NAME: RESHMA AL

DATE:13.10.25 ROLLNO.:241901089

EXERCISE 15

DEMONSTRATE NETWORK FORENSICS USING PCAPXRAY TOOL

AIM:

To perform network forensics analysis on packet capture (PCAP) files using the PcapXray tool to visualise network traffic, identify devices, detect malicious communication, and extract important network information.

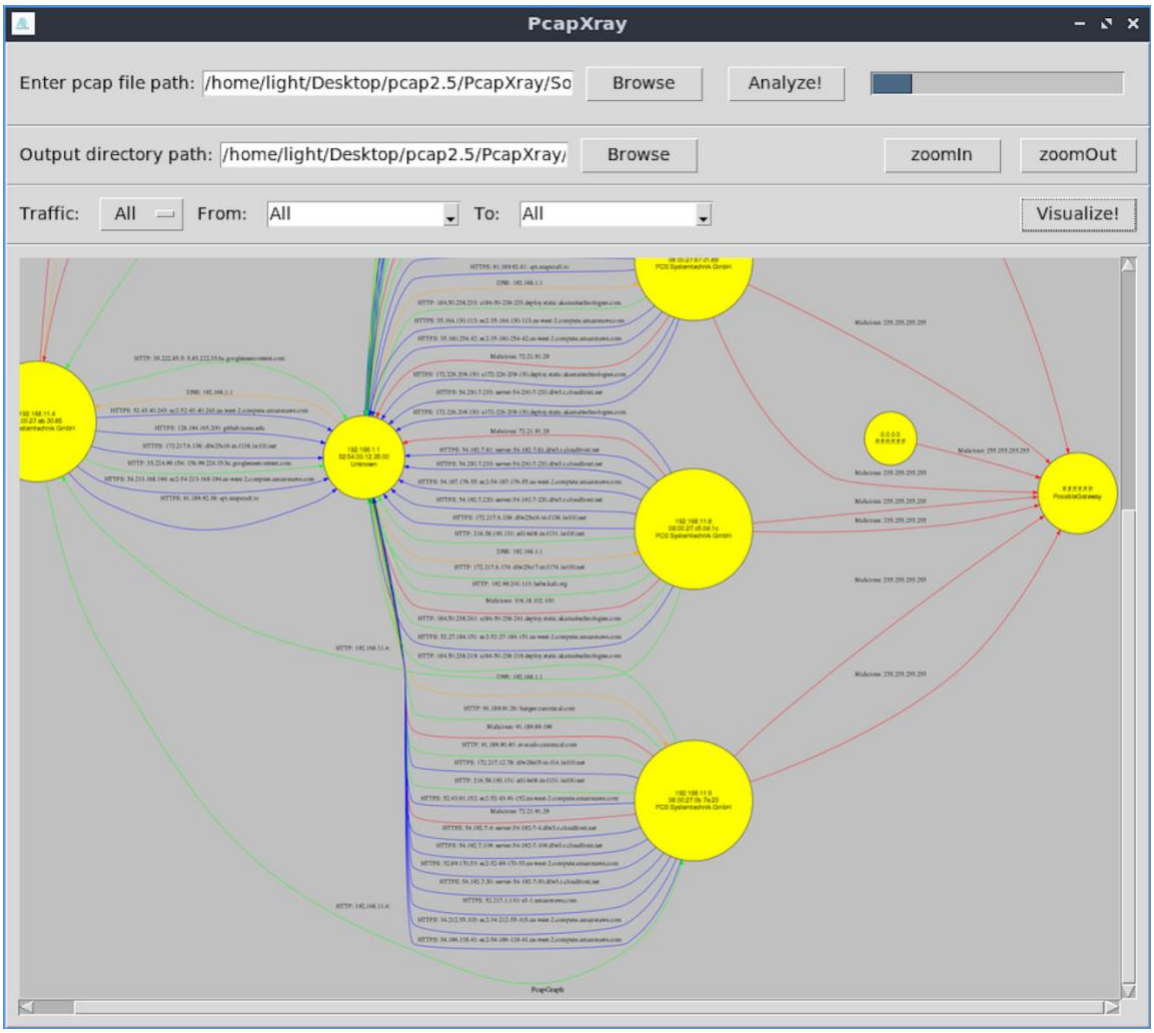
PCAPXRAY TOOL:

