GURUGRAM CYBER POLICE

Keeping Gurugram Cyber Safe

GURUGRAM POLICE CYBER SECURITY SUMMER INTERNSHIP

GPCSSI-2025

{Advanced IP-Scanner Tool}

Submitted To:

Dr. Rakshit Tandon

(GPCSSI Mentor and Coordinator)

Submitted By:

Aman Chauhan (CW034)

Samay Kumar (CW320)

Sonu Kumar (CW362)

Advanced IP Information Scanner Tool

➢ PROBLEM STATEMENT

- Cybersecurity professionals, ethical hackers, and law enforcement often require quick access to real-time IP data (e.g., location, ISP, ASN, etc.) for reconnaissance, tracking, or incident response. Manual methods or online IP lookup tools are often slow and inefficient for bulk analysis. A fast, automated, and report-generating tool is needed to streamline the process.

➢ SOLUTION

- We developed a **Flask-based Advanced IP Scanner Tool** that performs fast IP intelligence lookups, supports bulk IP submission, and generates professional reports in PDF format. It can extract key IP metadata such as country, city, ISP, ASN, coordinates, and time zone with multi-IP processing capabilities. The tool also maps IPs on Google Maps and is suitable for forensic reporting, OSINT, and real-time investigation

➢ TOOLS & TECHNOLOGIES USED:

CATEGORIES	TOOLS & TECHNOLOGIES
BACKEND	*Python 3,Flack*
FRONTEND	*HTML, CSS(Static UI)*
LIBRARY	***requests, fpdf2, json, os, datatime, threading***
DEPLOYMENT	*Localhost (127.0.0.1:5000) on kali Linux*
PDF REPORT	***Fpdf2*** *For structure report generation*
DATA SOURCE	*IP Geolocation APIs (ipinfo.io / ip-api.com)*

➢ FEATURES:

1. Single and Bulk IP Scanning Support

- The tool is designed to handle both individual and multiple IP address inputs. Users can manually enter one or more IP addresses (comma-separated) or upload a text file containing a list of IPs. This dual input mode enhances flexibility and usability in real-world reconnaissance or investigative operations

2. Advanced IP Intelligence Retrieval

- Each IP is processed through an external API (e.g., **ip-api.com**), which returns detailed metadata, including:
  - **City and Region**
  - **Country and Postal Code**
  - **Latitude and Longitude**
  - **Internet Service Provider (ISP)**
  - **Autonomous System Number (ASN)**
  - **Time zone information**
- This data is crucial in OSINT tasks, cyber investigations, and geolocation mapping.

3. File Upload for Batch IP Scanning

- The scanner supports uploading a **.txt** file containing multiple IP addresses (one per line or comma-separated). Once uploaded, the tool processes all entries in sequence or in parallel, depending on threading logic. This feature is ideal for bulk IP analysis during audits or threat intelligence operations.

4. Professional PDF Report Generation

- After scanning, users can generate a well-structured and exportable PDF report using the **fpdf2** library. The report includes:
  - Timestamp of generation
  - All scanned IPs with their metadata
  - Clean formatting with table-style layout
  - Easy to archive, share, and print for further use in documentation, evidence, or presentations.

5. Google Maps Geolocation Integration

- Each scanned IP's coordinates (latitude and longitude) are linked to Google Maps, enabling direct visual location checks. This feature aids in quickly identifying the physical region associated with the IP address—critical for field verification, network tracing, or cyber law enforcement tracking.

---

6. Multi-threaded Performance Optimization

- To enhance speed and responsiveness, the tool uses multithreading during batch IP processing. This parallel execution significantly reduces total scan time, especially useful when scanning hundreds of IPs in a single session.

