| EXP NO: 13 | Network forensics with PcapXray |
|---|---|

## Aim

Visualize and analyze PCAP files to identify host relationships, file transfers, suspicious connections, and communication flows using PcapXray's visual output.

## Procedure / Algorithm

1. Produce or obtain a PCAP (tcpdump -w capture.pcap or Wireshark save).
2. Run PcapXray on the PCAP to generate a visual HTML report showing host-to-host flows and file artifacts.
3. Inspect the visual map: identify large flows, unusual external hosts, or long-lived TCP sessions.
4. Extract files discovered in HTTP/FTP flows; correlate with timestamps and client IPs.
5. Produce a short report summarizing suspicious flows and artifacts.

## Results:

PcapXray excels at giving a quick visual overview of “who talked to whom” and surfacing embedded files (HTTP downloads, SMB/FTP transfers).

- Use timestamps and pcap filters (by IP or protocol) to drill down on suspect hosts.
- Combine with tshark or scapy for automated extraction and triage.