Wireshark Network Tracking with Google Maps

Name: Abhik Das
Registration Number: 22BCE8616
College Email: abhik.22bce8616@vitapstudent.ac.in
Personal Email: abhikdas0811@gmail.com

Project Report

---

1. Introduction

The rapid expansion of the internet has resulted in an exponential increase in network traffic, posing significant challenges in monitoring and securing network environments. This project, "Wireshark Network Tracking with Google Maps," addresses this challenge by integrating network packet analysis with geolocation visualization to aid in detecting and understanding suspicious IP activity in real-time.

2. Problem Statement

Traditional network monitoring tools like Wireshark provide packet-level insights but lack an intuitive interface to visualize where IP connections originate. This gap makes it harder for analysts to assess threats quickly, identify patterns, or understand the geographical spread of attacks.

3. Objective

The project aims to:

- Enable cybersecurity students and analysts to visualize source and destination IP geolocation from Wireshark captures.
- Correlate IPs with threat intelligence from AbuseIPDB and VirusTotal.
- Provide a user-friendly GUI to analyze and filter traffic by country.
- Generate maps and threat analytics to improve understanding and response.

4. Methodology

- **Packet Capture**: Wireshark is used to capture live traffic or analyze existing PCAP files.
- **Data Processing**: Packet data is exported in CSV format. Python scripts using pandas parse the source and destination IPs.
- **Threat Detection**: IPs are checked against AbuseIPDB and VirusTotal APIs.
- **Geolocation Mapping**: IPs are geolocated using external APIs and visualized on a map using Folium.
- **GUI Interface**: A Tkinter-based GUI enables users to load CSV files, filter traffic by country, and launch visualizations.

5. Findings

- Multiple packets originated from unknown or blacklisted IP addresses as flagged by AbuseIPDB and VirusTotal.
- IPs clustered from certain geographic locations were often found with high threat scores, mostly originating from specific countries.
- Bar charts helped illustrate protocol distribution (TCP, UDP, ICMP), and pie charts visualized proportions of malicious versus benign IPs.
- Filtering by country allowed focused inspection of regional network behavior and threat patterns.
- The use of APIs ensured real-time lookup, allowing up-to-date reputation insights for each source IP.
- During testing with a 20000-packet CSV export, approximately 6% of IPs were flagged as suspicious by AbuseIPDB, originating from regions in the United States. VirusTotal API confirmed several hits as hosting malware or botnet activity.

6. Conclusion

This project demonstrates how network packet data can be transformed into actionable intelligence by combining geolocation and threat detection APIs. It empowers users to:

- Identify suspicious or malicious IP activity.
- Understand the geographical spread of their network connections.
- Visualize and summarize traffic patterns intuitively.

The tool proves especially useful in educational environments and entry-level threat analysis roles, providing a bridge between traditional packet inspection and modern, visual-based cyber threat understanding.

7. Future Work

- Integrate real-time packet capture and map refresh.
- Add support for alert generation based on threat score thresholds.
- Expand visualizations with time-based traffic analysis and clustering.
- Implement multi-map views or export options for PDF/HTML reporting.

8. Summary and Experience

Screenshots of the generated map visualizations and analytics dashboard are included in the project ZIP submission. The application gracefully handles API failures or malformed CSV data by displaying appropriate error messages in the GUI. Working on this project provided hands-on experience with packet analysis, API integration, and GUI development, bridging theoretical cybersecurity knowledge with practical application.