Course Overview

This intensive program equips law enforcement professionals with practical skills across 40+ cyber forensics domains, from disk imaging and memory analysis to blockchain tracing and deepfake detection. Through targeted modules, participants master industry-standard tools, chain-of-custody protocols, and courtroom-ready reporting. Designed for rapid field deployment, the syllabus transforms complex digital evidence into prosecutable cases, covering mobile extractions, network traffic dissection, dark web investigations, and predictive policing analytics. Perfect for investigators advancing cybercrime response capabilities.

Module 1: Disk Forensics: The Foundation of Evidence

Date: 07th February, 12:00-1:00 PM

- Hardware Anatomy: Explore HDD magnetic platters, actuator arms, and servo patterns alongside SSD NAND flash wear-leveling and over-provisioning, plus NVMe controller queues for targeted data carving in unallocated clusters and bad sectors.
- Forensic Acquisition: Differentiate physical bit-stream imaging with Tableau write-blockers to capture deleted partitions from logical file copies via FTK Imager, employing ddrescue for skipping damaged areas while preserving original timestamps.
- Integrity Verification: Generate MD5/SHA-256 hashes pre- and post-imaging for chain-of-custody validation, parsing NTFS $MFT/$Bitmap for timeline reconstruction and detecting anti-forensic wiping patterns.

Module 2: Mobile Forensics: Pocket-Sized Crime Scenes

Date: 08th February, 12:00-1:00 PM

- Device Seizure: Isolate active phones in Faraday bags to prevent remote wipes, handling powered-on devices with airplane mode versus chip-off for bricked units requiring BGA reprogramming.
- Extraction Levels: Perform logical ADB backups for app databases, file system JTAG dumps bypassing locks, and physical NAND mirroring with Cellebrite UFED Physical, tackling full-disk encryption via checkm8 exploits.
- App Analysis: Decrypt SQLite artifacts from WhatsApp chats and Telegram secrets, reconstruct location timelines from Google Maps caches, and link cloud-synced deletions to on-device notifications.

Module 3: Video/CCTV/DVR Forensics: Capturing Motion Evidence

Date: 14th February, 12:00-1:00 PM

- Frame Authentication: Detect splicing via GOP inconsistencies, frame duplication ghosts, and compression artifacts using Amped FIVE for error level analysis and motion vector validation.

- Enhancement Techniques: Apply super-resolution upscaling, de-noising filters, and stabilization algorithms to clarify license plates and faces in low-light footage from Hikvision or Dahua DVRs.
- Timeline Synchronization: Correlate CCTV timestamps with NVR logs and EXIF data, building multi-camera event sequences for alibi disproval in assault or theft reconstructions.

Module 4: Audio Forensics: Decoding Sound Signatures

Date: 15th February, 12:00-1:00 PM

- Authenticity Verification: Identify editing seams through spectrogram discontinuities, phase mismatches, and background noise anomalies with Audacity or iZotope RX spectral repair.
- Voice Biometrics: Extract formant patterns and pitch contours for speaker identification, filtering environmental artifacts to isolate confessions or threats from call recordings.
- Enhancement Protocols: Amplify faint whispers, remove echo/reverb, and synchronize multi-track audio for courtroom playback, validating chain-of-custody via waveform hashing.

Module 5: GPS Forensics: Tracking Digital Footprints

Date: 21st February, 12:00-1:00 PM

- Device Data Harvesting: Parse GPX/KML files from Garmin/Apple Watches, extracting waypoints, speed profiles, and elevation changes from NMEA sentences in device SQLite databases.
- Track Reconstruction: Correlate satellite ephemeris with assisted GPS logs to validate alibis, detecting spoofing via signal strength anomalies and map projection errors.
- Cross-Device Linking: Merge vehicle OBD-II telematics with smartphone location histories, generating heatmaps and route animations for vehicular homicide or evasion cases.