PcapXray is a network forensics tool that helps investigators analyze captured network traffic data (PCAP files). It takes raw packet to capture data and converts it into easy-to-understand visual diagrams and reports.

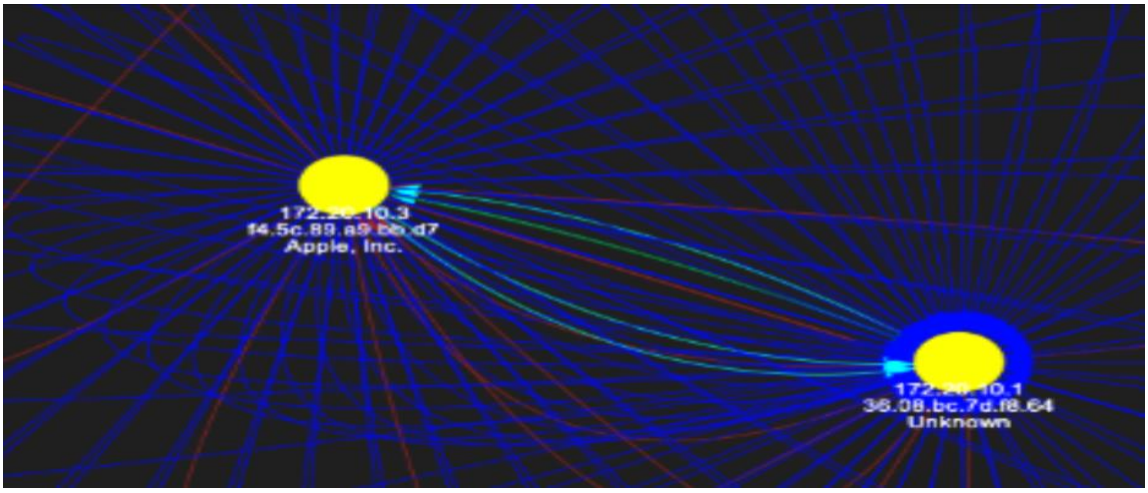
ALGORITHM:

1. **Install Prerequisites**: Install Python 3, Graphviz, and needed Python libraries (Scapy, IPwhois, Netaddr, Stem, pyGraphviz, NetworkX, Pillow, Tkinter).
2. **Clone Tool**: Clone the PcapXray GitHub repository and navigate to its directory.
3. **Launch PcapXray**: Run the tool with elevated privileges (sudo python3 Source/main.py) to open the GUI.
4. **Load PCAP File**: Use the GUI's browse button to select a PCAP file (.pcap or .pcapng).
5. **Start Analysis**: Click the “Analyze” button to begin automated parsing of packets.
6. **Packet Processing**: Tool reads packets with Scapy, extracting IPs, ports, and protocols.
7. **Lookups & Detection**: WHOIS queries run for external IPs; Tor nodes and malicious patterns get identified.
8. **Generate Visualization**: Network graph rendered showing devices as nodes and communications as edges, color-coded by protocol and threat.
9. **Create Reports**: Tool builds reports covering device details, traffic summary, payloads, and flagged suspicious activities.
10. **Review Results**: User views interactive diagrams, filters traffic types, examines reports, and exports findings.

