SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

DIGITAL FORENSICS

QUISITION . CHAIN OF CUSTO
DISK . MEMORY . NETWORK
ELINE ANALYSIS . REPORTIN

DURATION	LEVEL	MODULES	MODE
50 Hours	**Intermediate to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A digital forensics course covering evidence acquisition, artefact analysis and reporting fit for review. The course follows evidence from seizure to court-ready report: imaging, hashing, chain of custody, file system and registry analysis, memory forensics, browser and email artefacts, and timeline reconstruction.

All exercises use open-source tooling on prepared disk and memory images.

WHO IT IS FOR

- Security analysts and incident responders
- Law enforcement and legal support staff
- IT administrators handling investigations
- Audit and compliance teams

PREREQUISITES

Operating system fundamentals and basic command line.

02 LEARNING OUTCOMES

01 Acquire disk and memory images without altering evidence.

02 Maintain hashing and chain-of-custody records.

03 Analyse NTFS, FAT and ext file system artefacts.

04 Recover deleted and hidden data.

05 Extract registry, browser and email artefacts.

06 Reconstruct a timeline of user and system activity.

07 Write a factual report suitable for review.

03 MODULE STRUCTURE

8 MODULES

01 FORENSIC PRINCIPLES

- Evidence types
- Chain of custody
- Documentation
- Order of volatility
- Legal admissibility
- Anti-forensics awareness

02 ACQUISITION

- Write blockers
- Memory capture
- Hash verification
- Disk imaging
- Live vs dead acquisition

TOOLS

FTK IMAGER | DD | DUMPIT

03 FILE SYSTEM ANALYSIS

- NTFS and MFT
- ext4
- Slack space
- FAT
- Metadata
- Deleted file recovery

TOOLS

AUTOPSY | SLEUTH KIT

04 WINDOWS ARTEFACTS

- Registry hives
- Shellbags
- USB history
- Prefetch
- Event logs
- LNK files

LAB

USER ACTIVITY RECONSTRUCTION

05 MEMORY FORENSICS

- Process lists
- Injected code
- Malware indicators
- Network connections
- Credential artefacts

TOOLS

VOLATILITY

06 BROWSER, EMAIL AND MOBILE

- Browser history and cache
- PST and MBOX
- Cloud sync artefacts
- Email headers
- Mobile extraction overview

07 NETWORK AND LOG FORENSICS

- PCAP analysis
- Log correlation
- Session reconstruction
- Time zone handling

TOOLS

WIRESHARK | NETWORKMINER

08 TIMELINE AND REPORTING

- Super timelines
- Findings vs interpretation
- Expert conduct
- Correlating artefacts
- Report structure

PROJECT

FULL CASE ANALYSIS AND FORENSIC REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

DIGITAL FORENSICS ANALYST | INCIDENT RESPONSE SPECIALIST | CYBER CRIME INVESTIGATOR | EDISCOVERY ANALYST | SECURITY CONSULTANT

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com