Module 6: Vehicle Forensics: Engines of Evidence

Date: 22nd February, 12:00-1:00 PM

- ECU/EDR Extraction: Interface with CAN bus via OBD-II dongles to dump event data recorders for speed, braking, and airbag deployment sequences in Bosch CDR tools.
- Infotainment Mining: Recover navigation histories, Bluetooth pairings, and dashcam loops from SYNC/CarPlay modules, parsing exFAT partitions for deleted media.
- Tamper Detection: Analyze firmware checksums and odometer discrepancies against GPS logs, reconstructing accident timelines for insurance fraud prosecutions.

Module 7: Drone Forensics: Aerial Incident Analysis

CENTRE FOR POLICE TECHNOLOGY

Date: 28th February, 12:00-1:00 PM

- Flight Log Acquisition: Extract telemetry from DJI .DAT files including GPS tracks, battery telemetry, and no-fly zone breaches using DroneDEPLOY or Autel Explorer parsers.
- Media Artifact Recovery: Carve video stills from SD cards, validating geolocation metadata against flight paths to confirm surveillance over restricted areas.
- Controller Synchronization: Link remote controller logs with drone blackbox data for operator attribution, detecting remote hacks via anomalous command injections.

Module 8: DarkWeb Forensics: Shadows of the Onion

Date: 01st March, 12:00-1:00 PM

- Tor Network Mapping: Deploy hidden service crawlers and bridge scanners to index .onion sites, tracing exit nodes via correlation attacks on traffic timing.
- Marketplace Evidence: Cluster vendor wallets and PGP keys across forums using Memex or Flashpoint, de-anonymizing via shipping address leaks and captcha solves.
- Chain Analysis Integration: Link blockchain transactions to dark pools with Crystal Blockchain, generating attribution graphs for RICO takedowns of cybercrime syndicates.

Module 9: Face Forensics: Identifying Individuals from Images

Date: 7th March, 12:00-1:00 PM

- Facial Recognition Basics: Use landmark detection to map eyes, nose, and mouth positions, comparing feature vectors with tools like FaceNet for matching suspects across CCTV and social photos.
- Liveness Detection: Check micro-movements like eye blinks or head tilts to spot spoofing attempts with masks or printed images, using optical flow analysis.
- Aging and Disguise Handling: Apply GAN models to simulate age progression or remove glasses/beards, ensuring matches despite appearance changes in long-term investigations.

Module 10: OSINT: Gathering Public Intelligence

Date: 8th March, 12:00-1:00 PM

- Source Collection: Scrape social media profiles, forums, and news sites using tools like Maltego or SpiderFoot to build target dossiers from usernames and emails.
- Geolocation Mapping: Extract EXIF data from photos and correlate IP addresses with WHOIS lookups, plotting movements on Google Earth overlays.
- Relationship Mapping: Link entities via graph visualization, uncovering networks from shared contacts, hashtags, or domain registrations.

Module 11: E-Discovery: Managing Legal Data Searches

Date: 14th March, 12:00-1:00 PM

- Data Identification: Scan custodians' emails, drives, and cloud storage for keywords, dates, or custodians using Relativity or Nuix for scalable processing.
- Review and Redaction: Apply predictive coding with machine learning to prioritize relevant documents, auto-redacting PII like SSNs before production.
- Production Export: Generate Bates-numbered TIFFs with metadata load files, ensuring defensible chain-of-custody for litigation holds and court submissions.

Module 12: Document Tampering Detection: Spotting Fake Files

Date: 15th March, 12:00-1:00 PM

- Metadata Examination: Check creation dates, author names, and revision history in PDFs/Word docs for inconsistencies using ExifTool or PDF Analyzer.
- Visual Artifact Checks: Look for font mismatches, cloning edges, or unnatural alignments with ELA (Error Level Analysis) in Photoshop or Forensically.
- Hash and Signature Validation: Compare file hashes against originals and verify digital signatures to confirm unaltered documents for court evidence.

Module 13: Photo/Image Forensics: Authenticating Visual Evidence

Date: 21st March, 12:00-1:00 PM

- Compression Analysis: Detect JPEG artifacts and resaving traces to identify edits, using tools like FotoForensics for level discrepancies.
- Noise Pattern Matching: Analyze sensor noise (PRNU) to link images to specific cameras, even after cropping or resizing.
- Clone Detection: Find duplicated regions via block matching algorithms, exposing composite images in fraud or alibi cases.