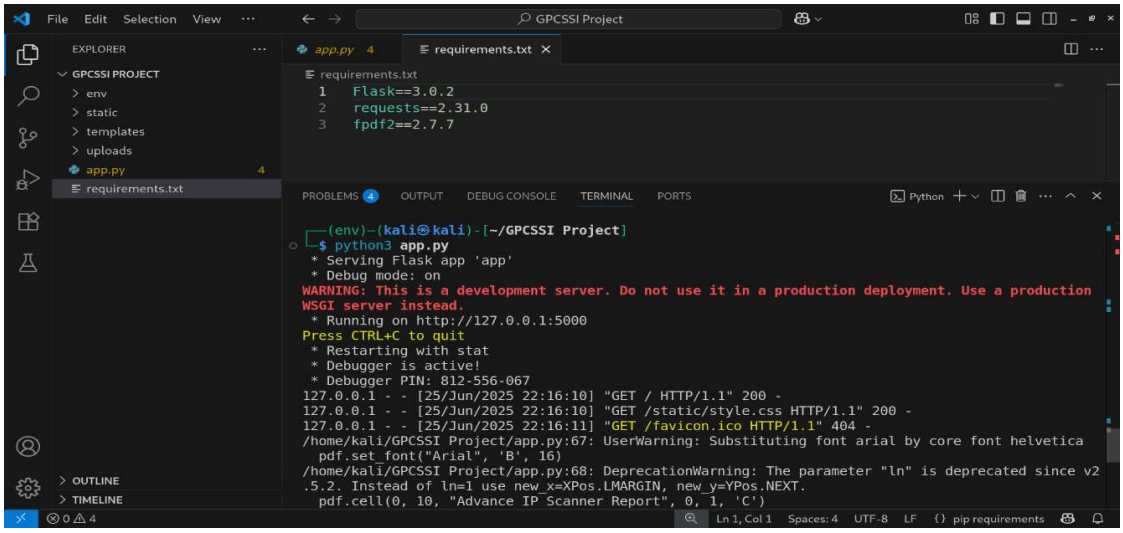
---

7. Flask-based Web Interface

- The entire application is deployed via a **Flask** server and accessible on localhost:5000. It features:
  - A clean, user-friendly interface
  - IP input forms and file upload options
  - Result display and report download button
  - This ensures accessibility even on low-resource systems and does not require cloud hosting, making it secure and offline-compatible.

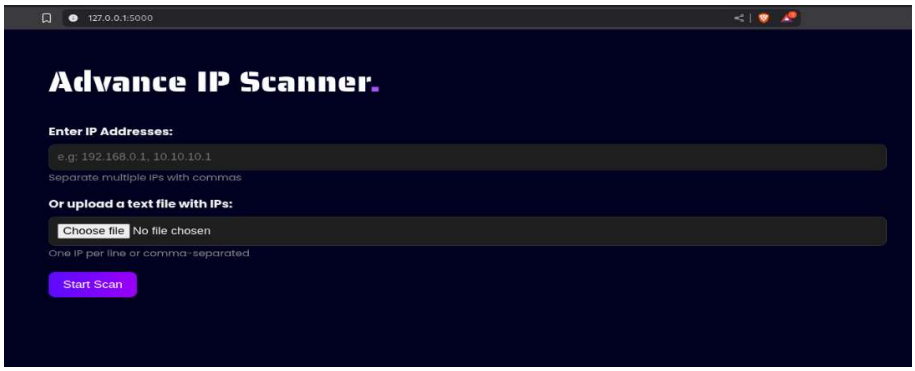
Project Execution in Terminal

- The project is executed on Kali Linux using **python3 app.py**. Flask server is running on localhost with necessary libraries like Flask, requests, and fpdf2.



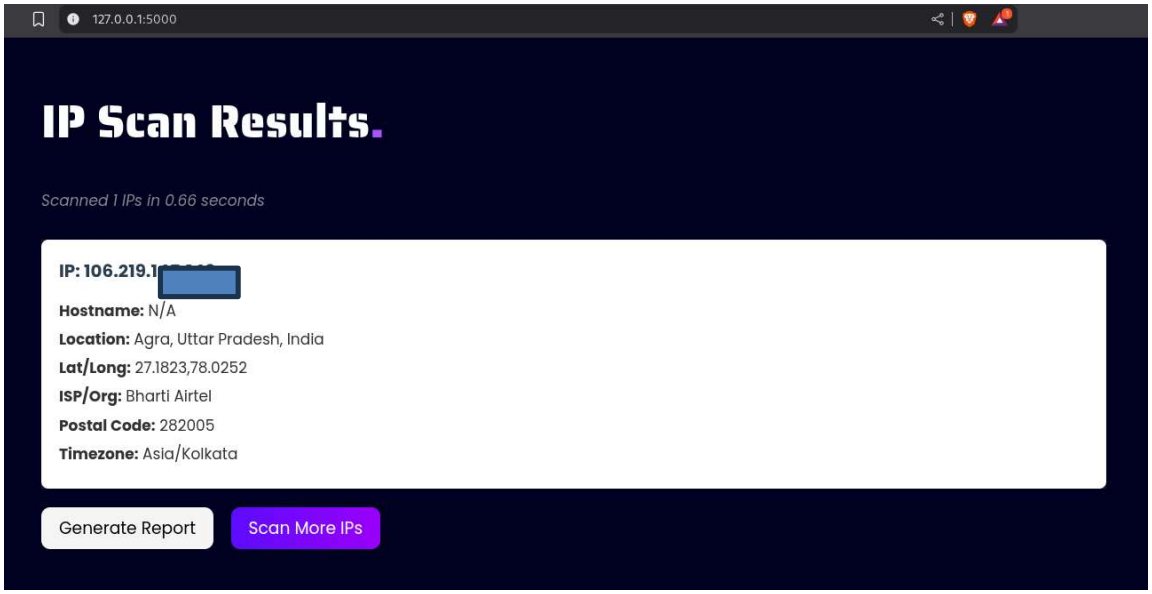
IP Scanner Interface (Input)

