

Nicholas Signorelli

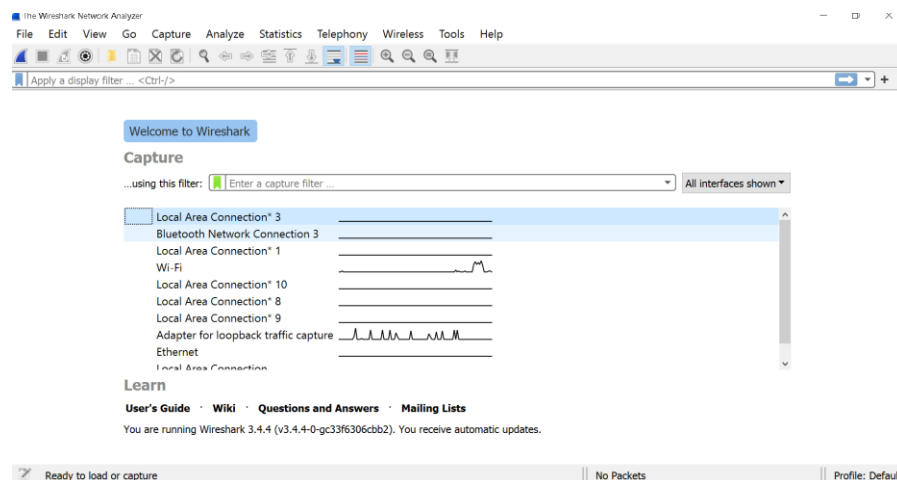
4/14/2021

CPSC 3600

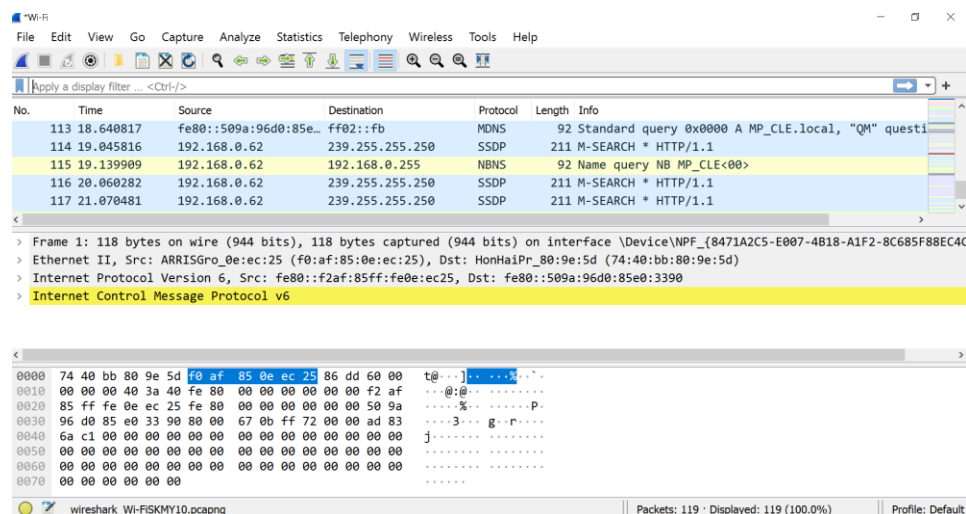
Homework 3, Part 2 and Extra Credit

Wireshark:

Wireshark is free, open-source software that is a packet analyzer. This tool is used to analyze network protocols and gives the user the ability to see what is happening on their network.



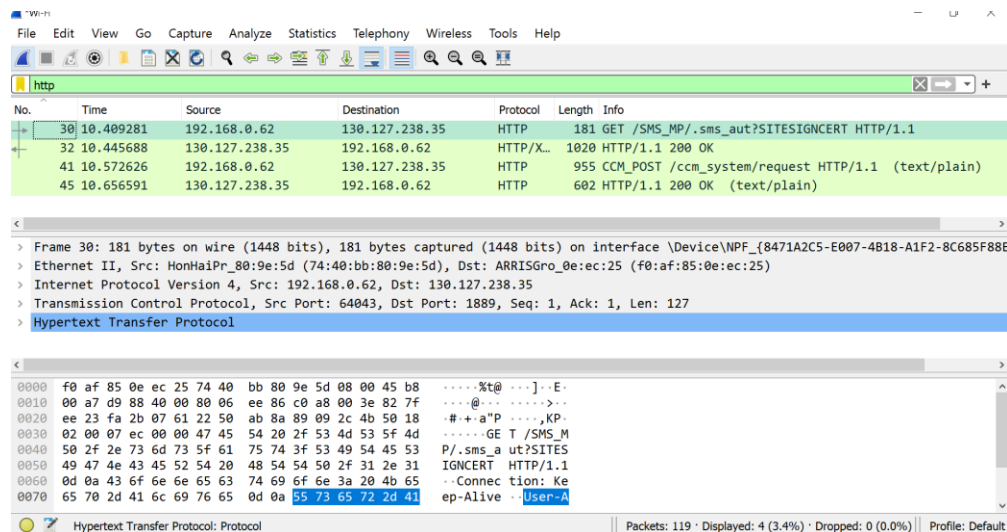
When Wireshark is opened, you are given a list of network interfaces. These are all networks that your computer is sending and receiving packets to, or waiting to do so. I am going to click on Wi-Fi, so I can analyze what packets are being sent. I chose to only analyze for about 20 seconds and 117 packets are available to be looked at.



When selecting to analyze Wifi, a new screen pops up. Displayed is:

- The source IP (my device)
- The packet destination
- Which protocol is being used
- The length of the packet
- Additional information
- The hex and ascii number

Other information, and information from specific packets can be viewed through Wireshark's tools.

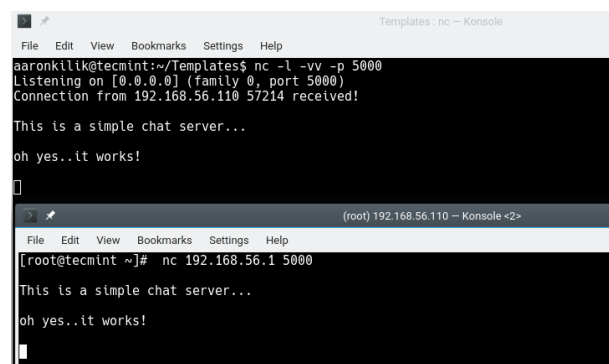


One specific tool that can be used is the filter tool, or the search bar located right below the toolbar (highlighted green). This allows the user to filter all packets that are being analyzed by any feature the user wishes. In this example, I chose to filter by any packets that are being collected that are using the HTTP protocol. The list is then provided, and I can inspect further into any packets that are using HTTP.

Overall, Wireshark is a very helpful tool to anyone who works with network and network security, and should be used if wanting to look at network activity, even through personal use.

netcat:

Netcat is another tool used for networking that can be installed and used on one's Linux command line. It can be used with TCP and UDP, and it can read and write to certain network connections and ports.



Above is a simple example of netcat working on 2 Linux command lines. It connects over a specific port (port 5000), and sends a message between them. Netcat is commonly used as a dependable back-end service. It can be applied to other scripts. Other features it includes is port scanning, transferring files, and as a backdoor to websites.