SWARNAMALA.V **241901116**

EXP 13 DEMONSTRATE NETWORK FORENSICS USING PcapXray TOOL

AIM:

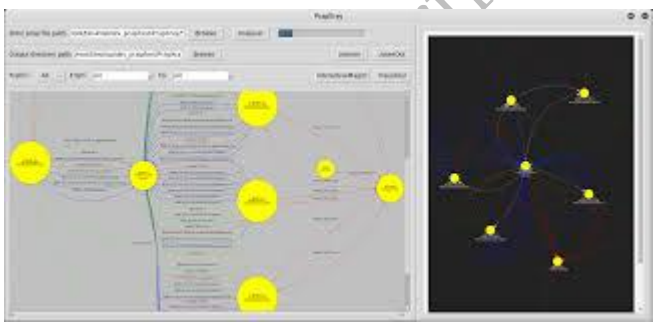
To analyze captured network traffic and reconstruct communication patterns using the PCAPXray tool, thereby demonstrating basic network forensics such as packet inspection, flow visualization, and detection of suspicious activities.

ALGORITHM :

1. **Start the PCAPXray tool** on your system.
2. **Load the PCAP file** (network capture) into the tool.
3. The tool **parses and processes the packets** in the PCAP.
4. PCAPXray automatically **generates visual graphs** showing communication flows.
5. **Inspect IP addresses, ports, and protocols** shown in the diagram.
6. Identify **suspicious connections** (unusual ports, unknown IPs, repeated failed requests, etc.).
7. Open packet details to **view payloads, headers, and metadata**.
8. **Correlate events** such as DNS queries, HTTP traffic, or anomalies.
9. Use PCAPXray's interface to **export findings or screenshots** if required.
10. **Conclude** by summarizing suspicious activities or forensic observations.

swarnamala 241901116

OUTPUT:



RESULT:

The PCAP file was successfully analyzed using the PCAPXray tool. The network traffic was visualized as a communication graph showing the interaction between different IP addresses and ports. Suspicious or unusual connections were identified by examining packet details, protocols, and flows. Thus, network forensic analysis was effectively demonstrated using PCAPXray.