

Information Booklet cum Syllabus Of Cyber Security & Digital Forensics



September 2026

National Institute of Electronics and Information Technology

An Autonomous Scientific Society under
Ministry of Electronics and Information Technology, Government of India

NIELIT Gorakhpur
MMMUT Campus, Deoria Road
Gorakhpur (U.P.)-273010

S.C Agrawal (Course Coordinator), mob: 8317093881

Sumesh Kannaujia (Course Instructor), Mob: 9161366575

CONTENTS		
Sl. No.	Title	Page No.
1.	About the Course	3
2.	NIELIT	3
3.	Objective of Course	3
4.	Course Outcomes	3
5.	Job Roles of Course	4
6.	Eligibility	4
7.	Total Duration of the Course	4
8.	Course Details (Day-wise, 20 Days)	5-7
9.	Reference Books / Study Material	8

About the Course

This course introduces students to the fundamentals of Cyber Security and Digital Forensics in a step-by-step, beginner-friendly manner. The course begins with Computer and Networking basics so that every student, even with no prior background, can follow along comfortably. It then builds up to core Cyber Security concepts such as threats, attacks, authentication, cryptography and network security, before moving into Digital Forensics — covering evidence handling, disk, memory, mobile and multimedia forensics, and practical exposure to industry-standard forensic tools. The course is designed to be practical, safe and legal throughout, using the instructor's own system, sample files and sample forensic images for all demonstrations.

NIELIT

National Institute of Electronics and Information Technology, NIELIT, (Erstwhile DOEACC Society) is an autonomous scientific society of the Ministry of Electronics & Information Technology, Government of India. The Society is registered under the Societies Registration Act, 1860. NIELIT was set up to carry out Human Resource Development and related activities in the area of Information, Electronics & Communications Technology (IECT). NIELIT is engaged both in Formal & Non-Formal Education in the areas of IECT besides development of industry-oriented quality education and training programmes in the state-of-the-art areas. NIELIT has endeavored to establish standards to be the country's premier institution for Examination and Certification in the field of IECT. It is also one of the National Examination Bodies, which accredits institutes/organizations for conducting courses in IT and Electronics in the non-formal sector.

Objective of Course

The objective of this Cyber Security & Digital Forensics course is to equip NIELIT O Level beginners with a clear, practical understanding of how computer systems, networks and digital evidence work — and how to protect and investigate them. Key Objectives:

- Build strong fundamentals of Computers and Computer Networking before moving to security concepts.
- Understand core Cyber Security concepts – the CIA Triad, threats, vulnerabilities and risk.
- Identify and explain common cyber attacks such as malware, phishing, ransomware and DoS/DDoS.
- Learn Authentication, Access Control and basic Cryptography (encryption, hashing, digital signatures).
- Understand Network and Web Security basics – firewalls, VPN, SQL Injection and XSS concepts.
- Learn the fundamentals of Digital Forensics – evidence handling and the Chain of Custody.
- Gain hands-on exposure to Disk, Memory, Mobile, Browser and Multimedia Forensics.
- Practice with industry-standard forensic tools such as Autopsy, FTK Imager and Wireshark on sample data.
- Prepare a basic forensic investigation report from a sample case study.
- Understand the career scope and ethical/legal responsibilities of a Cyber Security & Digital Forensics professional.

Course Outcomes

After successful completion of this course, students will be able to:

- Understand and explain basic Computer and Networking concepts.
- Identify and explain common Cyber Security threats, vulnerabilities and attacks.
- Explain the CIA Triad, authentication, access control and basic cryptography concepts.
- Understand the fundamentals of Digital Forensics and digital evidence.
- Understand the basic process of evidence collection, preservation and Chain of Custody.
- Perform basic forensic analysis of disk, memory, browser, file and network evidence using sample data.
- Use basic forensic tools such as Autopsy, FTK Imager and Wireshark in an authorized lab environment.
- Prepare a basic Digital Forensics investigation report based on a sample case study.
- Follow ethical, legal and safe practices during Cyber Security and Digital Forensics activities.

