Certified Cyber Crime Investigator

JOIN NOW

The **Certified Cyber Crime Investigator (CCCI)** is a comprehensive 60-day (12-week) online certification program designed to equip police officers and law enforcement professionals with practical, courtroom-ready cybercrime investigation skills. Delivered through live Zoom sessions, the course spans 60 hours of structured learning, organized across 12 core themes and 60 specialized topics, covering the full lifecycle of modern digital investigations.

This program bridges the critical gap between conventional policing methods and technology-driven crime investigation. Participants gain hands-on exposure to 50+ cyber forensics, digital crime, and emerging technology domains, including ransomware investigations, financial and banking fraud, social media crimes, dark web activities, cryptocurrency tracing, and AI-driven cyber frauds.

The curriculum is fully aligned with India's latest criminal and procedural laws—**BNS, BNSS, and BSA**—and integrates institutional and operational frameworks involving **I4C, CERT-In, RBI**, **DoT** and other national cyber ecosystems.

The first of its kind in India, the CCCI program is led by **Prof. Triveni Singh**, a renowned cybercrime expert and former IPS officer. This certification is designed to make participants field-ready, legally confident, and technologically empowered.

Fundamentals and Legal Frameworks

Week 1: IT Fundamentals & Cyber Crime Concepts

Focus: Non-technical basics of how computers, networks, and criminals operate.

APRIL 6

Computer Basics for Investigators

Understanding computer definitions, file management, and IT significance.

APRIL 7

How the Internet Connects

LAN/WAN networks, OSI model, and TCP/IP protocols.

APRIL 8

Cyber Crime & Threats

The "CIA Triad" and threats like malware and phishing.

APRIL 9

Social Engineering & Fraud

Fake websites and online frauds.

APRIL 10

The Cyber Kill Chain

MITRE TTPs and real-world case studies.

Week 2: New Legal Frameworks (BNS, BNSS, BSA)

Focus: India's new criminal laws and digital evidence rules effective from 2024.

APRIL 13

The Information Technology Act (IT Act 2000)

Penalties for hacking and data theft.

APRIL 14

Data Privacy Law (DPDP Act 2023)

Consent requirements and penalties.

APRIL 15

New Penal Law (Bharatiya Nyaya Sanhita - BNS)

Organized crime and digital extortion.

APRIL 16

New Procedure Law (Bharatiya Nagarik Suraksha Sanhita - BNSS)

Mandatory audio-video recording and e-FIRs.

APRIL 17

New Evidence Law (Bharatiya Sakshya Adhiniyam - BSA)

Electronic records as primary evidence.

Institutional Ecosystem & Evidence Collection

Week 3: Institutional Ecosystem & First Response

Focus: The role of Indian agencies (I4C, Regulators) and handling crime scenes.

APRIL 20	**Indian Cyber Regulatory Frameworks** RBI, IRDAI, SEBI, CERT-In, and NCIIPC.
APRIL 21	**The I4C (MHA) Ecosystem** NCRP Portal, Sahyog Portal, Samanvaya Platform & Patibimb.
APRIL 22	**DoT (Department of Telecommunication) Ecosystem** Sanchaar Sathi, Chaksu, ASTR/CEIR/TAFCOP/DIP
APRIL 23	**Search and Seizure** SOPs for raiding and seizing live systems.
APRIL 24	**Basic Forensic Procedure & Labs** Role of National Cyber Forensic Labs (NCFL), State FSL & Police Cyber Lab

Week 4: Evidence Collection & Hardware Forensics

Focus: Setting up the forensic lab and securing physical hard drives.

APRIL 27	**The Forensic Workstation** Write-blockers and high-speed drives.
APRIL 28	**Essential Software Tools** EnCase, FTK, Autopsy, ProDiscover.
APRIL 29	**Understanding Storage (Disk Forensics)** Unallocated clusters and hidden data.
APRIL 30	**Making Safe Copies (Imaging)** "Bit-stream" forensic imaging.
MAY 1	**Proving Integrity (Hashing)** MD5/SHA-256 hashes for court.

Mobile & Network Forensics

Week 5: Mobile Phones & Damaged Devices

Focus: Recovering data from smartphones and broken electronics.

