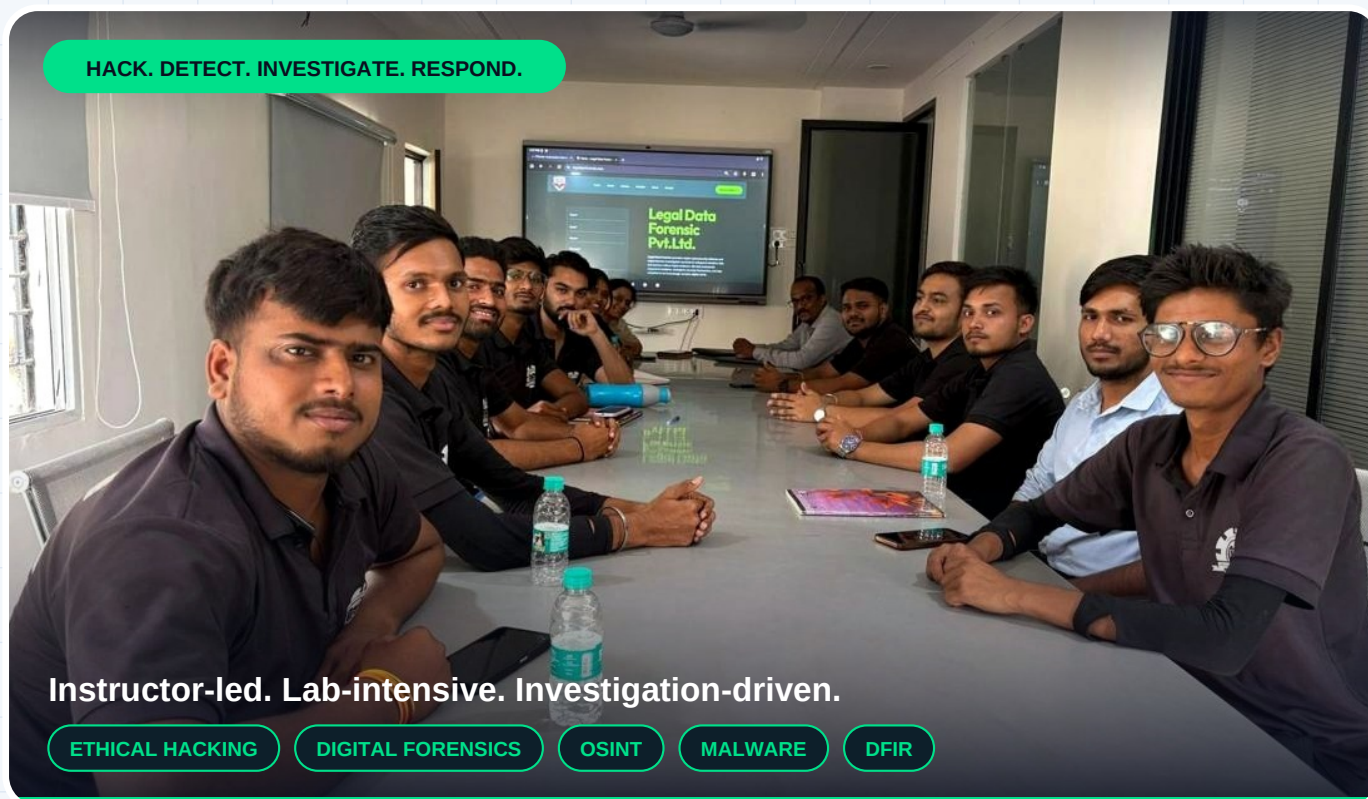




DFIROPS

Digital Forensics, Hacking and Incident Response Operations Professional Program

Think Like an Attacker. Investigate Like an Expert. Respond Like a Professional.

Hack. Detect. Investigate. Respond.

3

MONTHS

180

TRAINING HOURS

50%

PRACTICAL LABS

5

CAPSTONE SCENARIOS

Ethical Hacking | Digital Forensics | OSINT | Mobile Forensics | Malware Analysis | DFIR

upskill.pw

Presented by Crypto Forensic Technology

Proposed course syllabus. Schedule, tools and certification rules are subject to final confirmation by Upskill.

CONTACT US

Phone: 7773900082

Email: shrikant@cryptoforensic.in

Web: www.cryptoforensic.in

Program Overview

Hacking and forensics taught as one connected investigation pathway.