- User interface to input **IP addresses** manually or via uploading a **.txt** file. Once submitted, the scan begins.



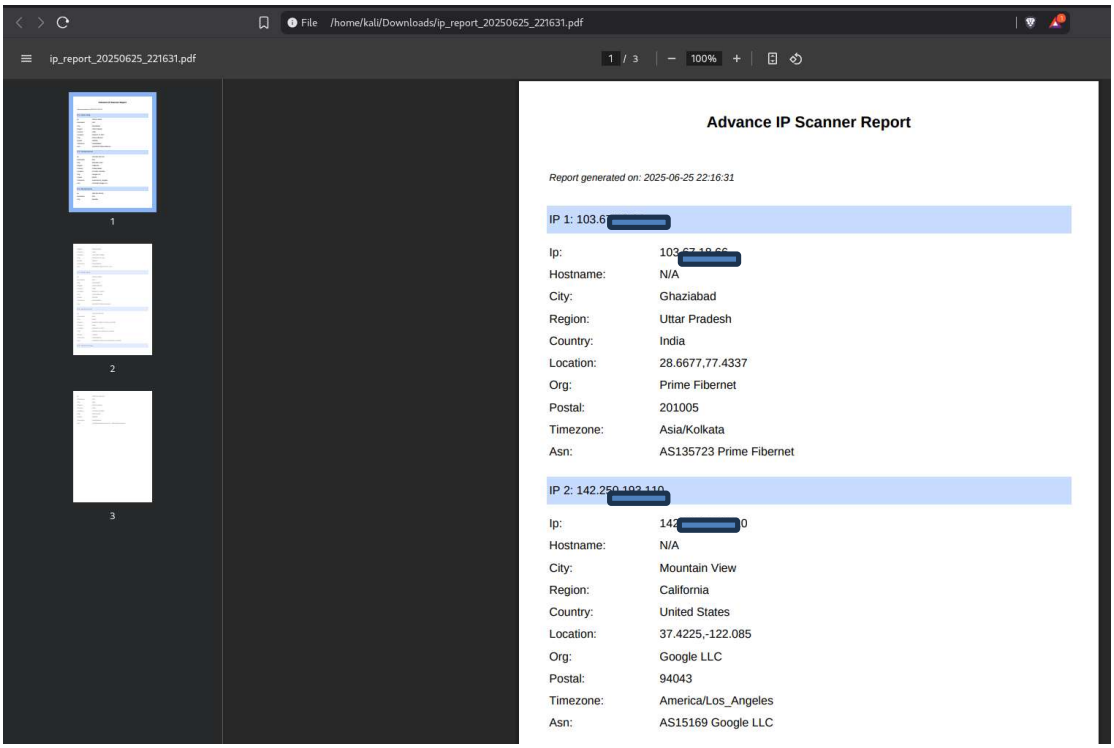
Scan Result UI

- After scanning, results are displayed on the screen showing IP address, city, country, ISP, and more.



