TCP/IP Model Encapsulation Headers

Introduction

As a member of the IT team at Nerdify Enterprises, you notice an unusual amount of heavy traffic on the network. To make sure that all of the traffic is legitimate, you use a protocol analyzer to capture some random packets for further testing.

Note: Protocol Data Unit (PDU) refers to how data is packaged when being transferred between two points. This includes units such as bits, frames, packets, segments, and data/payload. Look for these key terms in the textbook when describing layers to find where they fit in the OSI and TCP/IP models.

Objective

In this lab, the student will use a protocol analyzer to capture packets and enforce OSI model layers, Protocol Data Units, Protocol types, and addressing.

Resources

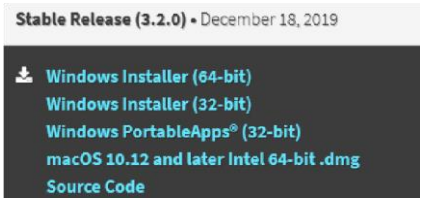
- ***Computer with Internet connection***
- ***Access to the textbook/e-book or presentation slides for reference***
- ***Wireshark Protocol Analyzer application installed on the computer***

Assignment

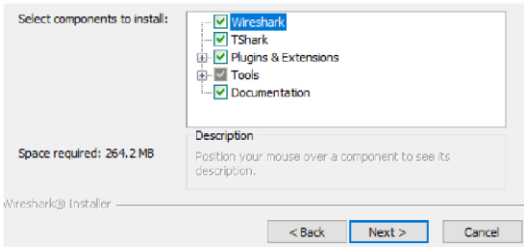
Estimated Time for Completion: 30 minutes

1. ***Download and install Wireshark***
   a. ***Video Instructions Install Wireshark***
   b. ***Step by step instructions:***

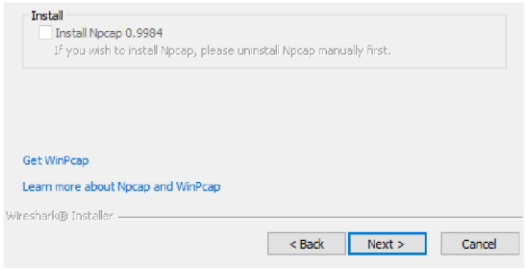
Click Download > Choose your Operating System



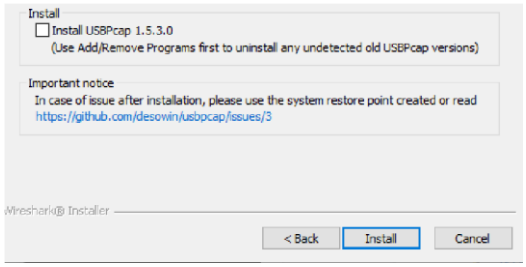
Select all components > Next



Select Install Npcap> Next



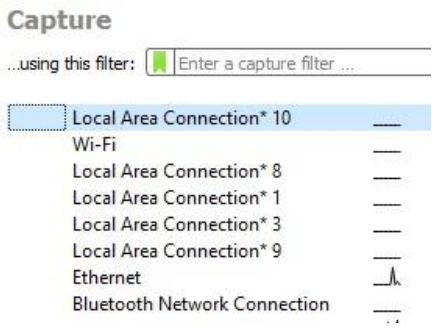
Do not select Install USBPcap >Click Install



Procedure

1. ***Right-click on the Wireshark Protocol Analyzer icon on the computer desktop and select Run as Administrator. If prompted by the application to make changes to your computer, select Yes.***

