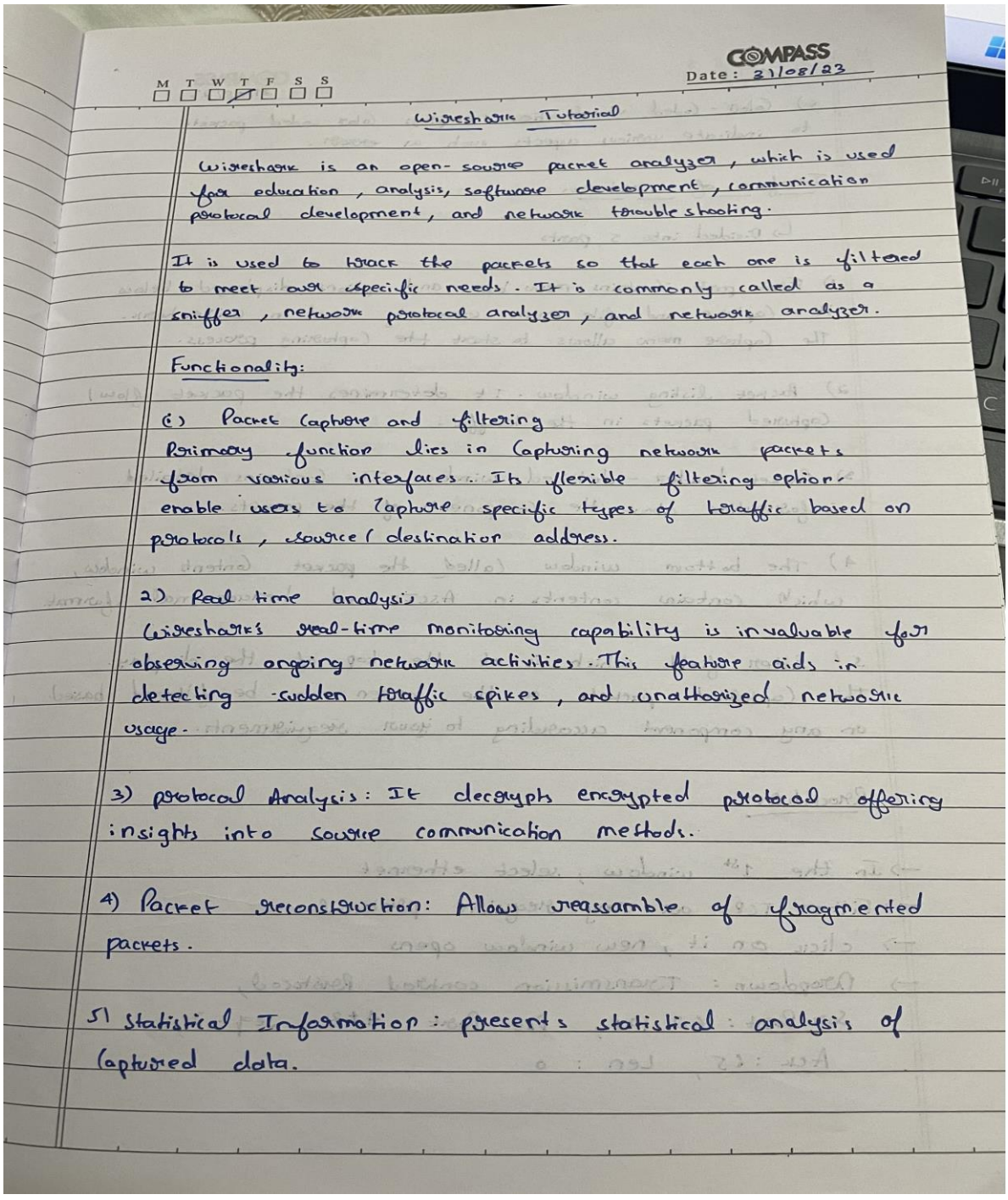
LAB PROGRAM – 17

Q) Tool Exploration –Wireshark

Procedure :



M T W T F S S

COMPASS
Date: 21/08/23

Wireshark Tutorial

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer.

Functionality:

1) Packet Capture and filtering
Primary function lies in capturing network packets from various interfaces. Its flexible filtering options enable users to capture specific types of traffic based on protocols, source/destination addresses.

2) Real time analysis
Wireshark's real-time monitoring capability is invaluable for observing ongoing network activities. This feature aids in detecting sudden traffic spikes, and unauthorized network usage.

3) protocol Analysis: It decrypts encrypted protocol offering insights into source communication methods.

4) Packet reconstruction: Allows reassamble of fragmented packets.

5) Statistical Information: presents statistical analysis of captured data.

COMPASS
Date : 31/08/23

M T W T F S S

6) Color-coded visualization : employs color-coded packets to indicate various aspects such as error.

Interface of wireshark:

↳ Divided into 5 parts

1) First part contains menu bar and options displayed below it. Capture and file menu commonly used in wireshark. The Capture menu allows to start the capturing process.

2) Packet listing window. It determines the packet flow / captured packets in the traffic.

3) Packet header - detailed window. It contains detailed information about the components of the packets.

4) The bottom window called the packet contents window, which contain contents in ASCII and hexadecimal format.

5) filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements.

Procedure:

→ In the 1st window, select ethernet
→ Filter TCP or any require protocol
→ click on it, new window opens
→ Dropdown : Transmission control Protocol,
Scr Port : 62 148, Dst Port : 443, Seq : 2,
Ack : 65, Len : 0

M T W T F S S

COMPASS

Date: 31/08/23

→ This is available in the prev windows in the left split of screen.

→ clicking on dropdown of it, clicking on any of them highlights its counterpart in right split side of screen.

→ In Cmd, type > ipconfig

RESULT:

Windows IP configuration

Ethernet adapter Ethernet

Connection-specific DNS suffix :

Link-local IPv6 Address fe80::be78:f609:ed25:e329%8

IPv4 Address 10.124.2.83

Subnet Mask 255.255.0.0

Default Gateway 10.127.0.11