The DFIOPS program combines ethical hacking, penetration testing, digital forensics, cybercrime investigation, malware analysis and incident response into one integrated learning pathway. Instead of teaching hacking and forensics as separate subjects, participants learn how an attack is conducted in an authorised lab, how it generates digital traces, how investigators collect and analyse those traces, and how incident responders detect, contain and document the activity.

Our signature approach: every major hacking module has a corresponding forensic examination module, so you understand both how an attack works and how to investigate its digital traces.

From attack to evidence to response

1 ATTACK	2 TRACES	3 ACQUIRE	4 ANALYSE	5 RESPOND
Authorised attack in an isolated lab	Logs, artefacts and traffic are generated	Forensic imaging, hashing, chain of custody	Reconstruct the timeline from evidence	Detect, contain, document and report

Program at a glance

Particulars	Details
Duration	3 months / 12 weeks
Total hours	180 hours
Training approach	30% theory, 50% practical labs, 20% integrated casework and assessment
Level	Foundation to intermediate, with advanced exposure
Core domains	Ethical hacking, VAPT, digital forensics, OSINT, malware analysis, DFIR
Lab environment	Isolated cyber range and forensic investigation laboratory
Final project	Integrated cyberattack simulation, forensic investigation and incident-response report

What you will learn

Ethical Hacking and VAPT Recon, scanning, network, web and API testing	Digital Forensics Imaging, Windows and Linux artefacts, file systems
OSINT and Cybercrime Source validation, digital identity investigations	Mobile Forensics Android and iOS acquisition and app artefacts
Malware Analysis Static, dynamic and memory-based analysis, YARA	DFIR, SOC and Threat Hunting SIEM, live response, MITRE ATT&CK mapping
Active Directory Security Attack paths, lateral movement, logon analysis	Integrated Capstone Attack simulation, investigation and expert report

Integrated 12-Week Syllabus

MONTH 1

Weeks 1-4 | 60 hours

Ethical hacking, attack techniques and forensic evidence acquisition

MODULE 1 Cybersecurity, ethical hacking and cybercrime investigation

- Cybersecurity fundamentals, attack surfaces, threat actors and attack vectors
- Ethical hacking lifecycle and penetration-testing methodologies
- Cybercrime investigation lifecycle and digital forensic principles
- Legal authorisation, scope, rules of engagement, responsible disclosure
- PTES, NIST security testing guidance, ISO/IEC 27037 and MITRE ATT&CK overview
- Cybercrime scenarios: financial fraud, phishing, account compromise, ransomware, insider threats
- Evidence integrity, chain of custody and investigative documentation

MODULE 2 Networking, Linux, Windows and hacking fundamentals

- TCP/IP, OSI, subnetting, DNS, DHCP, routing, ports and protocols
- Linux command line, Bash, permissions, processes and services
- Windows architecture, PowerShell, event logs and security configuration
- Network traffic analysis using Wireshark
- Basic scripting with Python and Bash for security tasks
- Authentication, authorisation, password security, common misconfigurations
- Security controls, firewalls, endpoint protection, network segmentation

MODULE 3 Reconnaissance, OSINT, scanning and enumeration

- Passive and active reconnaissance
- OSINT research and digital footprint analysis
- Domain, DNS, IP, subdomain and technology enumeration
- Network discovery and port scanning using Nmap
- Vulnerability scanning and asset identification
- Service enumeration and exposure analysis
- Attack-surface mapping and threat modeling
- Linking reconnaissance observations to potential investigative evidence

MODULE 4 Forensic acquisition, crime-scene response and evidence preservation

- Digital crime-scene management and first-response procedures
- Identification and documentation of electronic evidence
- Seizure planning and evidence-handling precautions
- Volatile and non-volatile evidence
- Forensic imaging and acquisition using FTK Imager, Guymager and compatible tools
- Write blockers, hash verification, image formats and acquisition logs
- Chain of custody, evidence labeling and forensic working copies
- Capturing baseline system state and logs before and after simulated attacks

MONTH 1 INTEGRATED PRACTICAL

- ✓ Conduct an authorised reconnaissance and network discovery exercise
- ✓ Simulate selected security weaknesses on a controlled lab network
- ✓ Collect system logs and traffic generated during the exercise
- ✓ Acquire and verify forensic images of designated lab devices
- ✓ Prepare an initial attack-surface and evidence-preservation report

