NEHAL JHAJHARIA (U20CS093)

COMPUTER NETWORKS

ASSIGNMENT 02

1.

Packet Sniffer is a network analyser, a piece of hardware or software, used to monitor network traffic.

- **Hardware Packet Sniffers**
  A hardware packet sniffer is designed to be plugged into a network and to examine it. A hardware packet sniffer is particularly useful when attempting to see traffic of a specific network segment. By plugging directly into the physical network at the appropriate location, a hardware packet sniffer can ensure that no packets are lost due to filtering, routing, or other deliberate or inadvertent causes. A hardware packet sniffer either stores the collected packets or forwards them on to a collector that logs the data collected by the hardware packet sniffer for further analysis.

➢ **Software Packet Sniffers**

Most packet sniffers these days are of the software variety. While any network interface attached to a network can receive every bit of network traffic that flows by, most are configured not to do so. A software packet sniffer changes this configuration so that the network interface passes all network traffic up the stack. This configuration is known as *promiscuous mode* for most network adapters. Once in promiscuous mode, the functionality of a packet sniffer becomes a matter of separating, reassembling, and logging all software packets that pass the interface, regardless of their destination addresses. Software packet sniffers collect all the traffic that flows through the physical network interface. That traffic is then logged and used according to the packet sniffing requirements of the software.

2.

Steps to install wireshark on a mac -

1. Go to https://www.wireshark.org.
2. Click on Download.
3. Select the version according to your operating system, in this case macOS.
4. The file shall start downloading.
5. Double click the file, it should be installed.
6. Drag the icon into the Applications folder and you are done.

Running the wireshark -

1. Double click the Wireshark icon.
2. A list of various networks is in the center with simple line graphs of network traffic.
3. Double click the one you wish to analyze the traffic for.

3.

1. Run wireshark.
2. Open a web browser and put http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html in the url and hit search.
3. To analyze traffic for a website, in the wireshark search bar, type “tcp contains <website keyname>” without the quotes and the angular brackets. In this case, tcp contains umass.
4. Hit enter.

4.

a)

TCP, UDP and SSDL are the 3 most prominent protocols to be seen in the list.

b)

Time difference in nanoseconds -

HTTP GET - 993336

HTTP OK - 913363

Difference = 79973 nanoseconds

c)

Internet address of gaia.cs.umass.edu - 128.119.245.12

Internet address my computer - 172.39.5.22