LAB ASSIGNMENT - 3

Name: Ashwin Balaji
Roll Number: 2020PMD4221
Course: M.Tech (Mobile Computing and Data Analytics)

Title: Analyze the network packets using WIRESHARK

Software Requirements: Wireshark, WinPCap 5.1.31

Theory:

Network packets are a granular unit of data used to distribute information across the internet and network. These packets are broken down into **two general sections — a header or control information and the payload or user data.**

The **header contains information for delivering the data in the payload, like Ethernet ll segments, where the DMAC and SMAC addresses are defined; if there is a VLAN or not; and IPv4 or IPv6 protocols where the Source IP and destination IP address are defined — these are considered layer 2-3 data.**

The **payload is the data that is the actual intended information, the end user videos, phone audio, images and information data.**

But **sending data over a network is just like shipping a package: you have to follow certain rules and go through a specific process before your final product gets delivered.** This is the defined import/export laws of the internet.

This set of rules, known as the Transmission Control Protocol/Internet Protocol (TCP/IP), is called a protocol stack. It's composed of four layers:

- **Application protocol** is the first TCP/IP layer. It defines and standardizes how data gets sent over your network.
- **Transmission control protocol (TCP)** is where your data packet is assigned port and sequence numbers to ensure that it arrives at the correct application, in the correct order.
- **Internet protocol (IP)** assigns source and destination IP addresses to your data packets. It also determines the best route for your data to travel over your network so it can reach its final destination efficiently.
- **Hardware** is the machine that receives all this information to reassemble your data packets in the correct order.

Packet analyzers, also known as packet sniffers or network analyzers, are a network monitoring tool that examines data traffic moving in and out of the network. These tools analyze network performance issues that can lead to traffic bottlenecks, network downtime, and other common performance issues that ultimately effect end-user experience and a company’s productivity.

Continuing with our shipping analogy, you can think of packet analyzers as the gate agents and security scanners in the data transportation process. They work behind the scenes to ensure everything runs smoothly on your network.

Packet sniffers are a go-to tool for everything from making sure network traffic is routed correctly, to ensuring employees aren't using company internet time for inappropriate websites. Packet analyzers also help detect potential network intrusion by looking for network access patterns inconsistent with standard usage.

In a process known as packet capture (PCAP), analyzers snag packet data as it moves over your network. It saves a copy of this data as a file on your monitoring device. You can analyze these copies of your packet data, to detect usage spikes, suspicious data transfer, and inconsistent network performance.

Advantages:

- **Find the root cause of various issues to secure your network**

  When you have access to your packet data, you can dig into the root cause of network issues. Thinking like a good threat hunter, you can familiarize yourself with typical traffic patterns and use your knowledge to identify inconsistencies. When you understand your standard network performance, you can also use packet analyzer data to detect network vulnerabilities. When you know where you can improve, you can bolster your network security to prevent future threats, issues, or attacks.

- **Better understand your network speed**

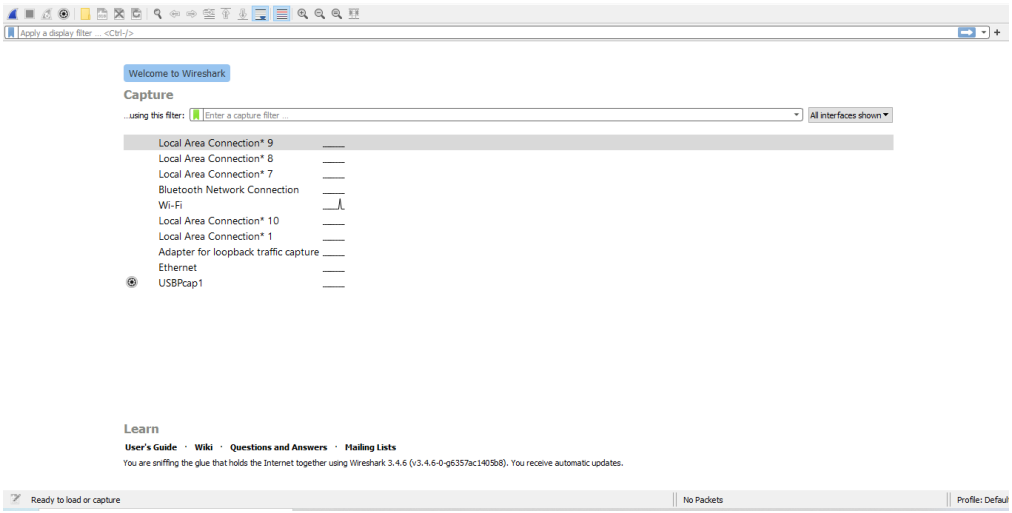
  Armed with your PCAP analysis, you can figure out the average time it takes for a packet to travel across your network. Using these numbers, you can more quickly and easily figure out the source of any network slowdowns. When you understand the source, you can determine which applications are impacted and take action to fix any issues.