Integrated 12-Week Syllabus

MONTH 2

Weeks 5-8 | 60 hours

Penetration testing, computer and mobile forensics, and attack reconstruction

MODULE 5 Network penetration testing and vulnerability exploitation

- VAPT methodology and engagement planning
- Network and infrastructure vulnerability assessment
- Controlled exploitation of intentionally vulnerable services
- Authentication and access-control weaknesses
- Linux and Windows privilege-escalation concepts in isolated labs
- Metasploit fundamentals and controlled proof-of-concept validation
- Network segmentation and security-control testing
- Post-exploitation artifact awareness and forensic trace generation
- Remediation, retesting and technical reporting

MODULE 6 Web application and API hacking with forensic analysis

- Web architecture, HTTP/S, cookies, sessions and authentication
- OWASP Top 10 and web application security testing
- Burp Suite and OWASP ZAP workflows
- SQL injection, XSS, access-control flaws, CSRF, file upload weaknesses, SSRF
- Authentication and session management testing
- REST API security, token handling and authorisation weaknesses
- Web server logs, database logs and application-level evidence
- Investigating web attacks via server logs, browser artifacts and network traffic
- Correlating application vulnerabilities with incident evidence

MODULE 7 Computer, memory and network forensics

- Windows artifacts: Registry, Event Logs, Prefetch, Amcache, LNK files, Jump Lists
- Linux artifacts: authentication logs, shell history, system logs, persistence traces
- File-system analysis, deleted-file recovery and file carving
- Browser artifacts, downloads and user activity reconstruction
- Memory acquisition and analysis using Volatility
- Processes, network connections, injected-code indicators, suspicious activity
- Network forensics with Wireshark, Zeek and NetworkMiner
- Timeline reconstruction and correlation of attack events
- Forensic analysis of traces left by simulated network and web attacks

MODULE 8 Mobile forensics, OSINT and cybercrime investigation

- Android and iOS architecture and forensic evidence sources
- Logical, file-system and physical acquisition concepts
- Mobile app data, SQLite databases, messages, calls and media
- WhatsApp and other messaging application artifact analysis
- Mobile device security, authentication, encryption, extraction limitations
- OSINT investigation workflows and public-source verification
- Email, domain, IP, social-media and digital-identity investigations
- Image metadata, geolocation and timeline correlation
- Linking mobile evidence, online activity and computer artifacts in a simulated cybercrime case

MONTH 2 INTEGRATED PRACTICAL

- ✓ Perform network and web application testing in a controlled environment
- ✓ Analyse logs and forensic artifacts produced by the simulated attacks
- ✓ Reconstruct a selected attack timeline using computer and network evidence
- ✓ Examine a simulated mobile-device evidence set
- ✓ Prepare a combined penetration-testing and forensic investigation report

Integrated 12-Week Syllabus

MONTH 3

Weeks 9-12 | 60 hours

Advanced hacking scenarios, malware analysis, DFIR and integrated investigation

MODULE 9 Active Directory security, lateral movement and enterprise attack investigation

- Active Directory architecture, authentication and access control
- Domain enumeration and common configuration weaknesses
- Kerberos and NTLM security concepts
- Enterprise identity security and privilege relationships
- Controlled attack-path simulation in a dedicated lab
- Lateral movement and persistence concepts
- Windows security logs and authentication event analysis
- Investigating suspicious logons, remote execution and account misuse
- Correlating endpoint and domain-controller evidence
- Mapping simulated adversary behaviours to MITRE ATT&CK

MODULE 10 Malware analysis, threat hunting and detection engineering

- Malware types, delivery mechanisms and infection chains
- Safe malware-analysis lab setup and isolation
- Static analysis: hashes, strings, PE structure and imports
- Dynamic analysis: process, file, registry and network behaviour
- Introduction to Ghidra and reverse-engineering fundamentals
- Memory-based malware investigation
- YARA rules and indicators of compromise
- Ransomware behaviour and investigation fundamentals
- Threat intelligence and threat hunting
- Detection rules, alert triage and security monitoring
- Connecting malware behaviour with forensic artifacts and response actions