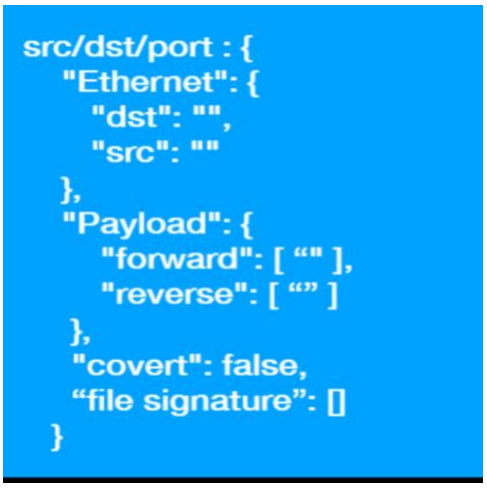
OUTPUT:



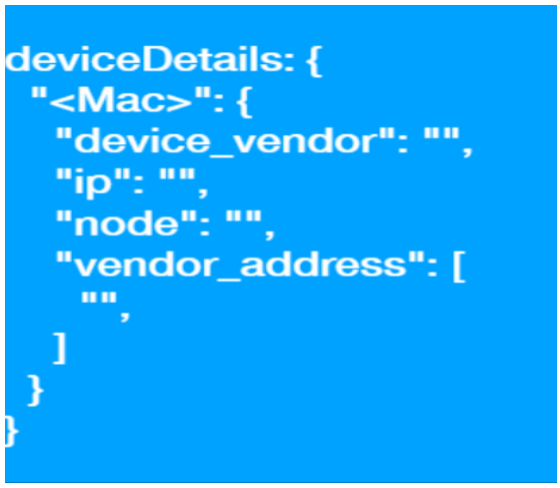
PcapXray interface showing a network traffic visualization graph from a pcap file, highlighting IP addresses and potential malware communications



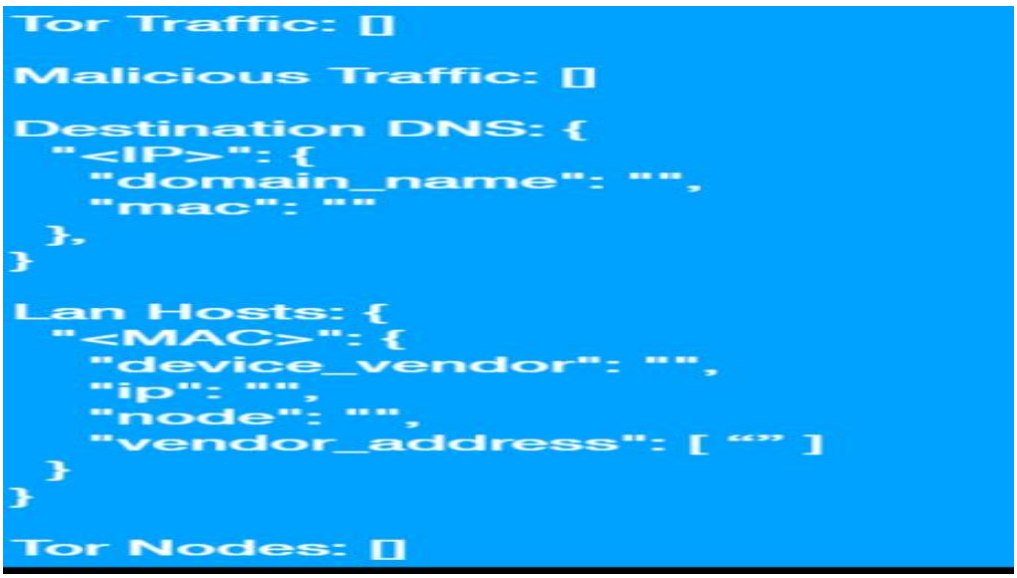
PACKET DETAILS:



DEVICE DETAILS:



COMMUNICATION DETAILS:



RESULT:

PcapXray quickly creates clear network diagrams from PCAP files, showing devices and suspicious traffic. It makes forensic analysis faster and easier for investigators.