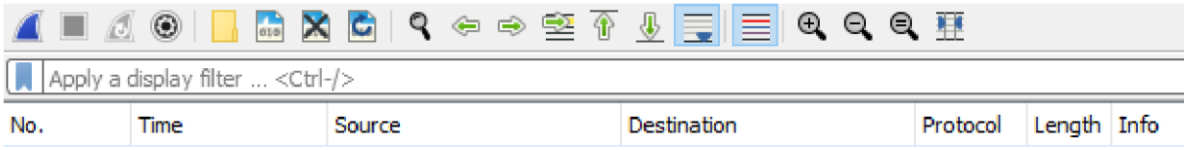
2. ***Once the Wireshark window opens, double-click the Ethernet option. (Depending on your computer configuration, this may be called something different. Select the line graph that does not have a flat line - this indicates traffic is flowing on the interface.)***



3. ***Let Wireshark perform 20 (twenty) seconds packet capture.***

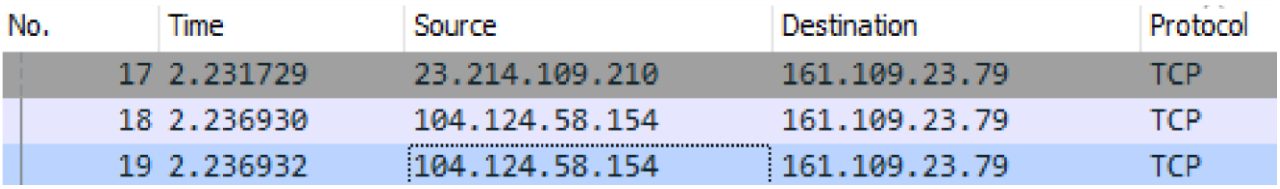
4. ***Stop the packet capture by clicking the Red Square (Stop Capture) button on the toolbar.***

5. ***Several fields will be listed at the top of the Wireshark screen. Double-click "Protocol."***

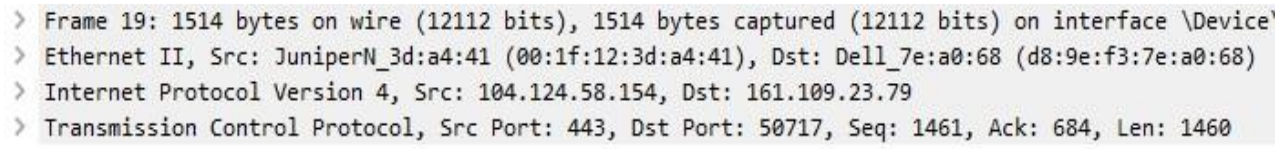


This will sort the packets in alphabetical order for easier use.

6. ***Scroll down until you see TCP in the Protocol field. Click on any TCP packet row.***



7. ***Using the information from Wireshark, complete the table below:***



Using the examples in the procedure, complete the table.

Layer #	***TCP/IP Layer Name***	***PDU name***	***Protocol***	***Address Information***
4	***Application***	***Data***	***N/A***	***N/A***

3	*Transport*	*Segment*	*TCP*	*Source: 60857 Destination 8009*
2	*Internet*	*Packets*	*IPv4*	*Source: 192.168.1.194 Destination: 192.168.1.234*
1	*Network Interface*	*Frames/Bits*	*Ethernet II*	*Destination: 44:5c:e9:4c:af:ca Source: 74:d8:3e:03:12:7c*

Reflection

1. ***In the twenty seconds you performed the packet capture, how many packets travelled across your network? 647 Packets***
2. ***Notice the many different colors of packets that appear on your capture. What could the colors represent? The types of traffic***

Standards for This Competency	*EXEMPLARY*	*ACCOMPLISHED*	*DEVELOPING*
Each cell in the table contains the correct answer. (2.85 pts each)	*Yes, (80 pt)*	*No, (0 pt)*	*No, (0 pt)*
Reflection Question #1	*Answer is correct and fully developed. (10 pt)*	*Answer is correct and partially developed. (5 pt)*	*Answer is incorrect. (0 pt)*
Reflection Question #2	*Answer is correct and fully developed. (10 pt)*	*Answer is correct and partially developed. (5 pt)*	*Answer is incorrect. (0 pt)*