MODULE 11 SOC operations, incident response and enterprise DFIR

- SOC workflows, alert triage and escalation
- SIEM architecture and security event correlation
- Introduction to Splunk, Wazuh or an equivalent SIEM
- Incident response lifecycle and operational procedures
- Phishing, ransomware, data theft and insider-threat investigations
- Endpoint detection and response concepts
- Live response, evidence preservation and forensic triage
- Containment, eradication, recovery and lessons learned
- Cloud and SaaS incident investigation fundamentals
- Incident timelines, case notes and executive reporting

MODULE 12 Integrated red-team, blue-team and forensic capstone

- Authorised attack simulation against a prepared enterprise lab
- Red-team activity and blue-team monitoring
- Collection and preservation of evidence generated during the exercise
- SOC detection, triage and incident escalation
- Computer, network, memory and application artifact analysis
- OSINT correlation where relevant to the scenario
- Investigation hypotheses, evidence correlation, timeline reconstruction
- Forensic report preparation and technical peer review
- Mock expert presentation and technical defense of findings
- Final assessment and professional portfolio review

MONTH 3 INTEGRATED PRACTICAL

- ✓ Investigate a simulated enterprise compromise
- ✓ Identify attack activity through logs and forensic artifacts
- ✓ Conduct malware triage and threat detection
- ✓ Execute incident-response procedures
- ✓ Present a defensible forensic report and a remediation plan

Hacking Paired with Forensics: Week by Week

Each offensive topic is matched with the forensic work that investigates it.

Wk	Hacking and offensive security	Forensic and investigative module	Practical exercise
1	Ethical hacking, attack lifecycle, networking, Linux and Windows security	Digital forensic fundamentals, cybercrime investigation, evidence principles	Establish a lab and document baseline evidence
2	OSINT, reconnaissance, footprinting, DNS and network enumeration	OSINT investigation, source validation, digital footprint analysis	Investigate a simulated online fraud case
3	Network scanning, service enumeration, vulnerability assessment	Forensic imaging, evidence acquisition, hashing and chain of custody	Scan a lab network, then acquire and examine selected system evidence
4	Network penetration testing, controlled exploitation, authentication weaknesses	Windows and Linux forensic artifacts, event logs, activity reconstruction	Investigate system traces produced during an authorised attack simulation
5	Web application hacking, OWASP Top 10, Burp Suite and security testing	Web server, browser, application and database forensics	Simulate a web application attack and reconstruct its activity from logs
6	API security, session management, access-control weaknesses	Network forensics, packet analysis, log correlation and timeline reconstruction	Investigate suspicious API requests using network and application evidence
7	Active Directory security, identity weaknesses, privilege escalation concepts	Windows enterprise forensics, authentication events, lateral-movement investigation	Investigate simulated suspicious domain activity
8	Mobile application security, mobile attack surfaces, wireless security fundamentals	Android and iOS forensics, mobile application artifacts, location and communication evidence	Examine a simulated mobile security incident
9	Malware delivery, persistence concepts, controlled payload behaviour	Memory forensics, malware triage, static and dynamic analysis	Analyse a benign or safely contained malware-analysis exercise
10	Enterprise attack paths, simulated adversary behaviour, threat-informed testing	DFIR, threat hunting, MITRE ATT&CK mapping and endpoint investigation	Reconstruct an enterprise intrusion from endpoint and network evidence
11	Red-team and blue-team exercises, detection evasion concepts, security-control validation	SOC operations, SIEM investigation, incident response and evidence preservation	Conduct a coordinated attack-detection-response simulation
12	Integrated authorised penetration-testing scenario	Full forensic examination, incident reconstruction, expert reporting and presentation	Complete an end-to-end cyber investigation capstone

Core Modules and Their Practical Integration

Network hacking and network forensics

- Nmap, vulnerability scanning, service enumeration and controlled exploitation
- Wireshark, Zeek, packet analysis, connection records and traffic reconstruction
- Investigate suspicious connections, scanning activity and exploitation indicators

Active Directory security and enterprise forensics

- Domain architecture, authentication, misconfigurations, controlled attack-path exercises
- Windows event logs, Registry, authentication traces and endpoint artifacts
- Investigate suspicious logins, privilege changes and lateral movement

Malware analysis and incident investigation

- Malware behaviour, persistence, static and dynamic analysis, reverse-engineering basics
- Memory analysis, YARA, process activity, file-system changes, network indicators
- Trace malicious behaviour and create evidence-supported incident timelines