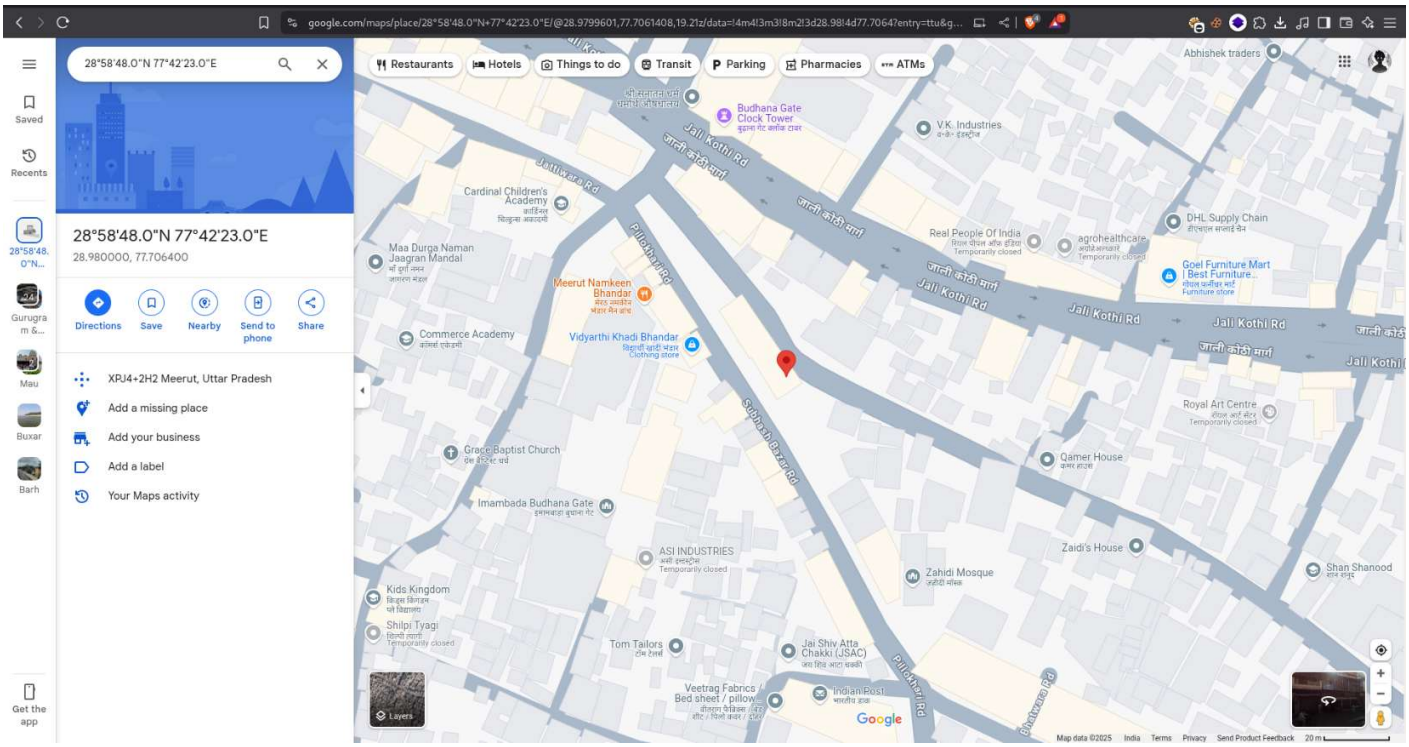
PDF Report Output

- The tool generates a well-formatted PDF report with all IP details which can be saved and used for investigation.



Google Maps Geolocation View

- Google Maps integration showing the IP's location using its latitude and longitude. This helps visualize physical presence.



Workflow

- The working of the **Advanced IP Scanner** follows a clear and efficient step-by-step flow:
  1. **User Input:**
     The user either enters one or more IP addresses manually or uploads a .txt file containing IPs.
  2. **Backend Processing with Flask:**
     The Flask backend receives the input, then initiates API calls to fetch geolocation and network metadata for each IP.
  3. **Data Parsing & Display:**
     The fetched data is parsed and displayed neatly on the web interface, showing location, ISP, ASN, time zone, etc.
  4. **Report Generation Trigger:**
     Upon clicking the "Generate Report" button, the backend formats the data using the fpdf2 library.
  5. **PDF Creation & Storage:**
     A clean, downloadable PDF report is generated, timestamped, and offered for saving.
  6. **Optional Visual Mapping:**
     Each IP's latitude and longitude are linked to Google Maps, allowing optional visual verification of the location.

Future Scope

- To enhance the capabilities of this tool, several future upgrades can be considered:
  - **Shodan or Censys Integration:**
    Add support for gathering open ports, banners, and known vulnerabilities using Shodan/Censys APIs.
  - **Authentication & Role-based Access:**
    Implement login systems with admin/user roles to make the tool secure and trackable.
  - **AI-Powered IP Anomaly Detection:**
    Integrate machine learning models to detect suspicious patterns in IP metadata or behaviour.
  - **Global Map Visualization:**
    Use libraries like Folium or Plotly to visualize all scanned IPs on an interactive world map.

Conclusion

The **Advanced IP Scanner** project effectively demonstrates how Python and Flask can be combined to create practical tools in the field of cybersecurity. It simplifies the process of gathering and organizing IP intelligence, provides a professional output in the form of downloadable PDF reports, and offers a user-friendly web interface.
With potential enhancements such as AI integration, port scanning, and interactive mapping, this project can evolve into a complete OSINT and forensic support toolkit — making it highly valuable for cybersecurity teams, law enforcement, and digital investigators.