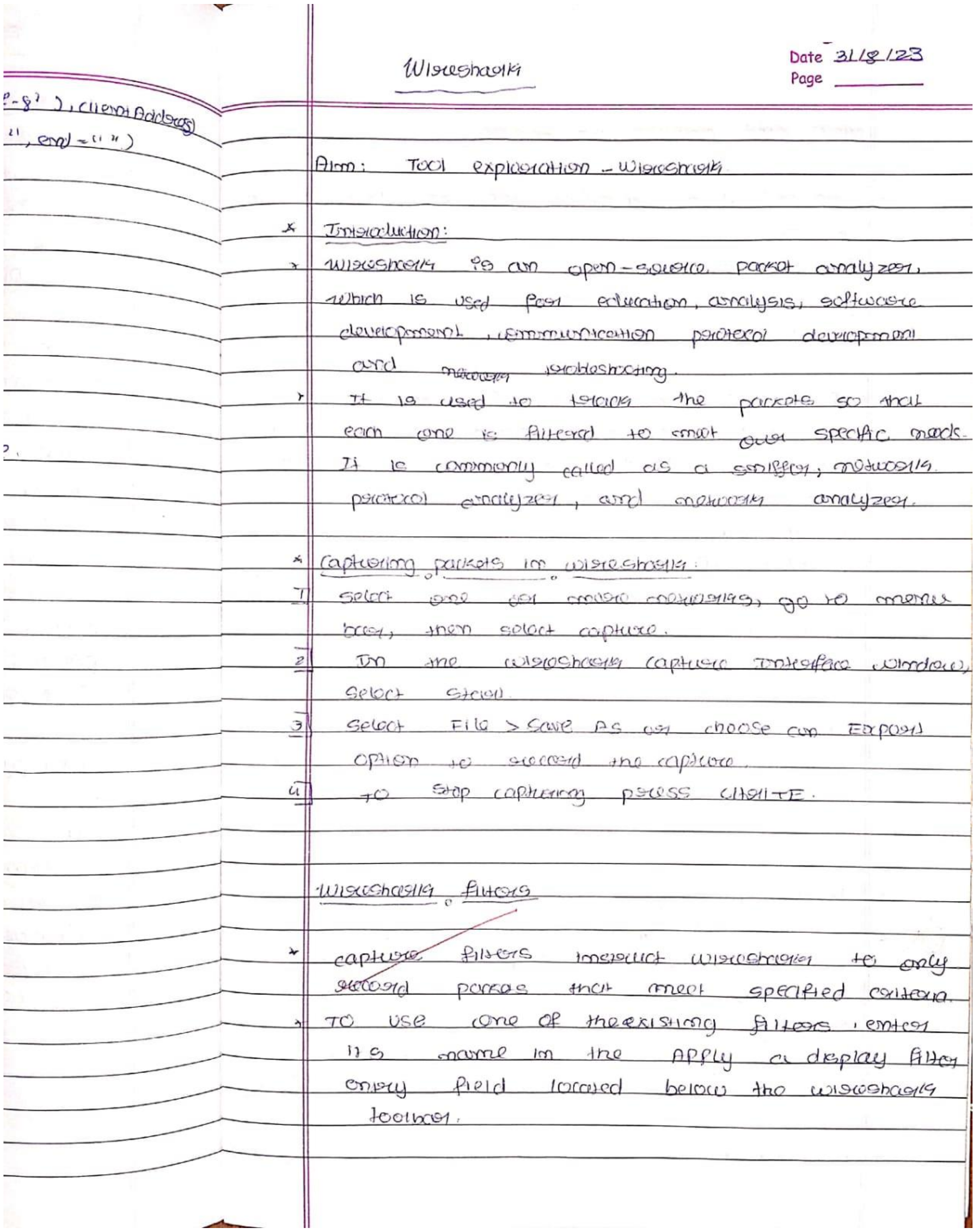
WEEK 17

Tool Exploration -Wireshark

OBSERVATION:



e-g'), client Address)

'', end = (' ')

?.

Wireshark

Date 31/8/23
Page

Aim: Tool exploration - Wireshark

* Introduction:

* 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.

* Capturing packets in wireshark:

1] Select one or more networks, go to menu bar, then select capture.

2] In the wireshark capture Interface window, select start.

3] Select File > Save As or choose an Export option to record the capture.

4] To stop capturing press Ctrl+E.

Wireshark filters

* capture filters instruct wireshark to only record packets that meet specified criteria.
* To use one of the existing filters, enter its name in the Apply a display filter entry field located below the wireshark toolbar.

View and Analyze the packets

- Captured data interface contains three main sections:

1] The packet list pane (the top section)
2] the packet details pane (middle section)
3] The packet bytes pane (bottom section)

- Packet list pane shows all packets found in active capture file. Each packet has its own row and a corresponding number assigned to it. Each packet contains
  - Timestamp
  - Source IP
  - Destination IP
  - Protocol
  - length

- The details pane, presents protocols and protocol fields of the selected packet in a collapsible format, which can be expanded on click.

- Packet bytes pane is present at the bottom of the bytes pane, which displaye the raw data of the selected packet in ~~a~~ hexadecimal bytes.

13/8/23

- Selecting a specific position of this ~~data~~ automatically highlights its corresponding section in the packet details and vice versa.
- Any bytes that cannot be printed are represented