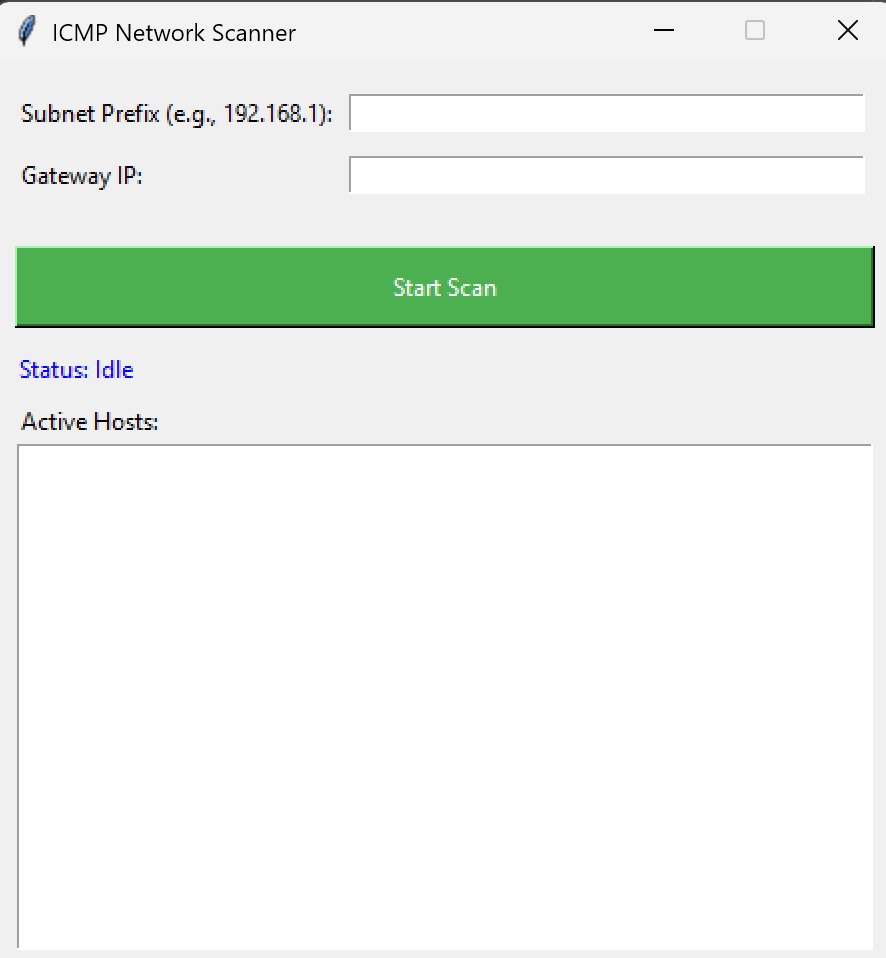
**IDENTIFICATION AND ANALYSIS OF NETWORK TOPOLOGY  
 USING ICMP FOR FORENSIC INVESTIGATION**