Module 14: AML/CTF: Tracking Money Laundering and Terror Financing

Date: 22nd March, 12:00-1:00 PM

- Transaction Monitoring: Flag suspicious patterns like structuring (smurfing) or rapid in-out transfers using rules-based systems in Actimize or SAS AML.
- Network Analysis: Map beneficial owners through shell companies with graph tools, linking wallets across exchanges via address clustering.
- Risk Scoring: Assign customer risk scores based on PEP status, high-risk jurisdictions, and behavioral anomalies for SAR filings.

Module 15: Banking Data Investigation: Uncovering Financial Crimes

Date: 28th March, 12:00-1:00 PM

- Account Ledger Review: Trace wire transfers, ACH batches, and check images for unauthorized access, reconstructing flows with Excel pivots or SQL queries.
- Know Your Customer Checks: Verify IDs against sanctions lists (OFAC/SDN) and match transaction velocities to stated business purposes.
- Fraud Pattern Detection: Identify synthetic identities or account takeovers via velocity rules and device fingerprinting in core banking logs.

Module 16: Cell Site Analyser: Mapping Mobile Locations

Date: 29th March, 12:00-1:00 PM

- Call Detail Record Parsing: Extract IMSI, cell tower IDs, and timing advances from CDR files to estimate subscriber locations within 100-500 meters.
- Tower Mapping: Overlay cell site polygons on maps using Google Earth or Tower Collector, correlating handovers for travel routes.
- Historical Analysis: Reconstruct timelines from historical dumps, validating alibis by matching signal strength to claimed positions during crimes.

Module 17: Forensic Workstation: Building Secure Analysis Platforms

Date: 04th April, 12:00-1:00 PM

- Hardware Configuration: Assemble high-RPM drives in RAID arrays, GPU accelerators for hashing, and write-block interfaces to process multiple evidence sources without contamination.
- Software Stack Setup: Install EnCase, FTK, Autopsy, and Volatility on hardened Linux distros like Kali or SIFT, with virtualized sandboxes for malware handling.
- Chain-of-Custody Logging: Automate audit trails with tamper-proof logging and remote attestation, ensuring workstation integrity for court validation.

Module 18: Forensics Audit: Ensuring Evidence Integrity

Date: 05th April, 12:00-1:00 PM

- Process Validation: Review acquisition hashes, tool versions, and analyst actions against NIST standards to confirm defensible methodologies.
- Artifact Verification: Cross-check timelines, file carvings, and extractions for

consistency across tools like Wireshark and X-Ways.

- Report Certification: Generate signed affidavits with embedded hashes, detailing deviations and peer reviews for admissibility challenges.

Module 19: Information System Audit: Securing Enterprise Environments

Date: 11th April, 12:00-1:00 PM

- Vulnerability Scanning: Run Nessus or OpenVAS to map assets, identifying unpatched systems and weak configurations pre-incident.
- Log Aggregation: Centralize SIEM feeds from Windows Events, Syslog, and firewall logs for anomaly baseline establishment.
- Compliance Mapping: Align controls with ISO 27001, PCI-DSS via checklists, recommending remediations with risk prioritization.

Module 20: Steganography: Detecting Hidden Communications

Date: 12th April, 12:00-1:00 PM

- Embedding Detection: Apply chi-square attacks and RS analysis to flag statistical anomalies in images, audio, and network packets.
- Payload Extraction: Use StegSolve and Outguess for LSB flips, palette manipulations, and DCT coefficient hiding recovery.
- Tool Signature Matching: Identify stego artifacts from OpenStego, SilentEye by entropy profiles and palette histograms.

Module 21: Quantum Cryptography: Securing Against Future Threats

Date: 18th April, 12:00-1:00 PM

- QKD Protocol Implementation: Deploy BB84 for key exchange over fiber, detecting eavesdroppers via quantum bit error rates.
- Post-Quantum Algorithms: Transition to lattice-based Kyber and Dilithium signatures resistant to Shor's algorithm attacks.
- Hybrid System Integration: Combine classical PKI with quantum-safe hashes for forward secrecy in high-value networks.

