**WireShark Project**

**Task 1**

**Install and set up Wireshark on Ubuntu:**

* To get the latest stable version of Wireshark on Ubuntu Linux, use the add-apt-repository command: ***sudo add-apt-repository ppa:wireshark-dev/stable***
* Wireshark should not be run as superuser for security reasons.
* The user can be added to the Wireshark group to add packet capture capabilities: ***sudo usermod -aG wireshark $USER***

**Task 2**

**Start a packet capture on an ethernet port and save it to file**:

* The wired interface includes the ethernet packet capture, which begins with ‘en’ in Wireshark.
* The Wireshark app includes controls to start packet capture, stop capture, save the packets to a file, and load the capture file.
* A capture can only be saved once the capture has stopped.

**Task 3**

**Use a display filter to detect HTTPS packets:**

* To display certain packets in an existing packet capture, use a display filter.
* To display only HTTPS traffic, use a filter on TCP port 443: ***tcp.port == 443***

**Task 4**

**Visit a web page and detect its IP address using a display filter:**

* A TLS handshake display filter may be used to detect a website visit in a packet list: tls.handshake.type ==1
* The IP address is used in a filter to obtain packet information for a particular website: ip.addr == 142.251.163.105

**Task 5**

**Locate all HTTPS packets from a capture not containing a certain IP address:**

* A Conditional statement may be used to include and eliminate packets from a Wireshark capture: !(ip.addr == 8.43.85.97) and tcp.port == 443
* A compound conditional should include parentheses to avoid order of execution errors: !(ip.addr == 8.43.85.97) and (tcp.port == 80 or tcp.port == 443)

**Capstone Task**

**Use Wireshark to capture and observe ethernet packets on HTTP and HTTPS ports**

You are to use Wireshark to create a capture file and then use a display filter to list all https and http packets.

1) Clear the cache in the Firefox browser.

2) Start a packet capture on the ethernet in Wireshark.

3) Visit Google.com, duckduckgo.com, and http://cygwin.com (not https!)

4) Stop the packet capture in Wireshark and save the capture to a file.

5) First, create a filter to just display port 80 TCP data. This should give you the IP address of Cygwin.

6) Next, Create a filter to display only HTTP AND HTTPS packets (hint: use an OR condition).

7) Now, eliminate the Cygwin site visits from the displayed packets (hint: use an AND condition).