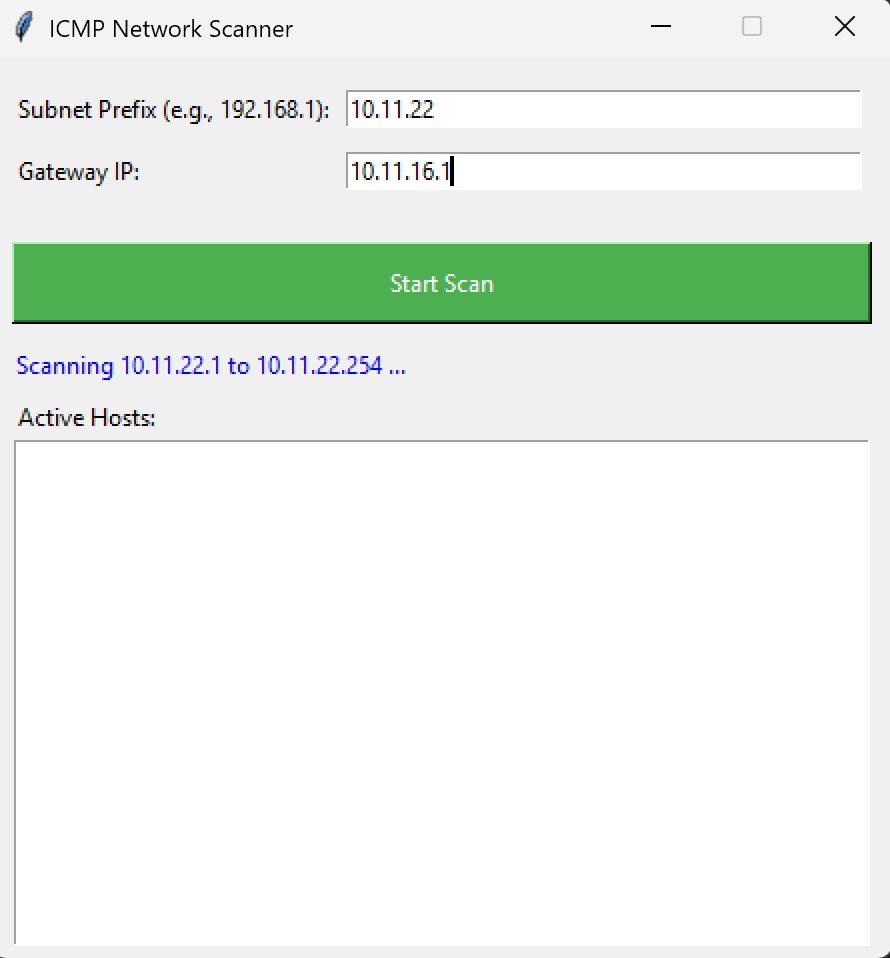
The tool opens with a user-friendly interface where users can input the subnet prefix (e.g., 10.11.22) and the gateway IP (e.g., 10.11.16.1). A button labeled “**Start Scan**” triggers the scanning process.



**Figure 1**: Initial GUI window for the ICMP scanner

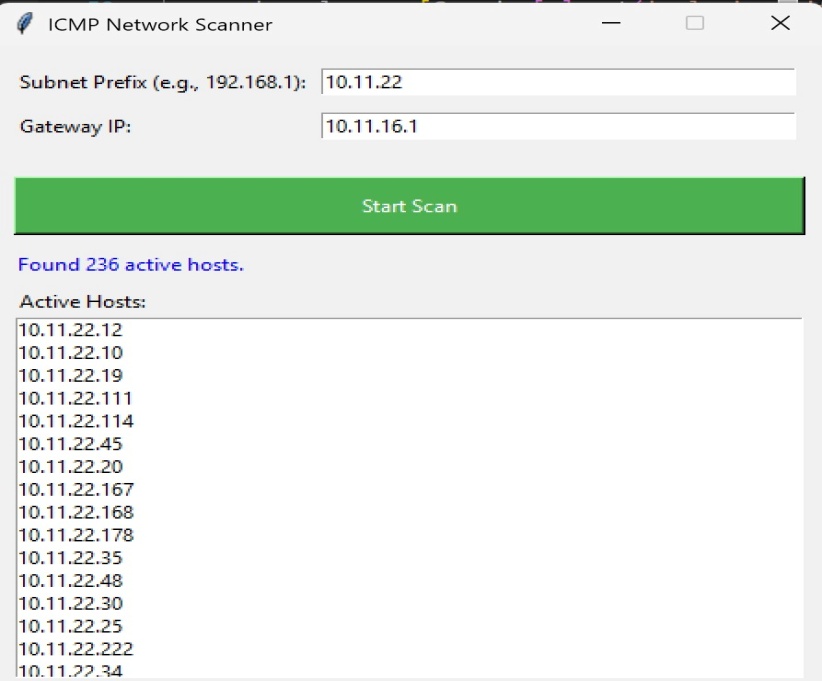
* **Scanning Phase**

Once the scan is initiated, the tool systematically sends ICMP echo requests (pings) to all IP addresses ranging from .1 to .254 within the specified subnet. It actively detects and identifies all responsive hosts on the network. Throughout the process, a scanning message is displayed, indicating the specific IP range currently under analysis, providing real-time feedback to the user.



