

GeoIP Forensics Console

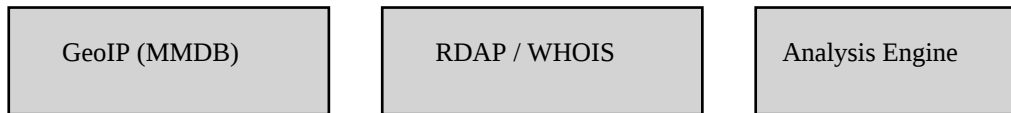
Operations Manual & User Guide

Version 1.1.0 — Locked Release

Comprehensive operational guide for investigative and analytical workflows.

Chapter 1 — Introduction & Architecture

GeoIP Forensics Console integrates local GeoIP databases, RDAP, WHOIS, CIDR derivation, Tor heuristics, confidence scoring, and ASN clustering into a single offline-capable workstation.



Chapter 2 — Installation & Setup

1. Extract the archive.
2. Create a virtual environment (recommended).
3. Install dependencies: `pip install -r requirements.txt`
4. Launch with: `python3 main.py`

Chapter 3 — Single IP Workflow

Step 1: Enter target IP. Step 2: Click RUN ALL. Step 3: Review GeoIP results. Step 4: Review CIDR/RDAP data. Step 5: Review Analysis tab. Step 6: Export report if needed.

Chapter 4 — Analysis & Confidence Scoring

Confidence scoring measures agreement between GeoIP, ASN, and RIR country attribution. Hosting and proxy signals reduce confidence.

Chapter 5 — Batch Mode & ASN Clustering

Batch mode processes multiple IPs and groups them by ASN to identify infrastructure density and cross-region activity.

Chapter 6 — Reports & Evidence Handling

Reports generate JSON and TXT artifacts stored in the reports directory. Exports are manual and operator-triggered.

End of Manual — GeolP Forensics Console v1.1.0