



EDUBLENDS

Fuel Your Future.

Fuel your **Future**

Dive into Edublends Academy's world of opportunities with industry internships, specialized training, and globally recognized certifications



Track 3: Digital Forensics & Incident Response

Basic to Advanced · 270 Hours Total

At EduBlends, we don't just train—we create future industry leaders!

Program Summary

Investigate, analyse and respond — from evidence collection and log analysis to malware forensics and cloud incident response.



Program Duration

270 hours across 3 levels
(approx. 20 weeks)



Weekly effort

12-15 hours a week



Learning Mode: Online and Offline
Classes, including Pre-Recorded
Videos, Live Sessions, and Interactive
Q&A Sessions.



Cyber Range & Cloud Lab access
with isolated attack and defence
environments



**Industry-Sponsored Internship
Facilitation**



Certificate Upon successful
completion of each level, participants
will be awarded a verified digital
certificate by EduBlends and Industry

A Progressive Learning Pathway Aligned to Your Graduation

At EduBlends Academy, we provide a structured learning pathway that allows students to build cybersecurity expertise across their graduation journey, with each level mapped to a semester window and a defined exit role.

1. **Basic Level (Sem 3–4) — Digital Forensics Foundations:** Triage, log analysis and artefact collection. Exit role: SOC Trainee.
2. **Intermediate Level (Sem 5–6) — Network & Ethical Forensics:** Deep-dive artefact analysis, network forensics and threat hunting. Exit role: Network Forensic Analyst · Threat Hunter.
3. **Advanced Level (Sem 7) — Incident Response & Digital Forensics:** Malware analysis, cloud IR and breach simulation. Exit role: Digital Forensic Investigator · IR Analyst.

By following this structured pathway, students complete the full track within their graduation period, emerging as industry-ready professionals with a portfolio of evidenced, lab-based security work.

Track 3 – Digital Forensics & Incident Response

Basic → Advanced · 270 hours total · 30 practical lab sessions and a panel-assessed capstone

Program Levels

Level	Title	Semester	Hours	Focus
Basic	Digital Forensics Foundations	Sem 3–4	90 hrs	Triage, log analysis and artefact collection
Intermediate	Network & Ethical Forensics	Sem 5–6	90 hrs	Deep-dive artefact analysis, network forensics and threat hunting
Advanced	Incident Response & Digital Forensics	Sem 7	90 hrs	Malware analysis, cloud IR and breach simulation

Target Roles

Level	Semester	Role
Basic	Sem 3–4	SOC Trainee — supporting initial triage, log analysis, and artifact collection
Intermediate	Sem 5–6	Network Forensic Analyst · Threat Hunter
Advanced	Sem 7	Digital Forensic Investigator · IR Analyst

Certification Alignment

Level	Certifications
Basic — Digital Forensics Foundations	IBM Cybersecurity Analyst Professional · Microsoft SC-200 · Google Professional Cloud Security Engineer · AWS Certified Security – Specialty
Intermediate — Network & Ethical Forensics	Microsoft AZ-700 · Google Professional Cloud Security Engineer
Advanced — Incident Response & Digital Forensics	IBM Cybersecurity Analyst Professional · Microsoft SC-200 · Google Professional Cloud Security Engineer · AWS Certified Security – Specialty

Vendor certification examinations are sat separately and are not included in programme fees. Preparation coverage is indicative and does not guarantee an examination pass.

Top Recruiters

IBM · Microsoft Azure · Google · AWS · TCS · Wipro

Recruiter names indicate the employers and sectors our graduates target; they do not constitute a placement guarantee or a formal hiring partnership.

Entry Requirements

The Basic level is open entry; no prior programming or security experience is assumed. The Intermediate level requires completion of the Basic level or equivalent networking and Linux competence. The Advanced level requires completion of the Intermediate level or demonstrable hands-on security experience.

Program Frameworks – Basic Level: Digital Forensics Foundations

Sem 3–4 · 90 hours · Triage, log analysis and artefact collection · 10 practical lab sessions

M1 | Forensic Principles & Legal Framework 18 hrs

Module / Topic

- Chain of custody, admissibility, evidence integrity, investigator ethics, reporting obligations

Practical Lab Sessions

- Lab 1:** Complete a full chain-of-custody record for a simulated seizure.
Lab 2: Audit a flawed evidence log and document every integrity failure

M2 | Operating Systems & Filesystem Artefacts 20 hrs

Module / Topic

- Windows and Linux filesystem structures, registry and log locations, metadata, deleted file recovery

Practical Lab Sessions

- Lab 3:** Locate and interpret key artefacts across a Windows and a Linux image.
Lab 4: Recover deleted files and verify their integrity by hash

M3 | Disk Imaging with FTK Imager 18 hrs

Module / Topic

- Write blocking, acquisition formats, verification hashing, memory capture, documentation

Practical Lab Sessions

- Lab 5:** Acquire a forensically sound disk image with verification hashes.
Lab 6: Capture volatile memory and record the acquisition conditions