- **Identify inefficient network usage**

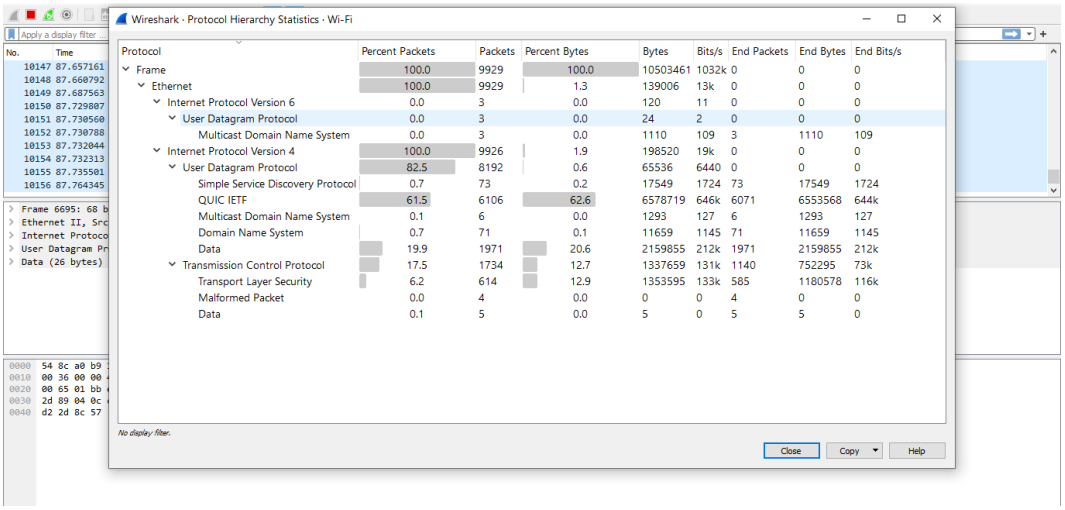
  Packet analyzers can help you categorize the traffic on your network. With this data, you can identify non-business uses of your network, like visits to social media sites that might slow your network performance.

Procedure:

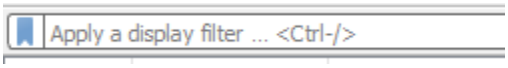
1. Download and Install WireShark
   Linux: sudo apt-get install wireshark