Job Roles of Course

After successful completion of this course, students will have a strong foundation for entry-level roles such as:

- Cyber Security intern
- Cyber Security Analyst
- SOC (Security Operations Center) Analyst
- Digital Forensics Trainee
- Network Security Analyst
- Cyber Forensics Associate

Eligibility

10+2 / Graduate (Passed/Appearing) with basic knowledge of computers, Btech / Mtech /BCA/ Bsc (IT/CS), NIELIT O/A Level Courses.

Total Duration of the Course

20 Days (Online) — 3 Hours daily online class, including theory, practical demonstration, examples, quiz, revision and assignment.

Course Details

Week 1 – Computer & Networking Basics

Day	Topics Covered
Day 1	Computer Fundamentals • What is a Computer? • Hardware and Software • CPU, RAM, Hard Disk • Input, Process, Output • Operating System • Files and Folders
Day 2	Introduction to Networking • What is a Computer Network? • Why do we need Networks? • LAN, MAN, WAN, PAN • Internet and Intranet • Client and Server
Day 3	Networking Devices & IP Address • Router, Switch, Hub, Modem, Access Point • IP Address – IPv4 and IPv6 • MAC Address
Day 4	Networking Protocols & OSI Model • What is a Protocol? TCP and UDP • HTTP and HTTPS, DNS and DHCP • OSI 7 Layers with a simple data transfer example
Day 5	Networking Practical • ipconfig, ping, nslookup • Basic network troubleshooting • Week 1 revision and quiz

Week 2 – Cyber Security Fundamentals

Day	Topics Covered
Day 6	Introduction to Cyber Security • Cyber meaning, Cyber Security meaning • CIA Triad • Threat, Vulnerability, Risk • Real-life examples
Day 7	Types of Cyber Attacks • Malware, Virus, Worm, Trojan, Ransomware • Phishing and Social Engineering

	• Brute Force, DoS and DDoS
Day 8	Authentication & Access Control • Authentication vs Authorization • Password Security, MFA/2FA • Least Privilege, Account Protection
Day 9	Cryptography & Data Security • Encryption and Decryption • Symmetric vs Asymmetric Encryption (AES, RSA basics) • Hashing (SHA-256), Digital Signature
Day 10	Network & Web Security • Firewall, VPN • Web Security basics • SQL Injection and XSS concept • Introduction to Incident Response

Week 3 – Digital Forensics

Day	Topics Covered
Day 11	Introduction to Digital Forensics • Digital Forensics meaning • Cyber Security vs Digital Forensics • Types of Digital Forensics, Evidence, Investigation Process
Day 12	Digital Evidence & Chain of Custody • Types of Digital Evidence • Volatile and Non-Volatile Evidence • Evidence Collection, Preservation, Chain of Custody
Day 13	Disk Forensics • Hard Disk and SSD, File Systems (FAT, NTFS, ext4) • Deleted Files concept • Disk Image, Forensic Imaging, Hash Verification
Day 14	Memory Forensics • RAM vs Hard Disk, Volatile Data • Running Processes, Network Connections • Introduction to Memory Dump
Day 15	File, Browser & Network Forensics • File Metadata, Timestamps, File Signatures • Browser History, Cookies, Cache • Network Logs, Timeline Analysis

Week 4 – Practical Forensics & Final Project

Day	Topics Covered
-----	----------------

Day 16	Mobile & Android Forensics • Android Security basics, Mobile Evidence • App Permissions, APK basics • Android Logs
Day 17	Image, Audio & Video Forensics • Multimedia Evidence, EXIF Metadata • Image Authenticity, Audio/Video Properties • Steganography introduction, Hidden Data concept
Day 18	Forensic Tools Practical • Autopsy, FTK Imager, Wireshark (sample data only) • Hash Verification • Preparing a basic Forensic Report
Day 19	Case Study & Investigation • Sample Cyber Incident, Evidence Collection • Log Analysis, Timeline Creation • Suspicious File Examination, Report Preparation
Day 20	Final Assessment & Career Guidance • Cyber Security & Digital Forensics revision • MCQ Test, Viva Questions, Mini Project Presentation • Career Scope and Ethical Responsibilities