**Figure 2**: Live scanning status displayed in the GUI

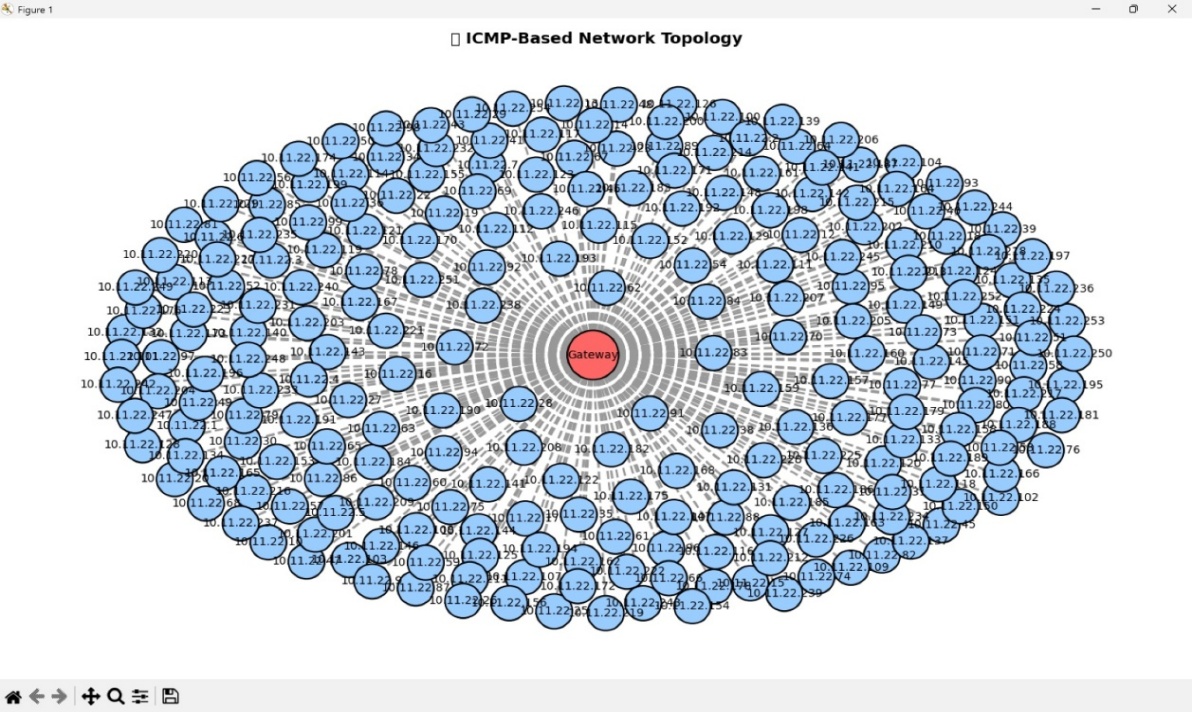
* **Active Hosts Discovery**

After the scan completes, the scanner displays the list of all active IP addresses detected within the subnet. In this case, a total of **236 active hosts** were found on the 10.11.22.0/24 subnet. These hosts are listed in the GUI under the “**Active Hosts**” section.

**Figure 3**: Display of active hosts in the scanned subnet

* **Network Topology Visualization**

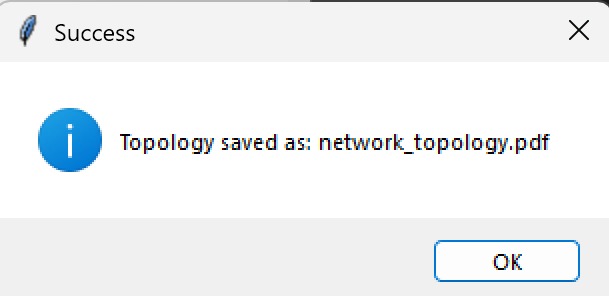
The tool dynamically generates a network topology diagram using **NetworkX** and **Matplotlib**. The central node represents the **gateway**, and all active hosts are arranged around it. Each host is connected to the gateway, indicating its reachability and presence in the network.