Module 22: Web Browser Forensics: Tracing Online Activities

Date: 19th April, 12:00-1:00 PM

- Cache and History Recovery: Parse Chrome SQLite databases for visited URLs, download paths, and favicon caches from WebCacheV01.dat.

- Session Artifact Analysis: Extract cookies, LocalStorage, and IndexedDB for login persistence and form autofill data.
- Extension Telemetry: Link rogue add-ons to C2 domains via manifest.json and background script logs.

Module 23: Password Recovery: Cracking Access Controls

Date: 25th April, 12:00-1:00 PM

- Hash Extraction: Dump SAM hives, APFS containers, and keychain files for NTLM, bcrypt, and FileVault2 hashes.
- Attack Method Selection: Run Hashcat GPU attacks with dictionary, brute-force, and hybrid rulesets optimized by PRINCE.
- Rainbow Table Usage: Accelerate recovery with precomputed tables for LM/NTLM while handling salting defenses.

Module 24: CDR/IPDR/PCAP Analysis: Reconstructing Network Events

Date: 26th April, 12:00-1:00 PM

- Record Parsing: Extract ANI/DNIS, cell IDs, and durations from CDR files; decode SIP/RTP from IPDR dumps.
- Traffic Flow Visualization: Filter PCAPs in Wireshark for VoIP signaling, geolocating via timing advance and tower dumps.
- Correlation Timeline: Merge call logs with packet captures for full communication graphs in fraud and threat hunting.

Module 25: Big Data Analytics: Processing Massive Evidence Volumes

Date: 02nd May, 12:00-1:00 PM

- Data Ingestion Pipelines: Load petabyte-scale logs from SIEMs and endpoints into Hadoop/Spark clusters for distributed processing and real-time indexing.
- Anomaly Detection Models: Train machine learning algorithms like Isolation Forests to flag outliers in transaction streams and user behaviors.
- Visualization Dashboards: Build interactive Kibana/Elastic graphs correlating IoT telemetry with financial flows for investigative insights.

Module 26: Email Forensics: Tracing Digital Communications

Date: 03rd May, 12:00-1:00 PM

- Header Analysis: Parse SMTP envelopes for SPF/DKIM failures, routing hops, and sender IPs to expose spoofing and relay abuse.
- Attachment Carving: Recover embedded PDFs/images from EML/MBOX files, scanning for malware and metadata discrepancies.
- Thread Reconstruction: Link reply chains via Message-ID references, timeline-building across PST/OST archives for harassment cases.

Module 27: Network Forensics: Capturing Traffic Trails

Date: 9th May, 12:00-1:00 PM

- Packet Capture Setup: Deploy taps and SPAN ports feeding Wireshark/Zeek for full-protocol dissection and session reconstruction.
- Flow Analysis: Aggregate NetFlow/sFlow data to map C2 communications, identifying beacons via periodic DNS queries.
- Encryption Decryption: Extract session keys from memory dumps, correlating TLS handshakes with endpoint artifacts.

Module 28: Malware Forensics: Dissecting Malicious Code

Date: 10th May, 12:00-1:00 PM

- Static Analysis: Reverse binaries with IDA Pro/Ghidra, identifying packers and API import tables without execution.
- Dynamic Sandboxing: Monitor Cuckoo/ANY.RUN behaviors, capturing registry changes, file drops, and network callbacks.
- IOC Generation: Extract YARA signatures and atomic indicators for threat intel sharing and endpoint protection.

Module 29: Cyber Forensics Van: Mobile Response Unit

Date: 16th May, 12:00-1:00 PM

- Field Acquisition Kit: Equip with Tableau imagers, Faraday tents, and rugged laptops for on-scene disk/memory dumps.
- Live Network Triage: Run tcpdump mirrors and nmap scans from vehicle-mounted cellular arrays during active incidents.
- Satellite Data Relay: Encrypt and beam evidence previews to HQ labs for parallel processing and warrant support.