M4 | Network Evidence with Wireshark 20 hrs

Module / Topic

- Packet capture as evidence, session reconstruction, extracting transferred files, identifying exfiltration

Practical Lab Sessions

- Lab 7:** Reconstruct a file transfer from a packet capture and extract the payload.
Lab 8: Identify and evidence data exfiltration in a provided capture

M5 | Log Analysis & Initial Triage 14 hrs

Module / Topic

- Log sources and formats, timeline building, correlation across sources, triage decisions and escalation

Practical Lab Sessions

- Lab 9:** Build a cross-source incident timeline from raw logs.
Lab 10: Triage the incident and write a structured escalation summary

Program Frameworks – Intermediate Level: Network & Ethical Forensics

Sem 5–6 · 90 hours · Deep-dive artefact analysis, network forensics and threat hunting · 10 practical lab sessions

M1 | Deep Disk Forensics with Autopsy & Sleuth Kit 22 hrs

Module / Topic

- Filesystem carving, registry and browser artefacts, timeline analysis, keyword and hash sets, reporting

Practical Lab Sessions

Lab 1: Conduct a full disk examination in Autopsy and produce a findings report.

Lab 2: Use Sleuth Kit at the command line to carve and validate artefacts

M2 | Network Forensics with Tcpdump 18 hrs

Module / Topic

- Command-line capture, BPF filters, protocol reconstruction, long-running capture strategy, storage and rotation

Practical Lab Sessions

Lab 3: Capture and filter traffic with tcpdump under a defined evidence strategy.

Lab 4: Reconstruct an attacker session from the captured stream

M3 | SIEM-Based Investigation 18 hrs

Module / Topic

- Query construction, pivoting across data sources, entity timelines, enrichment, case management

Practical Lab Sessions

Lab 5: Investigate a multi-stage intrusion using SIEM queries and pivots.

Lab 6: Build an entity timeline and document the full attack path

M4 | Threat Hunting Methodology 18 hrs

Module / Topic

- Hypothesis development, MITRE ATT&CK mapping, behavioural indicators, hunt execution and documentation

Practical Lab Sessions

Lab 7: Run a structured hunt mapped to ATT&CK techniques across the estate.

Lab 8: Convert hunt findings into detection rules and document coverage gaps

M5 | Anti-Forensics & Evidence Validation 14 hrs

Module / Topic

- Timestamp manipulation, wiping and encryption, steganography, detecting anti-forensic activity, validation techniques

Practical Lab Sessions

Lab 9: Detect and evidence anti-forensic activity on a prepared image.

Lab 10: Validate a contested finding using two independent methods

Program Frameworks – Advanced Level: Incident Response & Digital Forensics

Sem 7 • 90 hours • Malware analysis, cloud IR and breach simulation • 10 practical lab sessions

M1 | Static Malware Analysis 20 hrs

Module / Topic

- File triage, strings and headers, packing and obfuscation, disassembly basics, IOC extraction

Practical Lab Sessions

Lab 1: Triage an unknown binary and extract static indicators safely.

Lab 2: Identify packing and document the sample's capabilities from static evidence

M2 | Dynamic Malware Analysis 20 hrs

Module / Topic

- Sandbox construction, behavioural monitoring, network callbacks, persistence mechanisms, report writing

Practical Lab Sessions

Lab 3: Detonate a sample in an isolated sandbox and record its full behaviour.

Lab 4: Produce a malware analysis report with indicators and detection guidance

M3 | Cloud Incident Response 18 hrs

Module / Topic

- Cloud logging and audit trails, evidence acquisition in AWS and Azure, containment of cloud workloads, shared responsibility

Practical Lab Sessions

Lab 5: Acquire evidence from a compromised cloud workload without destroying state.

Lab 6: Contain and remediate the incident, documenting each action taken

M4 | Cyber Range Breach Simulation 18 hrs

Module / Topic

- Full-scope simulated breach, team roles, containment under time pressure, communication and escalation

Practical Lab Sessions

Lab 7: Respond to a live simulated breach in the cyber range as part of an IR team.

Lab 8: Deliver an incident report and executive briefing on the response

M5 | Investigation Capstone 14 hrs

Module / Topic

- End-to-end investigation, evidence package assembly, expert reporting, panel defence

Capstone Lab

Lab 9: Complete a full investigation from acquisition to conclusion.

Lab 10: Present the evidence package and defend the findings to a panel

Track 3 Toolkit – Core Tools & Technologies

Every tool below is used in a defined lab session at the level shown.

