Wireshark Network Tracking with Google Maps

Name: Abhik Das

Registration Number: 22BCE8616

College Email: abhik.22bce8616@vitapstudent.ac.in

Personal Email: abhikdas0811@gmail.com

This project presents a real-time network monitoring tool that leverages packet capture data from Wireshark to visualize IP geolocation on an interactive map. The primary objective is to aid cybersecurity professionals and researchers in tracking potentially malicious IP traffic, identifying geographical trends, and generating actionable threat insights. The system uses a GUI built with Tkinter that allows users to import packet data (CSV format), filter by country, and visualize the results using Folium-powered maps. Integrated with AbuseIPDB and VirusTotal APIs, it enables real-time threat reputation analysis of each IP address. Additionally, the tool features analytics dashboards with charts and summaries for quick insights into threat levels, protocol distribution, and top attacker origins. This project bridges network data with threat intelligence and geospatial awareness, offering a visual and intuitive approach to network forensics.

Objectives

- To develop a visual tool that maps IP addresses from packet captures onto a world map.
- To identify and analyze potentially malicious traffic using external threat intelligence APIs.
- To provide network threat insights through interactive analytics and visualizations.
- To bridge the gap between raw network data and intuitive threat intelligence.

Key Features

- **Real-Time Monitoring:** Load packet captures in CSV format and view associated IP geolocations.
- **GUI Interface:** Built using Tkinter for ease of use and real-time interaction.
- **Map Visualization:** Interactive maps generated using Folium to display IP activity.

- **Threat Intelligence Integration:** AbuseIPDB and VirusTotal APIs used for checking IP reputation.
- **Analytics Dashboard:** Displays charts and summaries (threat levels, top attacker origins, protocol distribution, etc.).
- **Country Filtering:** Allows users to focus on traffic from specific regions.

Tools Used

- Language: Python
- GUI Library: Tkinter
- Visualization: Folium, Matplotlib
- APIs: AbuseIPDB, VirusTotal
- Data Source: Wireshark (CSV Export via PyShark)
- Libraries: pandas, geopy, requests