SPYRIOT CYBER OPS

CYBER CRIME INVESTIGATION MASTERY

⚠ DISCLAIMER ⚠

"This program is conducted strictly for educational, research, and professional skill development purposes in accordance with applicable laws and ethical standards. It does not grant any government-recognized detective license, law-enforcement authority, police powers, or legal investigative jurisdiction. Any illegal, unauthorized, unethical, or malicious use of the knowledge, tools, techniques, or skills provided during the training shall be the sole responsibility of the participant, and the training provider shall not be held liable for any misuse, legal violations, damages, or consequences arising therefrom."

A Highly Impactful Industry-Level Professional Training Program Specially Designed By Combining:

Red Hat & Kali Linux + Ethical Hacking + Cyber Security + SOC + Cyber Crime Investigation

PROGRAM INTRODUCTION:

Spyriot Cyber OPS is an advanced practical-oriented cyber security master program designed to build industry-ready professionals with hands-on experience in offensive security, defensive security, digital forensics, Linux administration, cybercrime investigation, and enterprise security operations.

The course focuses on real-world attack simulation, threat analysis, forensic investigation, incident response, security monitoring, and practical cyber defence techniques used in modern organizations and cyber investigation environments.

STUDENTS CAN PREPARE FOR ROLES SUCH AS: Ethical Hacker, Cyber Security Analyst, Linux System Administrator, Digital Forensic Investigator, Threat Intelligence Analyst, Incident Response Analyst, Vulnerability Assessment Analyst, Security Consultant, Red Team Operator & Blue Team Analyst.

COURSE STRUCTURE:

Fee: ₹24,999 | Duration: 3 Months (Training + Internship) | Timing: 07 PM (Mon-Fri)

After Spyriot Cyber OPS Training, Students Will Be Able To Do:

- Investigate fake loan app blackmailing cases.
- Trace criminals involved in online harassment cases.
- Investigate investment and online money fraud scams.
- Identify fake social media profiles and impersonation.
- Track real IP addresses of cyber criminals.
- Perform GPS and digital location tracking.
- Investigate OTP, banking, and payment frauds.
- Analyse phishing attacks and credential theft.
- Investigate sextortion and video call scams.
- Detect malware, spyware, and RAT attacks.
- Investigate remote access and device hacking cases.
- Handle fake job and recruitment scam investigations.
- Investigate hacked email and social media accounts.
- Collect and analyse digital forensic evidence.
- Investigate cyber stalking and online threats.
- Analyse suspicious websites, links, and scam activities.
- Perform Android mobile forensic investigations
- Perform network traffic and packet analysis.
- Trace digital footprints and online activities.
- Recover deleted files and digital evidence.

- Analyse suspicious logs and security incidents.
- Investigate cyberattacks on companies and organizations.
- Perform incident response and attack handling.
- Detect data breaches and information leaks.
- Investigate identity theft and fake document frauds.
- Secure websites against common cyberattacks.
- Perform Wi-Fi security testing and investigations.
- Investigate malicious APKs and mobile applications.
- Analyse server attacks and unauthorized access.
- Perform cyber threat intelligence and OSINT investigations.
- Create professional VAPT and investigation reports.
- Work with law enforcement in cyber investigations.
- Provide cyber security consulting to organizations.
- Handle corporate cyber security audits.
- Perform cloud and server security assessments.
- Identify social engineering and manipulation attacks.
- Work as an Ethical Hacker or Cyber Crime Investigator.
- Build industry-level cyber security investigation skills.

(Contents)

Specialized Cyber Crime Investigation Techniques Included For Online Blackmailing or Harassment, IP/GPS Tracking, Fake Social Media Profile, Online Loan/Job & Investment Fraud Detection & Hacked Device Recovery

- Network Scanning, Service Enumeration & Digital Asset Discovery Investigation Techniques

UNIT 04: Ethical Hacking & Cyber Attack Investigation Techniques

- Vulnerability Assessment, Security Weakness Investigation & Cyber Risk Analysis
- Attack Simulation, Exploitation Techniques & Controlled Penetration Investigation
- Android And System Hacking Techniques And Investigation.
- Privilege Escalation Investigation & Administrative Access Control Analysis
- Post-Exploitation Operations, Persistence Tracking & System Enumeration Investigation
- Pivoting, Lateral Movement & Internal Network Intrusion Investigation Techniques

UNIT 05: Web Application Exploitation & Website Crime Investigation

- SQL Injection Investigation, Database Exploitation & Web Application Security Assessment
- Cross-Site Scripting (XSS) Attack Investigation & Client-Side Payload Analysis
- Authentication Bypass Investigation & Login Security Vulnerability Analysis
- Malicious File Upload Investigation & Server Security Validation Techniques
- API Security Investigation, Endpoint Traffic Analysis & Web Service Vulnerability Assessment
- Session Hijacking Investigation, Cookie Forensics & User Session Security Analysis

UNIT 06: Wireless Network Investigation & Wi-Fi Attack Analysis

- Wireless Packet Analysis, Wi-Fi Traffic Capturing & Communication Investigation Operations
- WPA/WPA2 Security Investigation, Wireless Password Auditing & Access Validation
- Rogue Access Point Detection, Unauthorized Device Tracing & Wireless Threat Monitoring
- Evil Twin Attack Investigation, Fake Wi-Fi Simulation & Social Engineering Scenario Analysis
- Wireless Traffic Monitoring, Suspicious Activity Investigation & Wireless Security Assessment

