

**-Ping**

-Start your Wireshark capture by clicking the Blue Fin if you have not already done so.

-Without going to any websites, just watch the packets go by for about 15-20 seconds.

-Open a command line terminal

-Ping a few websites... "Ping www.yourFavoriteWebsite.com"

-Observe how the Wireshark window changes in response to your ping commands.

-After pinging a few websites of your choice and watching Wireshark change, STOP

Wireshark. You stop Wireshark by clicking the red stop button next to the blue fin that you clicked to start capture. With Wireshark stopped, you can use the scrollbar in Wireshark and trace the message sequence of your ping transactions.

**-Questions**

1) What is the protocol of your ping requests? (\*HINT: Look in the protocol column)

2) For the websites that you visited, what is its corresponding IP address? (\*HINT: Think of how a website name is translated to its IP address. You may see another protocol involved in the transaction).

PLEASE LIST THE WEBSITE NAME AND CORRESPONDING IP ADDRESS.

3) What messages do you see about ping requests/responses (\*HINT: Look in the "Info" column for "Echo")

**-Traceroute**

-Start your Wireshark capture by clicking the Blue Fin if you have not already done so.

-Without going to any websites, just watch the packets go by for about 15-20 seconds.

-Open a command line terminal and run traceroute.

-\*\*\*\*\*\* THE COMMAND USED IS OPERATING SYSTEM SPECIFIC \*\*\*\*\*\*

-For Windows users, it is "tracert". For Mac users, it is "traceroute"

-\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-For Windows users, in your command line, "tracert www.yourFavoriteSites.com"

-For Mac users, in your command line, "traceroute www.yourFavoriteSites.com"

-Observe how the Wireshark window changes in response to your traceroute commands.

-After tracing a few websites of your choice and watching Wireshark change, STOP

Wireshark. You stop Wireshark by clicking the red stop button next to the blue fin that you clicked to start capture. With Wireshark stopped, you can use the scrollbar in Wireshark and trace the message sequence of your trace transactions.

**-Questions**

1) What is the protocol of your trace requests? (\*HINT: Look in the protocol column)

2) For the websites that you visited, what is its corresponding IP address? (\*HINT: Think of how a website name is translated to its IP address. You may see another protocol involved in the transaction).

PLEASE LIST THE WEBSITE NAME AND CORRESPONDING IP ADDRESS.

**-HAVE FUN!!!!!!**

-Wireshark has lots of capabilities...You learn most by just playing with the tool!!! Go for it!!!