Practical 6

Wireshark

* Theory

• Purpose :-

-> Wireshark is a packet analyzer used for network troubleshooting, analysis, communication protocol development, and security auditing.

• How it Works :

-> Wireshark captures live network traffic from a specified interface and provides detailed insights into individual packets. It allows filtering, deep inspection, and protocol analysis.

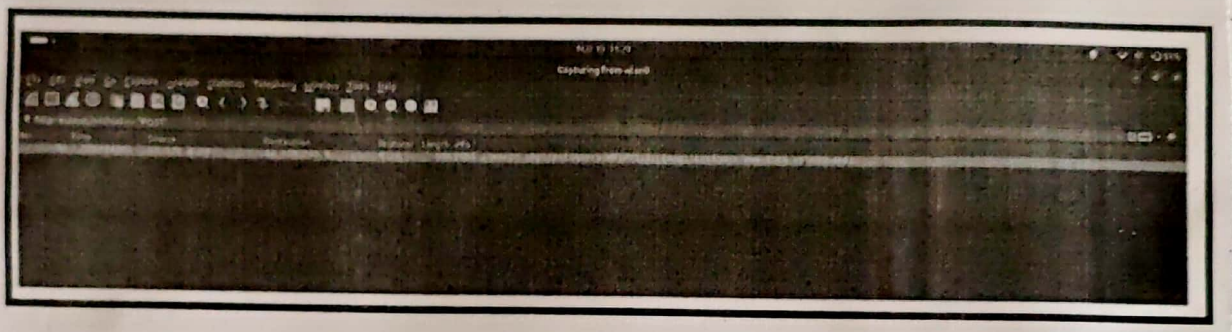
• Types of Analysis :

-> Filtering HTTP traffic :
http.request.method == "GET"

-> Analyzing DNS queries : dns.qry.name contains "example.com".

* Practical.

frame matches "youtube"



http.request.method == "POST" -> to get post request