UNIT 07: Malware Investigation & Reverse Engineering Operations

- Static Malware Investigation, Suspicious File Examination & Malware Signature Analysis
- Dynamic Malware Investigation, Live Execution Monitoring & Threat Behaviour Analysis
- Malware Behaviour Monitoring, Process Investigation & Malicious Activity Detection
- Reverse Engineering Fundamentals, Binary Investigation & Malware Code Analysis
- Ransomware Investigation, Encryption Behaviour Analysis & Incident Response Operations

UNIT 08: Social Engineering Attack Investigation & Phishing Operations

- Phishing Campaign Investigation, Email Attack Simulation & Credential Theft Awareness
- Fake Login Page Investigation, Credential Harvesting Detection & Web Impersonation Analysis
- Social Engineering Attack Investigation, Psychological Manipulation & Human Exploitation Techniques
- Human Intelligence Gathering, Information Extraction & Real-World Social Engineering Operations
- Security Awareness Simulation, Employee Attack Readiness Testing & Cyber Crime Prevention Training

UNIT 09: Digital Forensics & Cyber Evidence Acquisition

- Forensic Disk Imaging, Digital Evidence Acquisition & Secure Evidence Cloning Techniques
- Timeline Investigation, System Activity Tracking & Digital Event Reconstruction Analysis
- Memory Forensics, RAM Investigation & Live Threat Analysis Techniques
- Digital Evidence Preservation, Chain of Custody Management & Forensic Evidence Handling Procedures

UNIT 10: Mobile Forensics, Tracking & OSINT Intelligence Investigation

- Android Data Extraction, Mobile Device Acquisition & Smartphone Crime Investigation Techniques

- Call Log & Chat Recovery, Deleted Communication Investigation & Evidence Retrieval
- Metadata Investigation, EXIF Data Analysis & Digital File Tracking Operations
- Social Media Investigation, Online Activity Monitoring & Digital Evidence Collection
- OSINT Profiling, Open-Source Intelligence Gathering & Target Information Investigation Techniques

UNIT 11: Advanced Cyber Crime Investigation & Criminal Tracing Techniques

- Email Header Investigation, Sender Trace Analysis & Phishing Email Verification
- Scam Website Investigation, Fake Domain Analysis & Fraudulent Website Detection
- IP Tracking & Geolocation Investigation for Cyber Threat Source Identification
- Cyber Fraud Investigation, Online Scam Analysis & Digital Financial Crime Investigation
- Digital Evidence Documentation, Case Reporting & Cyber Investigation Evidence Management

UNIT 12: Cyber Threat Intelligence & Incident Investigation Response

- IOC Analysis, Threat Indicator Investigation & Malicious Activity Detection Techniques
- Threat Hunting, Suspicious Behaviour Investigation & Advanced Threat Discovery Operations
- Incident Response Workflow, Security Breach Investigation & Cyber Attack Containment Procedures
- MITRE ATT&CK Mapping, Adversary Tactics Investigation & Threat Behaviour Classification
- Security Event Investigation, Log Correlation & Enterprise Security Incident Analysis

UNIT 13: SIEM Monitoring, SOC Analysis & Log Investigation

- SIEM Dashboard Monitoring, Real-Time Security Visibility & Enterprise Threat Investigation Operations
- Log Correlation, Security Event Investigation & Multi-Source Threat Detection Techniques
- Alert Rule Creation, Automated Threat Detection & Security Notification Investigation Workflow

- Security Event Investigation, Incident Analysis & Suspicious Activity Monitoring Procedures
- Brute Force Attack Detection, Unauthorized Access Investigation & Attack Pattern Analysis Techniques

UNIT 14: Active Directory Security & Windows Crime Investigation

- Active Directory Deployment, Domain Configuration & Enterprise User Investigation Management
- Group Policy Administration, System Access Control & Windows Security Policy Enforcement
- Windows Event Log Investigation, Security Event Monitoring & Suspicious Activity Analysis
- Kerberos Attack Investigation, Authentication Security Testing & Credential Threat Analysis
- Windows Security Hardening, Endpoint Protection & Enterprise System Defence Configuration

UNIT 15: Live Cyber Crime Case Investigation & Real-World Operations

- Phishing Case Investigation, Email Scam Analysis & Credential Theft Incident Examination
- Social Media Scam Investigation, Fake Profile Tracking & Online Fraud Detection Techniques
- Insider Threat Investigation, Unauthorized Access Analysis & Internal Security Breach Examination
- Digital Fraud Investigation, Cyber Financial Crime Analysis & Online Scam Investigation Procedures

UNIT 16: Professional VAPT Auditing & Digital Investigation Reporting

- Professional VAPT Investigation Reporting, Vulnerability Documentation & Security Assessment Preparation
- Digital Evidence Reporting, Forensic Documentation & Cyber Crime Evidence Presentation
- Executive Security Briefing, Client Investigation Reporting & Professional Cyber Security Communication
- Incident Documentation, Security Breach Investigation Reporting & Case Workflow Documentation Procedures


SPYRIOT
SECURITY
INCORPORATED UNDER MCA,
GOVERNMENT OF INDIA
LIVE ONLINE TRAINING
CYBER DETECTIVE &
CRIME INVESTIGATION MASTERY
SPYRIOT
CYBEROPS
DURATION: 2 MONTHS
REAL WORLD
CASE STUDIES
PRACTICAL
HANDS-ON LABS
EXPERT
LIVE SESSIONS
NATION FIRST
JAI HIND
SECURING INDIA'S DIGITAL FUTURE
CONFIDENTIAL
TOP SECRET
CYBER DIVISION
CYBER DETECTIVE &
CRIME INVESTIGATION MASTERY
SPYRIOT
CYBEROPS
DURATION:
2 MONTHS
AUTHORIZED PERSONNEL ONLY