Christopher Bazyani

Practical Cyber Security

Unit 3

Packet Sniffing - Protocol Layers

**Capture the Trace**

**Launching Wireshark**

Graphical user interface

Description automatically generated

**Startup screen**

Graphical user interface, text, application, email

Description automatically generated

**Selecting the ethernet network interface**

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**Filtering Traffic**

Applying the display filter tcp.port = = 80 in the main filter box

Text

Description automatically generated

Using the filter box feature found though Capture > Options to input the tcp.port = = 80 filter as just port 80

Graphical user interface, application, table

Description automatically generated

Packets will be recorded by Wireshark as the content is transferred using the port 80 capture filter through the capture options box. Capturing the trace has been successful.

Example website used:

http://openmaniak.com/wireshark\_filters.php in your browser

Text

Description automatically generated

**Inspect the Trace**

For inspecting the trace, it was done using the HTTP filter and then inspecting the block that lists the details pertaining to the frame and the ethernet. This is what it looks like for the pcap file.

Graphical user interface, text, application

Description automatically generated

**Run another Trace**

Starting new capture

Graphical user interface, text, application

Description automatically generated

We will use the site <http://www.derrycityfc.net/> to capture traffic

I was able to find a few protocol columns as HTTP with the info column as GET when incorporating the port = = 80 filter.

Graphical user interface, text, application

Description automatically generated

Then copy what is in the hypertext transfer protocol from the HTTP GET packet

Graphical user interface, application

Description automatically generated

Then open a text editor such as Notepad and paste what is within that hypertext transfer protocol

Graphical user interface, text, application

Description automatically generated