MAY 4	**Seizing Mobile Phones** Using Faraday bags.
MAY 5	**Mobile Data Extraction** Bypassing locks.
MAY 6	**Chat & App Analysis** WhatsApp, Telegram, and location history.
MAY 7	**Handling Damaged Media** "Chip-off" techniques for broken cards.
MAY 8	**Advanced File Recovery** Data carving reconstruction.

Week 6: Network Security & Web Investigations

Focus: Tracking suspects online and analyzing network traffic.

MAY 11	**Firewalls & Intrusion Detection** Investigating security logs.
MAY 12	**Network Forensics (PCAP)** Analyzing live traffic.
MAY 13	**Analyzing Web Browsers** History, cookies, and downloads.
MAY 14	**Email Investigation** Header analysis and spoofing detection.
MAY 15	**CDR & IPDR** Mapping calls and locations.

Security Strategy & Malware Response

Week 7: OS Security & Defense Strategy

Focus: Operating systems, logs, and the ecosystem of attack and defense.

MAY 18

Windows Security

Hardening and group policies.

MAY 19

Linux Security

Permission controls and access.

MAY 20

Blue Team vs. Red Team

Attackers vs. Defenders ecosystem.

MAY 21

Centralized Log Analysis

Splunk.

MAY 22

Automated Threat Detection (SIEM)

Real-time incident correlation.

Week 8: Malware & Ransomware Response

Focus: Investigating viruses, ransomware, and memory artifacts.

MAY 25

Malware Basics (Static Analysis)

Code analysis without execution.

MAY 26

Malware Behavior (Dynamic Analysis)

Sandbox testing.

MAY 27

Ransomware Attack & DFIR

Negotiation and root cause analysis.

MAY 28

Capturing Memory (RAM)

Dumping live memory.

MAY 29

Threat Hunting

Using Indicators of Compromise (IOCs).

Advanced Threats & Dark Web

Week 9: Multimedia, AI & Future Threats

Focus: Validating media and understanding AI risks.

JUNE 1

Video & CCTV Forensics

Authentication and enhancement.

JUNE 2

Audio Forensics

Voice biometrics and cleanup.

JUNE 3

Deepfake Detection

Spotting AI-generated videos.

JUNE 4

AI Risk and Forensics

AI voice scams and cyber attacks.

JUNE 5

Steganography

Detecting hidden data in images.

Week 10: Dark Web & Crypto

Focus: The hidden internet and digital money.

JUNE 8

Dark Web Investigation

Tor networks and marketplaces.

JUNE 9

Cryptocurrency & Blockchain

Tracing Bitcoin transactions.

JUNE 10

Drone Forensics

Flight logs and GPS tracks.

JUNE 11

Vehicle Forensics

EDR speed and location history.

JUNE 12

Cloud Forensics

AWS/Google Cloud evidence acquisition.

CPT
CENTRE FOR POLICE TECHNOLOGY

Financial Crime & Final Simulations

Week 11: Financial Crime & Asset Recovery

Focus: Banking fraud, money laundering, and freezing assets.

JUNE 15

Banking Fraud Investigation

Transaction logs and synthetic identities.

JUNE 16

Money Laundering (AML)

Smurfing and shell companies.

JUNE 17

Freezing & Defreezing Accounts

Legal procedures.

JUNE 18

E-Discovery

Automated large data search.

JUNE 19

Password Cracking

Accessing locked evidence.

Week 12: Simulations & Final Reporting

Focus: Practical application, war-gaming, and final assessment.

JUNE 22

Tabletop Exercise (Phishing/Malware)

Guided simulation.

JUNE 23

Tabletop Exercise (Ransomware/Data Breach)

Crisis management.

JUNE 24

Final Forensic Report

Drafting admissible reports.

JUNE 25

Charge Sheet Submission

Compiling evidence for prosecution.

JUNE 26

Course Review & Final Q&A

Roadmap for future learning.

Certification Completion: Upon successful completion of all 60 sessions and final assessments, participants will receive the **Certified Cyber Crime Investigator (CCCI)** certification, making them field-ready, legally confident, and technologically empowered to handle modern cybercrime investigations.

For any queries please email us at :- triveni@algoritha.in

JOIN NOW