Wireshark Network Tracking with Google Maps

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

System Requirements and Specifications

---

1. Hardware Components

- **Processor:** Dual-core or better (Intel i3/i5/i7, AMD Ryzen, etc.)
- **Memory:** Minimum 4 GB RAM (8 GB recommended for handling large PCAP files)
- **Storage:** At least 200 MB free disk space (more if storing large capture files)
- **Display:** Standard monitor (for GUI)
- **Network:** Ethernet/Wi-Fi adapter (required for capturing network traffic with Wireshark/tshark)

2. Software Tools and Versions

- **Operating System:**
    - Windows 10/11
    - macOS 10.15+ (Catalina or later)
    - Linux (Ubuntu 18.04+, Fedora 30+, etc.)
- **Python:** 3.7 or higher
- **Python Packages (Install via pip):**
    - pandas (tested with 1.3.x+)
    - tkinter (usually included with Python, for GUI)
    - matplotlib (tested with 3.4.x+)
    - folium (tested with 0.12.x+)
    - requests
    - ipaddress
- **Other Tools:**
    - **Wireshark** (for capturing and exporting CSV files)
      Version: 3.x or later recommended

3. Network and Other Dependencies

- **Internet Access:** Required for:
    - Retrieving geolocation data via public APIs (e.g., ip-api.com)
    - Threat intelligence lookups (AbuseIPDB, VirusTotal APIs)
    - Downloading Python packages and dependencies
- **API Keys:**
    - AbuseIPDB and VirusTotal require free API keys (place them in tracker.py or as environment variables as needed).

4. Special Configurations

- **Wireshark Configuration:**
    - Set up Wireshark to capture network packets.
    - Export your capture as CSV with columns for at least "Source" and "Destination" IPs (required by the scripts).
- **API Keys Configuration:**
    - Place your AbuseIPDB and VirusTotal API keys in tracker.py or configure as environment variables if you wish to keep them secret.
- **Firewall/Antivirus:**
    - Allow traffic for API calls (ip-api.com, AbuseIPDB, VirusTotal).
    - Permit local GUI applications (Tkinter) to run.
- **CSV File Format:**
    - The CSV should have columns named Source and Destination for IP extraction.
    - If using PCAP, you must export it to CSV format (Wireshark: File > Export Packet Dissections > As CSV).

Optional (for advanced use or development)

- **PyShark:** Only needed if you want to parse PCAP files directly in Python.
- **Tshark:** (Wireshark CLI) for automated/scripted packet capture or export.

Summary Table

COMPONENT	REQUIREMENT/VERSION
CPU	Dual-core+
RAM	4 GB+
OS	Win10+, macOS 10.15+, Linux 18.04+

PYTHON	3.7+
PANDAS	1.3+
MATPLOTLIB	3.4+
FOLIUM	0.12+
REQUESTS	Any recent
TKINTER	Included
WIRESHARK	3.x+
INTERNET ACCESS	Required
API KEYS	AbuseIPDB, VirusTotal