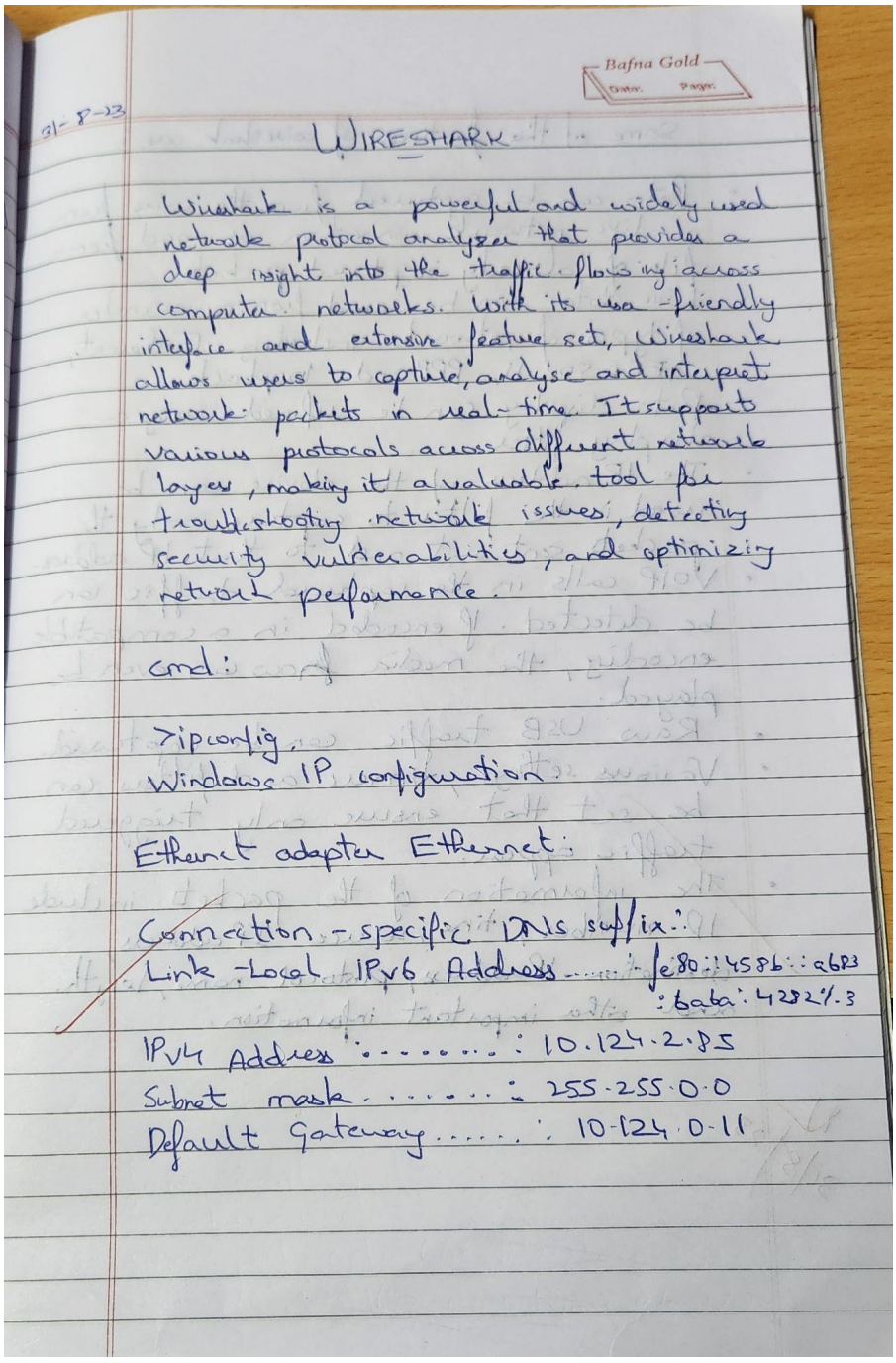
CYCLE 2

AIM:

Tool Exploration -Wireshark

OBSERVATION:



Bafna Gold

31-8-23

WIRESHARK

Wireshark is a powerful and widely used network protocol analyzer that provides a deep insight into the traffic flowing across computer networks. With its user-friendly interface and extensive feature set, Wireshark allows users to capture, analyse and interpret network packets in real-time. It supports various protocols across different network layer, making it a valuable tool for troubleshooting network issues, detecting security vulnerabilities, and optimizing network performance.

cmd:

>ipconfig

Windows IP configuration.

Ethernet adapter Ethernet:

Connection-specific DNS suffix:

Link-Local IPv6 Address ..... : fe80::4586::a6f3
:baba:4282%3

IPv4 Address ..... : 10.124.2.85

Subnet mask ..... : 255.255.0.0

Default Gateway ..... : 10.124.0.11

Some of the features of wireshark are:

- Data can be captured from the wire from a live network connection or read from a file of already captured packets.
- Live data can be read from a number of types of networks including Ethernet, IEEE 802.11, PPP and loopback.
- Data display can be refined using a display filter.
- The IP address of the device can be used in the filter to capture only the packets sent out and to that IP address.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Various settings, timers and filters can be set that ensure only triggered traffic appear.
- The information of the packets include ID number, time, source IP address, destination IP address, protocol name, length and other important information.

31/8/23