**Figure 4**: Automatically generated ICMP-based network topology

* **Exporting Topology as PDF**

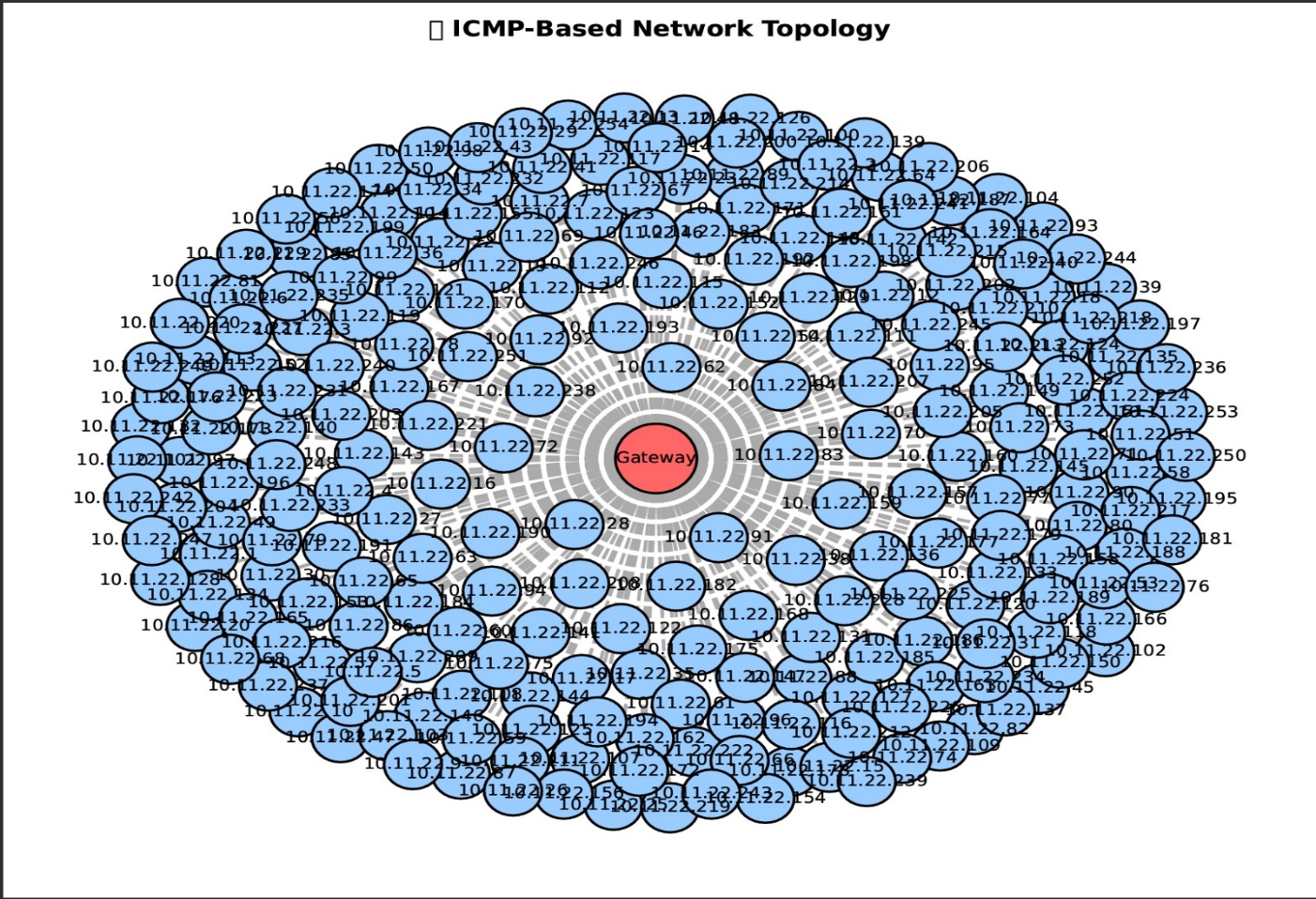
After successful topology generation, the tool provides an option to save the network diagram as a PDF file named network\_topology.pdf. A confirmation message is displayed to indicate the successful export.



**Figure 5**: Confirmation dialog after topology export

* **Final Topology Output**

The exported PDF contains a complete network graph visualizing all 236 active hosts in a circular layout around the gateway. This topology can be used for forensic analysis to detect anomalies, unauthorized devices, or unusual network structures.



**Figure 6**: Final network topology saved in PDF format