Module 30: Predictive Policing: Forecasting Criminal Patterns

Date: 17th May, 12:00-1:00 PM

- Risk Terrain Modeling: Overlay crime data with environmental factors on GIS maps to prioritize patrol zones.
- Recidivism Algorithms: Score individuals using COMPAS-like models balancing demographics with offense history.
- Real-Time Alerts: Push geofenced notifications from fusion centers when suspects approach high-risk areas.

Module 31: Case Management: Streamlining Investigations

Date: 23rd May, 12:00-1:00 PM

- Evidence Tracking: Log chain-of-custody entries with barcode scanners and blockchain timestamps across agency databases.
- Collaboration Portals: Share redacted report sections via secure portals like CaseGuard for multi-jurisdictional teams.
- Analytics Integration: Auto-generate link charts from entity extraction, surfacing connections across open cases.

Module 32: Social Media Analytics: Mapping Online Networks

Date: 24th May, 12:00-1:00 PM

- Profile Clustering: Group accounts by shared content hashes and interaction graphs using Gephi/Maltego transforms.
- Sentiment Trend Analysis: Run NLP on posts/comments to detect radicalization spikes and coordinated campaigns.
- Geosocial Mapping: Correlate check-ins, geotags, and device signals for movement patterns in extremism monitoring.

Module 33: Damaged Media Forensics: Recovering Corrupted Evidence

Date: 30th May, 12:00-1:00 PM

- Damage Assessment: Identify physical issues like scratches on HDD platters or NAND flash failures in SSDs, using magnifiers and electrical testing to map accessible sectors.
- Specialized Imaging: Apply chip-off techniques for NAND removal or JTAG for controller bypass, creating partial bit-stream copies with error correction codes.
- Data Carving Recovery: Reconstruct files from fragmented clusters using signature-based carving tools like Foremost, verifying fragments via hash matching.

Module 34: Memory Forensics: Capturing Volatile RAM Data

Date: 31st May, 12:00-1:00 PM

- Volatile Evidence Capture: Dump live RAM using tools like Volatility or Rekall before shutdown to preserve running processes and encryption keys.
- Process Analysis: Scan for hidden tasks with PSList/PSScan plugins, detecting injected code via process hollowing and cross-view validation.
- Artifact Extraction: Recover network connections, clipboard data, and unsaved files from VAD trees and kernel pools for attack timeline reconstruction.

Module 35: AI/Deepfake Forensics: Detecting Synthetic Media

Date: 06th June, 12:00-1:00 PM

- Facial Inconsistency Checks: Spot blending errors, unnatural eye reflections, and lip-sync mismatches using biological signal analysis like blood flow patterns.
- Model Artifact Detection: Identify GAN fingerprints such as frequency anomalies and noise inconsistencies with tools like Deepware Scanner.
- Provenance Tracing: Verify media origins via blockchain timestamps and sensor metadata to authenticate unaltered footage.

Module 36: Crypto/Blockchain Forensics: Tracking Digital Transactions

Date: 07th June, 12:00-1:00 PM

- Address Clustering: Group wallets by common spending patterns and dust attacks using Chainalysis or Elliptic tools.
- Transaction Graph Analysis: Map fund flows across mixers and exchanges, de-anonymizing via KYC data correlation.
- Privacy Coin Tracing: Apply timing analysis and decoy elimination to Monero rings for asset seizure support.

Module 37: Cloud Forensics: Investigating Virtual Storage

Date: 13th June, 12:00-1:00 PM

- Artifact Collection: Pull logs from AWS CloudTrail, Azure Monitor, and Google Cloud Audit via API queries under legal warrants.
- Multi-Tenant Isolation: Correlate VM snapshots with account activity, overcoming ephemeral storage challenges.
- Deleted Data Recovery: Parse recycle bins and version histories from S3/Blob storage for timeline reconstruction.

Module 38: Child Abuse Forensics: Protecting Vulnerable Victims

Date: 14th June

- Image Hash Matching: Scan collections against NCMEC/CAID databases using perceptual hashes to identify known abuse material.
- Metadata Timeline Building: Extract EXIF sequences and device IDs to trace

production and distribution networks.

- Victim Identification: Apply facial recognition with age estimation while preserving anonymity in multi-jurisdictional task forces.