



CYBER DETECTIVE



CRIME SCENE - DO NOT CROSS CRIME SCENE - DO NOT CROSS

Become A Private Cyber Crime
Investigator



ABOUT THE MASTER COURSE :

- **Total Modules:** 12 (Focused on Open-Source Intelligence)
- **Duration:** 1 Month
- **Mode:** Live Online Classes
- **Course Fee:** ₹5,999
- **Installment Option:**
 - ₹500 (One-time Admission Fee — adjusted in the total fee)
 - ₹2,500
 - ₹2,999
- **Class Timings:** 8:00 PM – 10:00 PM (Monday to Saturday)
- **Internship:** 1-Month Project-Based Cyber Forensics Internship Included

WHY ENROLL IN THIS COURSE ?

- **Hands-on training + Cybercrime Investigation Internship.**
- **ISO certified certification.**
- **Cybercrime investigation officer ID card.**
- **Cyber forensics software toolkits + study materials.**
- **Future support for students.**

CONTENTS

UNIT 01: Cyber Crime & OSINT – Detective Foundations

- Step into the world of cybercrime and understand the role of a cyber crime investigator.
- Collect digital evidence and follow the trail like a real cyber detective.
- Use OSINT tools (like Google & social media) to track online activities.
- Analyze famous cyber attacks to uncover clues and learn real lessons.

UNIT 02: Psychological Trap: Mind Games & Social Engineering Tactics

- Investigate how hackers manipulate people using psychology and tricks.
- Reverse social engineering: force cybercriminals to reveal their secrets.
- Detect emotional traps like fear, urgency, and greed used in online scams/cyber crime.
- Create undercover digital identities to hunt down cyber criminals.

UNIT 03 : Social Media Crime Investigation – Digital Evidences Hunting

- Crack cases of online blackmail, sextortion, and fake accounts with cyber forensics.
- File effective cybercrime reports and support victims with proper action.
- Extract social media evidence like a skilled cyber crime investigator.
- Trace and remove revenge pornography content-unmask the person behind it.
- De-activate fake social media profiles quickly with takedown strategies.
- Sextortion cases involving minors: special investigation protocols, a sensitive approach to handling underage victims.

UNIT 04 : CCTV Footage Investigation – Visual Crime Solving

- Analyze CCTV footage to identify suspects, vehicles, and crime scenes.
- Enhance low-quality videos to reveal hidden details.
- Recover key evidence from blurry or unclear footage.
- Stabilize crime scene videos for use in legal investigations.
- Examine photo metadata to track GPS location, date, and device info.

UNIT 05: Digital Footprint Tracing & Identity Verification

- Conduct PAN card verification for cyber identity investigation.
- Validate doctors' identities through official medical council databases.
- Perform smart name-based background checks and gather supporting digital evidence.
- Use government records to trace individuals by full name and date of birth.
- Employ social media intelligence (SOCMINT) to build digital suspect profiles.
- Extract and analyze public footprints with precision—just like digital forensics officers.

UNIT 06: Website Tracking & Domain Ownership Investigation

- Identify domain owners using WHOIS for cybercrime case building.
- Monitor suspicious website traffic like a cybercrime surveillance expert.
- Validate SSL/TLS certificates to verify site authenticity.
- Detect malicious scripts and conduct digital forensics on websites.
- Recover deleted or modified web content for legal investigations.
- Trace server locations using IPs to assist in takedown operations.
- Support cyber police in shutting down fake, scam, and criminal websites.

UNIT 07: Email Tracing & Cyber Forensics Investigation

- Extract and examine email headers to trace routing paths like a cyber detective.
- Detect spoofed or fake emails used in fraud or phishing.
- Perform IP tracing from email servers to locate the sender's real-world origin.
- Map IPs to physical locations using forensics-grade geolocation tools.
- Analyze suspicious emails, links, and files in sandbox environments to detect malware—just like a digital crime lab.

UNIT 08: Geo-Tracking Intelligence - IP Address Tracing Techniques

- Use open-source tools to trace mobile IP addresses like a cybercrime cell.
- Set up cyber traps with fake apps/web interfaces to capture criminal digital footprints.
- Extract GPS coordinates and map suspect movements for forensic tracking.
- Apply social engineering techniques to pinpoint criminal locations.
- Retrieve IMEI numbers for tracking stolen or suspect mobile devices.
- Work with telecom data to trace phones across international networks.
- Track mobile devices even without GPS using Wi-Fi & network forensics.
- Conduct full forensic investigations on suspect mobile activity and communication.

UNIT 09: Web Browser Artefact Analysis & Cyber Forensic Recovery

- Recover stored usernames and passwords from browsers (Chrome, Firefox, Edge) using advanced forensic tools.
- Conduct browser history forensics to investigate online behavior and digital traces.
- Reconstruct last browsing sessions to identify open tabs, recent pages, and suspect activities before shutdown.
- Perform RAM (Volatile Memory) analysis to extract live evidence before it's lost.
- Use forensic browser analysis to uncover hidden online movements and potential criminal patterns.

UNIT 10: Malware Detection & System Log Forensic Analysis

- Examine Windows event logs for signs of unauthorized system access or malware behavior.
- Analyze network traffic using forensic-grade packet capture tools (PCAPs), flow records, and proxy logs to trace malicious communication paths.
- Identify malware signatures and behavioral indicators like a digital forensic analyst.
- Monitor suspicious background processes used in cyber attacks.
- Detect and trace ransomware infections using threat intelligence techniques.

UNIT 11: Windows System Breach & Hacker Investigation

- Deploy forensic procedures to extract credentials from USB drives and other storage devices.
- Evaluate password strength and scan systems for brute-force or credential stuffing attempts.
- Monitor Wi-Fi networks, access points, and traffic for vulnerabilities during security audits.
- Capture and analyze system memory to uncover encryption keys, hacker tools, and hidden sessions.
- Use police-approved forensic tools to recover deleted or wiped data from systems—just like in real digital crime scenes.

UNIT 12: Joint Cybercrime Investigations with Cyber Cell

- Follow official protocols for collecting digital evidence and identifying suspects with forensic accuracy.
- Work in coordination with cyber crime police units for suspect tracking and legal prosecution.
- Combine intelligence from both cyber cells and law enforcement departments to crack complex cases.
- Support legal teams with proper chain-of-custody documentation and verified digital proof.
- Investigate with national and international cyber units for organized crime or cross-border attacks.

Ultimate Digital Resources for Cyber Crime Investigation

- Access over 80+ crore verified digital records (Phone Numbers, E-mails, Addresses)
- Explore 50+ real-world cybercrime casebooks, tools, and forensic e-guides.

ALL DATABASES AND TOOLS ARE FOR EDUCATIONAL TRAINING AND LAWFUL INVESTIGATION PURPOSES ONLY. FOR USE BY AUTHORIZED CYBERCRIME PROFESSIONALS AND TRAINEES.



agent.spyriot@gmail.com



www.spyriotsecurity.in



+91 6370634758

CERTIFICATIONS

Cyber Detective Certification + Certified Cyber Crime Investigator Officer I'd Card

