SPYRIOT SECURITY
CYBER INTELLIGENCE AGENCY

Enroll Now

Based on Real-World Practical Training

Cyber Intelligence Online Training Program

A comprehensive practical training program designed for aspiring cyber investigators, security professionals, and law enforcement enthusiasts — covering Cyber Crime Investigation, Cyber Security, Ethical Hacking, and Digital Forensics.

12	TOTAL UNITS
02	LEVELS
2	MONTHS
Live	ONLINE
100%	PRACTICAL

LEVEL 01 · FOUNDATION

Foundation Training

UNITS	Unit 01 – 06
DURATION	1 Month
FEE	₹5,000

LEVEL 02 · ADVANCED

Complete

Complete Advanced Training

UNITS	**Unit 01 – 12**
DURATION	**2 Months**
FEE	**₹6,999**

Monday – Friday
7:00 PM – 9:00 PM · Live Training

Saturday & Sunday
Practical Tests & Assignments

Mode
100% Online · Live Sessions

LEVEL 01 **Foundation Training**

⊞ Expand All

UNIT 01 **The Detective Mindset** ▶
Crime Pattern Analysis & the Framework of Cyber Law

- How to think like a cyber detective and understand the digital crime ecosystem.
- How to study criminal mindset, behavior patterns and investigation workflows.
- How to gather initial case details, evidence, and classify the type of cybercrime.
- How to understand Indian Cyber Laws: IT Act 2000, IPC sections & legal processes.
- How to choose where to report a case: Police, Cyber Cell, or Government Portal.

UNIT 02 **Open-Source Intelligence & Anonymity** ▶
Techniques for Criminal Background Investigation & Digital Profiling

- How to avoid OSINT mistakes, digital exposure, and identity leakage.
- How to stay anonymous using secure browsers & encrypted communication.
- How to create an undercover agent online identity for cyber investigations. (Ethically)
- How to track websites' past online activities using OSINT safely and legally.
- How to investigate email breaches, identity leaks & username traces.

UNIT 03 **Follow the Digital Footprint** ▶
Information Gathering from Websites, Social Media, Phone Numbers & Background Records

→How to find digital footprints using social media profiling (FB, IG, Telegram, LinkedIn).

→How to investigate phone numbers for identity clues, scam patterns and digital trails.

→How to perform domain investigation of a criminal website using OSINT tools.

→How to trace fake profiles, fake websites & online scam operations.

→How to perform reverse image search to get hidden information about a target.

UNIT 04 **Track, Locate & Investigate** ▶

Geo-Location Techniques & Forensic Evidence Collection in Cyber Crime Investigations

→How to use geolocation investigation tools to re-create the crime scene.

→How to authenticate screenshots, chats, images & metadata legally.

→How to trace GPS location of an image using metadata extraction techniques.

→How to document & store digital evidence without tampering.

→How to file a cybercrime complaint with proper evidential format.

UNIT 05 **Cyber Investigation Mastery** ▶

Kali Linux Techniques & Dark Web Exploration

→How to conduct a lawful network scan on an authorized target using Nmap.

→How to manage and organize data efficiently in Kali Linux for forensic workflows.

→How to capture unencrypted HTTP traffic on a LAN to identify credential exposure.

→How to forward network ports securely to access authorized systems over WAN during investigations.

→How to configure TOR, VPN & multi-layer anonymity for secure access.

→How to access the dark web safely and legally using proper OPSEC protocols.

→How to explore darknet marketplaces safely without identity exposure.

→How to analyze darknet case studies & recognize criminal behavior patterns.

UNIT 06 **Unmasking the Digital Lie** ▶

Deepfake Crime Investigation, Hidden Data Extraction & Malicious File Forensics

→How to investigate deepfake videos / images using face recognition analysis tools.

→How to extract hidden digital evidence from mobile devices and computers.

→How to analyze browsing history, deleted files & forensic artifacts.

→How to investigate unknown / suspicious files to trace malware behavior.

→How to investigate malicious files & identify payload behavior patterns.

→How to investigate system crashes or corrupted data during forensic analysis.

LEVEL 02 **Advanced Training**

⊞ Expand All

UNIT 07 **Vulnerability Analysis & Bug Bounty** ▶

Malware & Virus File Investigation in Hacked Systems

- How to detect hidden vulnerabilities in a weak web application using AI tools.
- How to begin bug bounty hunting with different platforms.
- How to write a professional vulnerability report.
- How to perform malware file-binding methods used to attach viruses with documents.
- How to perform reverse engineering of an Android app for malware investigation.
- How to investigate malicious (.apk) files for Android security. (Penetration Testing)

UNIT 08 **Android Hacking & Investigation Techniques** ▶

Mobile Crime Investigation — Legally & Ethically

- How to conduct authorized Android penetration testing to evaluate mobile security.
- How to investigate Android malware & malicious apps using static/dynamic analysis.
- How to investigate Android log files to trace unusual activities over the device.

UNIT 09 **Windows System Hacking & Investigation Methods** ▶

Ethical Penetration Testing & Forensic Analysis (Educational Purpose)

- How to perform a legal penetration test or gain full access on a Windows system.
- How to hack a Windows system using USB autorun (Ethically) for endpoint protection.
- How to build RAT (Trojan / Malware / Virus / Ransomware) for crime investigation.
- How to recover RAM memory or temporary data inside the Windows system.
- How to investigate a hacked Windows system using log analysis.

UNIT 10 **Women's Safety & Digital Protection** ▶

Investigating Harassment, Cyberbullying & Blackmailing Cases

- How to investigate blackmail, online harassment & cyberbullying cases.
- How to analyze cyberstalking patterns & cross-platform digital footprints.
- How to collect evidence for digital blackmail & extortion.
- How to investigate fake social media profiles using metadata & link analysis.

→How to deactivate / delete fake Instagram / Facebook accounts used for blackmailing.

→How to investigate online sexual harassment or exploitation ethically and legally.

→How to conduct cyberbullying investigations using timestamps & chat logs.

→How to detect deepfake & AI-generated scam content using forensic tools.

UNIT 11 **Fake Scams, Phishing & Financial Fraud** ▶

Investigating Fake Websites, Financial Crimes & Identity Theft

→How to investigate online financial fraud by tracing transaction trails.

→How to investigate fake loan & investment scams using domain & hosting OSINT.

→How to investigate e-commerce & marketplace frauds.

→How to investigate phishing & fake job scams using email header & URL analysis.

→How to investigate identity theft, KYC misuse & linked identifiers.

UNIT 12 **Location Tracking & Case Documentation** ▶

Final Investigation Reporting & Real-Case Simulations

→How to trace a criminal's IP Address using a Honey-Trap undercover operation.

→How to track a criminal's exact GPS-coordinate location using undercover operations.

→How to write an investigation summary & attach digital evidence.

→How to prepare a professional cyber investigation report for law enforcement.

→How to conclude findings, recommendations & case closure format.

→How to work on real-case simulations & handle complaints like a professional investigator.

Bonus Included with Level 02

Premium Ethical Hacking & Investigation Toolkit — a curated collection of professional-grade tools, templates, and resources used by real cyber investigators.

Ready to Start Your Cyber Intelligence Journey?

Join professionals from India, Afghanistan, Germany, Nigeria and more. Enroll today and gain real-world cyber investigation skills.

Enroll via WhatsApp | Download Syllabus

Cyber Intelligence **12 Units** **2 Levels** Based on Real-World Practical Training **Spyriot Security Pvt. Ltd.**