Web application hacking and web forensics

- OWASP testing, Burp Suite, authentication testing, SQL injection, access-control testing
- Web server logs, browser artifacts, application logs and database records
- Reconstruct requests, identify suspicious activity, document technical evidence

Mobile security and mobile forensics

- Mobile OS security, application vulnerabilities and mobile attack surfaces
- Android and iOS acquisition concepts, app databases, messaging and location artifacts
- Correlate mobile activity with online accounts and computer evidence

SOC, threat hunting and DFIR

- SIEM, alert triage, detection engineering and MITRE ATT&CK
- Evidence preservation, live response, forensic triage and incident handling
- Validate detections using controlled attack scenarios and investigate resulting alerts

Suggested Distribution of 180 Training Hours

Ethical hacking and penetration testing		45 hrs
Digital forensics and evidence acquisition		45 hrs
DFIR, SOC and threat hunting		30 hrs
Mobile forensics, OSINT and malware analysis		30 hrs
Integrated case studies and capstone		30 hrs

Proposed allocation; practical labs are integrated throughout the modules.

Major Capstone Scenarios

Five end-to-end cases that pair an attack with its investigation.

Capstone	Attack scenario	Forensic investigation
Corporate network compromise	Simulated unauthorised access and privilege misuse	Windows event analysis, network logs, timeline and attack-path reconstruction
Web application breach	Controlled exploitation of a vulnerable application	Server logs, database activity, browser evidence and incident report
Digital financial fraud	Simulated account compromise and suspicious online activity	OSINT, email, mobile, browser and transaction-related evidence correlation
Ransomware incident	Safe ransomware behaviour simulation in an isolated environment	Malware triage, memory and file-system analysis, containment and incident response
Integrated enterprise intrusion	Coordinated red-team and blue-team exercise	SIEM investigation, forensic imaging, evidence correlation, final expert-style report

Recommended Tools

Domain	Tools
Ethical hacking	Kali Linux, Nmap, Metasploit, Burp Suite, OWASP ZAP
Vulnerability assessment	Nessus, Greenbone/OpenVAS
Computer forensics	FTK Imager, Autopsy, Magnet AXIOM or equivalent licensed platforms
Forensic acquisition	Guymager, FTK Imager, write blockers, hashing utilities
Mobile forensics	Oxygen Forensics, MOBILedit, ALEAPP, iLEAPP
Memory forensics	Volatility 3, MemProcFS
Network forensics	Wireshark, Zeek, NetworkMiner
OSINT	Maltego, SpiderFoot, ExifTool, WHOIS and DNS utilities
Malware analysis	Ghidra, REMnux, FLARE-VM, YARA
SOC and DFIR	Wazuh, Splunk, Velociraptor, Sysmon, MITRE ATT&CK

Tools are indicative. Final selection depends on lab licensing, system requirements and instructor expertise.

Assessment and Certification Structure

Weighted across hacking, forensic, investigation and capstone work.

Ethical hacking and VAPT practicals		20%
Forensic acquisition and examination labs		25%
OSINT, mobile and malware investigation assignments		15%
SOC and incident-response simulation		15%
Integrated capstone investigation		25%
		Total: 100%

SUGGESTED CERTIFICATION TITLE

DFIOPS Certified Professional: Digital Forensics, Ethical Hacking and Incident Response

Awarded as an Upskill course-completion credential, subject to clearly defined certification criteria and assessment requirements.

Who Is DFIOPS For?

Built for learners who want to understand both sides of a cyber incident.

- ✓ Aspiring ethical hackers who want to understand the digital traces their techniques leave behind
- ✓ Aspiring forensic examiners and cybercrime investigators who want hands-on attack knowledge
- ✓ SOC and incident-response trainees preparing to detect, contain and document real incidents

Ready to go beyond the theory?

Build practical hacking and forensic skills.
Develop your technical portfolio.
Prepare for your next step in cybersecurity.

Enrol at upskill.pw

Explore the full program, batches and fees at <https://upskill.pw/>

CONTACT US

PHONE **7773900082**
EMAIL **shrikant@cryptoforensic.in**
WEB **www.cryptoforensic.in**



Crypto Forensic Technology

DFIOPS is a lab-based training program. It does not guarantee employment, accreditation, or exam coverage of any third-party certification.
All offensive techniques are practised only in isolated, authorised lab environments.