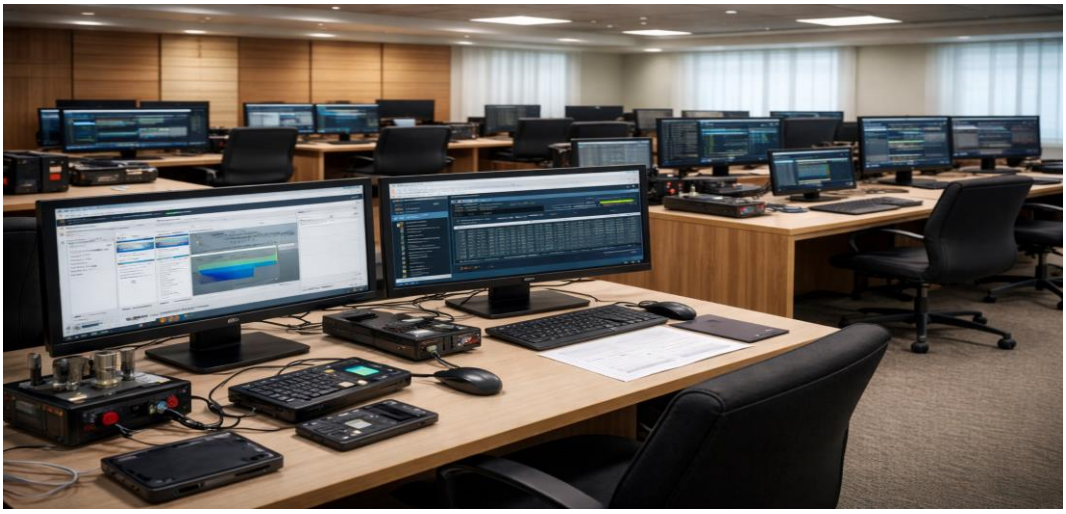
Akademika Lab Solution
Unit 128/129,Hema Industrial Estate,
Sarvodaya Nagar, Jogeshwari(E),
Mumbai - 400060, India.
Tele +91 7447438443
info@akademika.in | www.akademika.in

DIGITAL FORENSICS LABORATORY

Academic | Training | Research | Cybercrime Investigation



Overview

The Digital Forensics Laboratory (DFL) is a comprehensive, industry-aligned facility designed for academic teaching, hands-on training, research, and simulated cybercrime investigations. The laboratory equips students with practical expertise in digital evidence acquisition, analysis, preservation, and forensic reporting in alignment with Indian cyber laws and global best practices.

Objectives

- Hands-on exposure to digital forensic investigations
- Training on industry-standard forensic tools and methodologies
- Simulation of real-world cybercrime and incident response scenarios
- Ensuring forensic integrity and legal admissibility of evidence
- Alignment with Indian cyber laws and CERT-In guidelines

Laboratory Architecture

- Evidence Acquisition Zone
- Forensic Analysis Zone
- Malware and Memory Analysis Zone
- Mobile and Cloud Forensics Zone
- Reporting and Case Management Zone

Hardware Infrastructure

Forensic Workstations (10–15 systems recommended):
• Intel i7 / AMD Ryzen 7 or higher
• 32 GB RAM (64 GB recommended)

Akademika Lab Solution
Unit 128/129,Hema Industrial Estate,
Sarvodaya Nagar, Jogeshwari(E),
Mumbai - 400060, India.
Tele +91 7447438443
info@akademika.in | www.akademika.in

• 1 TB NVMe SSD (OS) + 2–4 TB Evidence Storage
• Dedicated GPU (recommended)

Servers: Central Evidence Repository, Case Management Server, Backup Server

Accessories: Hardware write blockers, encrypted storage, external HDD/SSD

Software Environment

Operating Systems: Windows 11, Linux (Ubuntu/Kali), macOS (optional)

Forensic Tools:
• Disk Forensics: Autopsy, FTK Imager, X-Ways (optional)
• Memory Analysis: Volatility, Rekall
• Network Forensics: Wireshark, Zeek, NetworkMiner
• Malware Analysis: Ghidra, IDA Free, Cuckoo Sandbox
• Mobile & Cloud: ADB, Mobile forensic plugins, cloud log analysis

Virtualization & Sandbox

VMware / VirtualBox based virtual machines with isolated malware sandboxes and snapshot-based system restoration after each lab session.

Evidence Handling & Legal Compliance

Chain of custody documentation, cryptographic hashing (MD5, SHA-1, SHA-256), secure evidence storage, and compliance with IT Act 2000, Indian Evidence Act Section 65B, and CERT-In guidelines.

Laboratory Experiments

- Disk Imaging and Hash Verification
- Deleted File Recovery
- Windows Registry Analysis
- Timeline and Event Correlation
- Memory Dump Investigation
- Network Traffic Analysis
- Ransomware Investigation
- Mobile Device Data Extraction
- Email Header and Log Analysis
- Incident Response Report Writing

Learning Outcomes

- Forensically sound evidence acquisition
- Disk, memory, network, and mobile analysis
- Incident reconstruction using timelines
- Malware behavior identification
- Legally admissible forensic reporting

Laboratory Security

Role-based access control, system audit logs, USB monitoring, and CCTV surveillance (recommended).