Ex.No:
13
M.Dhivya

14/10/2025
24190 1027

DEMONSTRATE NETWORK FORENSICS USING PCAPXRAY TOOL

Aim:

To analyze captured network traffic using PcapXray and identify hosts, traffic patterns,

and suspicious network activities for forensic investigation.

Algorithm:

1. Install prerequisites:

o Install Python 3, pip, Graphviz, Tkinter, and required libraries.

o Clone the PcapXray repository and install dependencies using pip install -r

requirements.txt.

2. Prepare input:

o Obtain a .pcap file containing network traffic to be analyzed.

o Ensure the PCAP is from a safe/testing source for learning purposes.

3. Launch PcapXray:

o Open main.py in the repository using Python.

o Load the selected .pcap file via the GUI.

4. Analyze traffic:

o Observe the network graph of hosts (nodes) and connections (edges).

o Filter traffic based on Web, Tor, Malicious, DNS, or ICMP.

o Click on nodes/edges to view traffic details, HTTP requests, or extracted

payloads.

5. Record observations:

o Note suspicious hosts, unusual ports, or Tor traffic.o Check extracted files or payloads for anomalies.

o Optionally, cross-verify suspicious IPs with WHOIS or threat intelligence

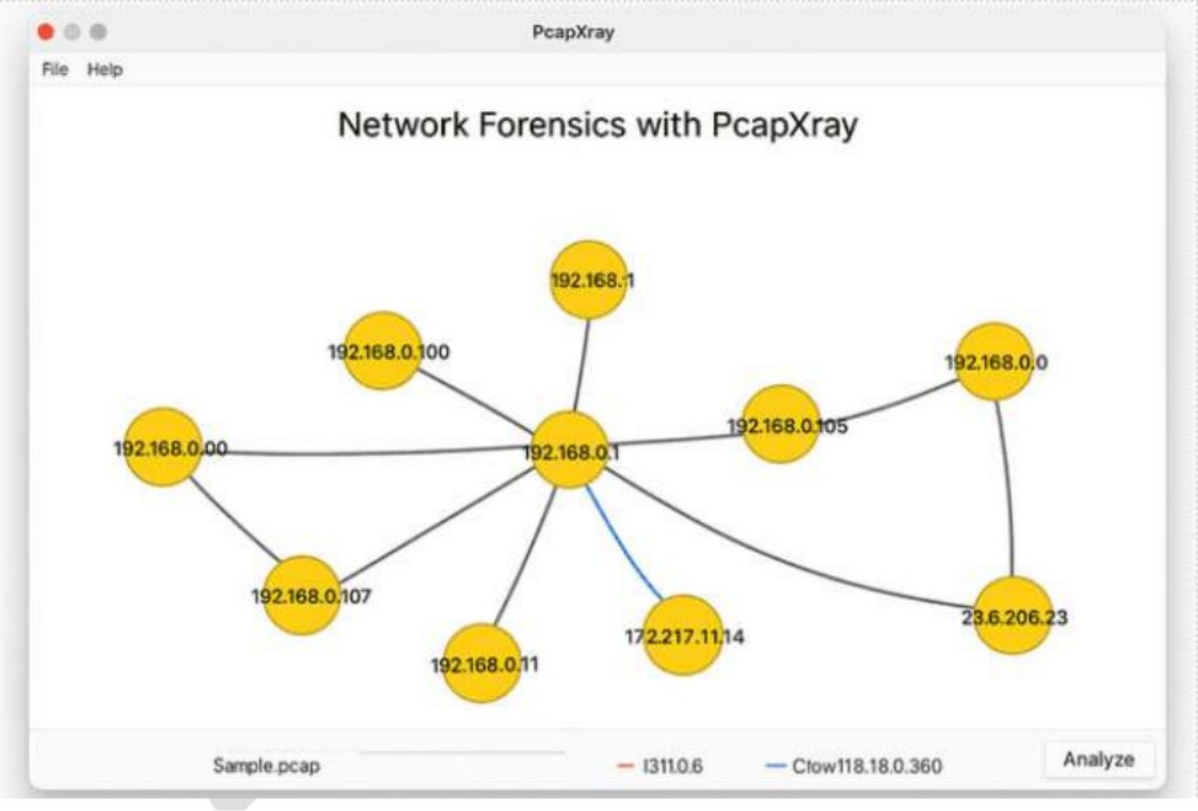
sources.

6. Document results:

o Capture screenshots of network diagrams and significant flows.

o Summarize the suspicious activities identified during analysis.

OUTPUT(status):



Result:

- Hosts with the most connections were identified as central nodes.
- Web traffic, Tor traffic, and DNS requests were visualized clearly.
- Suspicious or unusual traffic flows were highlighted for further investigation.
- Payload extraction revealed potential files or URLs of interest.