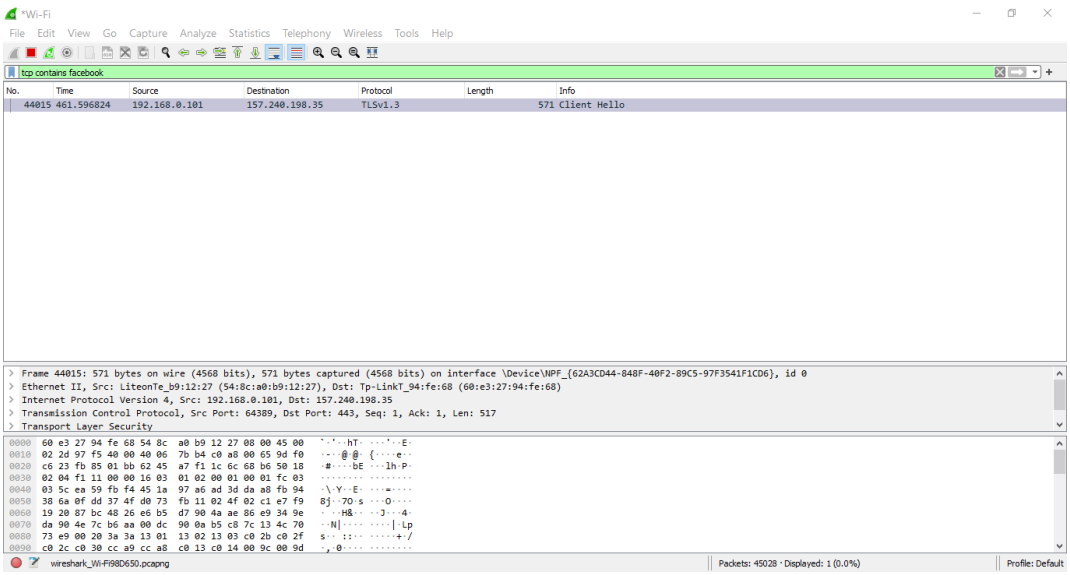
2. Check **Protocol Hierarchy**



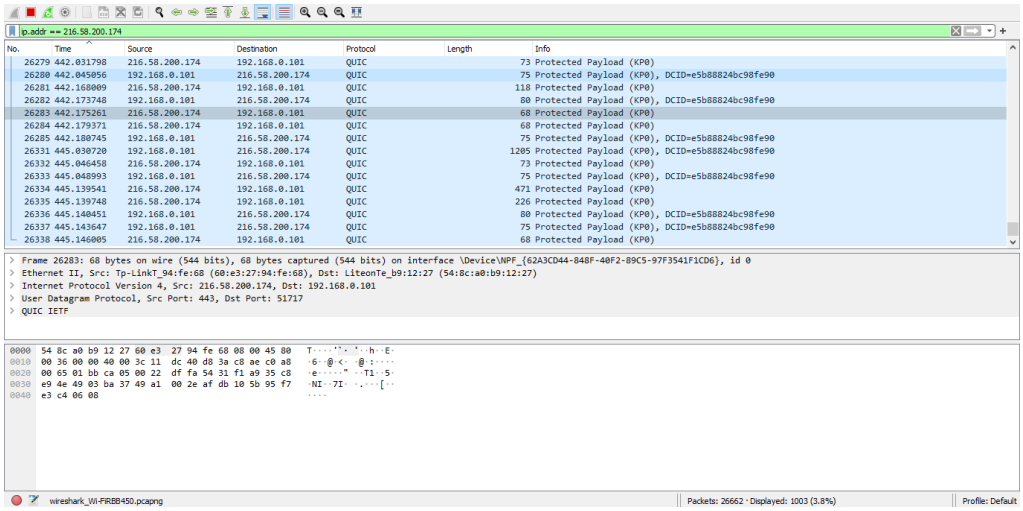
3. Check for ICMP (Internet Control Messaging Protocol for PING). For that we may require machine IP Address
   Windows: ipconfig (in cmd)
   Linux: ifconfig (in terminal)
4. To **capture a set of packets,** these  buttons can be used at the upper right corner of the window.
5. To apply **filter to the packets like TCP, HTTP, FTP, UDP, HTTPS, SSDP, TLS etc.,** filtering section can be used.