Category	Tools / Platforms
Traffic Analysis	Wireshark — packet capture and analysis
Imaging	FTK Imager — disk imaging and evidence preservation
Practice	Virtual Labs — isolated hands-on environments
Disk Forensics	Autopsy · Sleuth Kit
Network Forensics	Tcpdump
Detection	SIEM platforms
Malware Analysis	Static and dynamic analysis tooling
Cloud IR	AWS and Azure incident platforms
Simulation	Cyber Range Labs

Tools by Level

Level	Toolset
Basic — Digital Forensics Foundations	Wireshark — packet capture and analysis · FTK Imager — disk imaging and evidence preservation · Virtual Labs — isolated hands-on environments
Intermediate — Network & Ethical Forensics	Autopsy · Sleuth Kit · Tcpdump · SIEM platforms
Advanced — Incident Response & Digital Forensics	Static and dynamic analysis tooling · AWS and Azure incident platforms · Cyber Range Labs

Lab Environments

All practical sessions run in EduBlends cyber range and cloud lab environments. Offensive exercises are delivered on isolated, purpose-built ranges under defined rules of engagement, and forensic work uses write-blocked images and verified acquisition procedures.

Program Experience



Traffic Analysis

Wireshark — packet capture and analysis



Imaging

FTK Imager — disk imaging and evidence preservation



Disk Forensics

Autopsy · Sleuth Kit



Network Forensics

Tcpdump



Malware Analysis

Static and dynamic analysis tooling



Cloud IR

AWS and Azure incident platforms

Job Assistant
Upskilling and the Re-skilling
Entrepreneurship transition

The Digital Forensics & Incident Response track spans three levels and 270 hours, delivered through 30 structured lab sessions and a panel-assessed capstone. Learners progress from triage, log analysis and artefact collection at the Basic level, through deep-dive artefact analysis, network forensics and threat hunting at Intermediate, to malware analysis, cloud ir and breach simulation at Advanced. Every topic is reinforced in isolated cyber range and cloud lab environments that mirror live industry workflows, so that graduates leave with evidenced, portfolio-grade security work.

Expected outcomes



Advanced Industrial Internship Certifications

Differentiate yourself from your peers by earning the industrially recognized Advanced industrial internship Certification



Students Blending Team

EduBlends blends the students for the industry-ready



For the Industrial, By the Industry

Learn and apply concepts on industry projects from industry, along with personalized industry mentorship



Industry Integration Layer

This program is designed with integrated industry collaboration, where enterprise partners contribute to curriculum alignment, real-world problem statements, and internship pathways.



Cyber Range & Cloud Lab Facilities

Isolated attack and defence ranges, forensic workstations and cloud sandboxes for real industrial problems



360 Degree Career Support — Entrepreneurial Program

Idea-to-Enterprise Catalyst by EduBlends Academy is a structured entrepreneurial program that guides innovators from ideation to execution, helping them build and scale tech-driven businesses such as security consultancies, managed services and SaaS solutions.



Personalized Mentorship

Get unparalleled personalized mentorship and doubt resolution from industrialists and academicians.

Sample Weekly Program Planner



4–5 hours

Live interaction with the programme learning facilitator



1–2 hours

Recorded video lecture with faculty



1 hour

Group discussion with industrial mentor and academic instructor



4–5 hours

Cyber range and cloud lab practice exercises



2 hours

Rigorous, graded assignments to apply and reinforce the material

12–15 hours

Total weekly effort

Who Is This Program For?

Career Launchers

The Basic level (Sem 3–4) is designed for students and early-career IT professionals with no prior security background who want a structured, hands-on entry into cybersecurity.

Career Builders

The Intermediate level (Sem 5–6) suits IT support staff, network engineers and system administrators who want to move into hands-on security engineering and analysis roles.

Career Switchers

The Intermediate level also serves mid-career professionals working outside security who want credible, evidenced capability before making a career change.

Specialists & Founders

The Advanced level (Sem 7) is for learners who have completed the earlier levels, or who bring equivalent experience, and want to move into specialist and consultant roles — or to launch a security venture through the entrepreneurial programme.

Progressive Learning Pathway: Our curriculum is structured to provide a seamless learning experience, from foundational security skills at the Basic level through to specialist practice at Advanced.

- **Basic — Digital Forensics Foundations (Sem 3–4)** for students beginning their graduation, providing the core tools and foundations to start the journey
- **Intermediate — Network & Ethical Forensics (Sem 5–6)** for students who have completed the Basic level, and for individuals looking to upskill into hands-on security roles
- **Advanced — Incident Response & Digital Forensics (Sem 7)** for students who have finished the earlier levels, and experienced individuals transitioning into specialist roles or entrepreneurship

Programs Key Features

Why Choose Our Courses?

Cyber Range & Cloud Lab: Gain hands-on experience in isolated attack and defence ranges with forensic workstations and cloud sandboxes, for real-world, industry-level security projects.

Industrial Internships & Expert Mentorship: Work on live industry projects, receive guidance from practising security professionals, and get the support you need for your career or entrepreneurial journey.

Personalized Instructor Support: Learn from experienced instructors committed to your growth, whether you are triaging your first alert or leading a full-scope engagement.

	Cyber Range Access	Industry-Integrated Internship	Live Mentorship by Industry Experts	Entrepreneurship Support
Coursera				
Udemy				
UpGrad Online				
Scaler Academy				
Simplilearn				
Unacademy				
EduBlends Academy	✓	✓	✓	✓

Comparison rows left intentionally blank pending verification. Competitor feature claims must be sourced, dated and evidenced before publication.