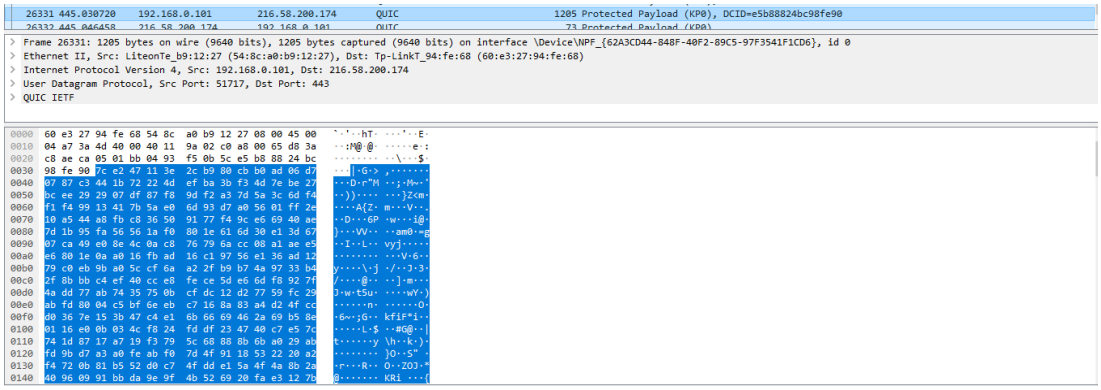
6. To apply **filter at the website**:
   a) Run the website through the browser.
   b) Type **tcp contains <domain name>** [EXAMPLE: tcp contains facebook]



7. To apply filtering using source/destination address:
   a) Type **ip.addr == <ip-address>** or **ipv6.addr == <ip-address>** at the filtering section for the website we have accessed [Example: ip.addr == 216.58.200.174]

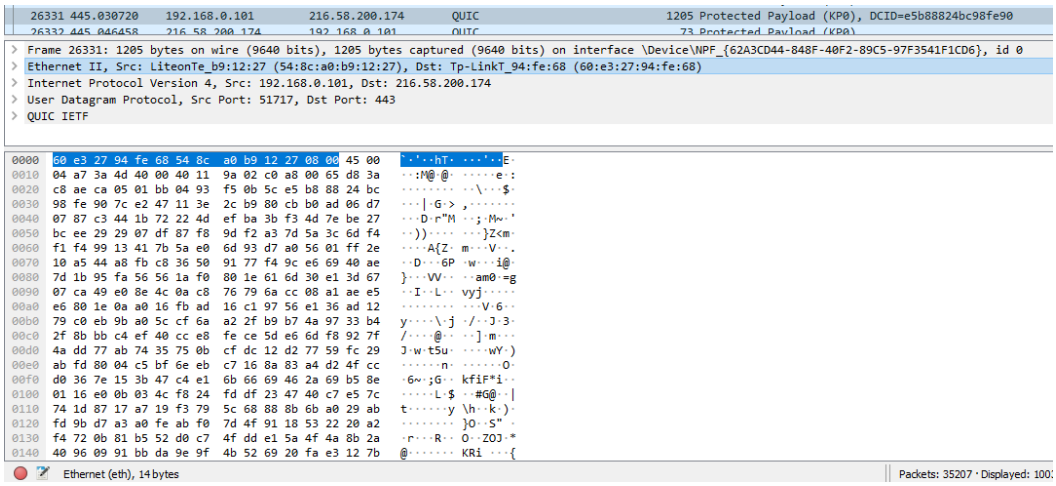


8. To analyze packets, click on a filtered packet, we will get information about the packet.



a) These message can be mapped with the packet received like clicking on **frame 26331**, whole packet gets selected (blue mark), explaining that this part of message is frame.

b) Suppose to check which part of received/sent frame is **Ethernet II,** hover around Ethernet II, and the corresponding section of that will be highlighted in the encrypted frame.



c) Likewise, we can explore the corresponding packet sections easily.

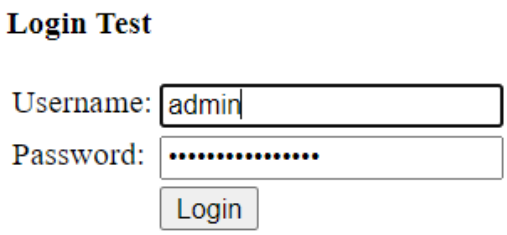
9. To check if the **packet is secure**

a) Since the packets received are all encrypted (till now what we have seen) as it is not in human understandable language.

b) Let's check for unencrypted packets by accessing a unsecure website.

c) Here, this website is not secure and the **attacker may listen to the information**.

d) **Username:** admin and **Password:** websitenotsecure, and click Login



e) Here we can see that, **information is revealed**. And, this is same for revealing credit information, bank details etc.