Laxhar Lab

NABL ACCREDITED
FORENSIC LABORATORY

LEARN from
The **EXPERT...**

LIFE

Laxhar Institute of Forensic Excellence

www.laxhar.com

Step into the captivating world of
Laxhar Institute of Forensic Excellence (LIFE)

LIFE is a forensic training program by **Laxhar Forensic Labs**, dedicated to scientific accuracy, ethical integrity, and legal compliance.

Courses We Offer

At LIFE, we bridge the gap between textbook theory and elite professional practice. We offer several Advance Training Certification Programmes, designed to transform students and professionals into industry-ready forensic experts through intensive hands-on training, navigated by world-class technology.

01
Training Certification in
INTEGRATED FORENSIC INVESTIGATION & EVIDENCE EXAMINATION

02
Advance Training Certification in
COMPUTER FORENSICS AND INVESTIGATION

03
Advance Training Certification in
MOBILE FORENSIC AND INVESTIGATION

04
Advance Training Certification in
QUESTIONED DOCUMENT EXAMINATION

05
Advance Training Certification in
MULTIMEDIA (AUDIO/VIDEO/IMAGE) FORENSIC EXAMINATION

06
Advance Training Certification in
TECHNICAL SURVEILLANCE COUNTER MEASURE

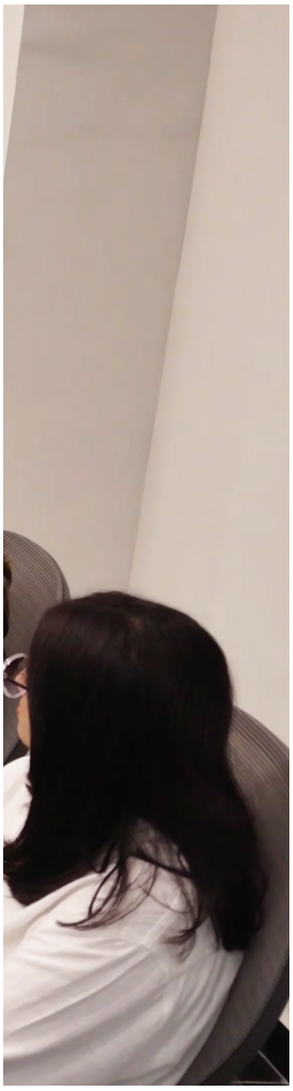
07
Advance Training Certification in
FORENSIC JOURNALISM

LEARN

from the expertise of Laxhar Forensic Lab?

Secure your future in forensics by training at a premier facility that bridges the gap between academic theory and high-stakes investigation.

Train in an elite forensic lab certified with ISO/IEC 17025:2015 certifications, ensuring your education meets the highest international standards for technical competence.



World-Class Technology

Gain hands-on mastery over the industry's most advanced equipment, including REI-USA TSCM kits, Tableau TX1, Video Spectral Comparators, FTK, Oxygen Forensics, iMazing, Amped, Semen detection Kit, Blood Detection Kit, Tyre Print Kit, Ballistic kit, Forensic Microscopes, 30+ CSI kits, etc.

Case-Driven Methodology

We move beyond textbooks to immerse you in real-world forensic cases, teaching you the entire professional workflow from pre-testing to final court-ready report making.

Elite Mentorship

Learn directly from distinguished working scientists and industry titans, including a world-record-holding forensic journalist.

Individualised Mastery

To ensure personalised guidance and maximum time with our high-end instruments, we strictly limit our intake to just 12 students per batch.

Career Launchpad

Benefit from comprehensive professional support, including internship assistance, interview preparation, and specialised grooming to make you immediately industry-ready.

Training Certification in

INTEGRATED FORENSIC INVESTIGATION & EVIDENCE EXAMINATION

This elite, multi-disciplinary programme is engineered for professionals or students who require a comprehensive mastery of the modern forensic landscape. By merging the core pillars of Digital Forensics, Questioned Documents, Multimedia Analysis, CSI and TSCM, this course provides a unified workflow for high-stakes investigations. Participants will learn to navigate complex cases that involve cross-platform evidence–from identifying hidden espionage devices and analyzing manipulated digital records to verifying the authenticity of physical documents and multimedia files.

Topics covered

- **Crime Scene Management & Reconstruction:** Master the physical search, crime scene sketching, and photography techniques required to reconstruct complex incident scenes and maintain a legally defensible chain of custody under BSA 2023.
- **Digital Evidence Acquisition and Investigation:** Execute bit-stream imaging and logical/physical extractions from HDDs, SSDs, and external storage using industry-standard hardware like the Tableau TX1 and FTK, Oxygen.
- **Mobile Device Forensics:** Perform deep-dive analysis of Android and iOS devices using Oxygen Forensic Detective, Imazing, to recover deleted media, encrypted app data (WhatsApp/Telegram), and system logs.
- **Disk Structure & File Systems:** Understand the architectural differences between HDD, SSD, and Hybrid drives, including interfaces (SATA/PCIe), connectors, and the mechanics of how data is stored across various file systems (NTFS/FAT32/APFS).
- **Multimedia Authentication:** Detect sophisticated tampering in images and videos, such as cloning or frame deletion, using Amped Authenticate and VideoCleaner.
- **Forensic Video Enhancement:** Apply stabilization, motion deblurring, and super-resolution algorithms in Amped FIVE to clarify obscured details like license plates or facial features.
- **Fingerprint Examination:** Identification, development, lifting of latest fingerprint, comparison & analysis of fingerprint pattern/ridges.
- **Metadata & Geolocation Forensics:** Extract hidden EXIF, XMP, and GPS data to map the spatial and temporal origins of digital evidence.
- **Speaker Identification & Biometrics:** Perform acoustic signal processing and phonetic analysis of formants (F1, F2, F3) to verify vocal identities and detect audio splicing.
- **Questioned Document Examination:** Verify the authenticity of signatures and handwriting while identifying chemical or mechanical erasures and obliterations in disputed documents.
- **Documents Security Feature Analysis:** Utilize Alternate Light Source, microscopy and other techniques to validate protective elements in high-security instruments like Passports, Banknotes, and Identity Cards.
- **Printed Documents Examination:** Printing Mechanisms, Analysis of Ink and Paper using microscopic techniques and alternate light sources.
- **Technical Surveillance Counter Measures (TSCM):** Conduct professional sweeps to detect and neutralize covert microphones, hidden cameras, and GPS trackers using Spectrum Analyzers, thermal imaging and NLJDs.
- **Network & Cloud Forensics:** Investigate indicators of compromise (IoCs) in iPhone and Android systems, C2 traffic, and cloud-based artifacts to identify data leaks or unauthorized access.
- **Expert Reporting & Legal Testimony:** Synthesize multi-domain technical findings into a unified, court-ready forensic report and practice expert defense in a mock courtroom setting.

Hands-on Training

1. **Crime Scene & Evidence Management**
   - Execute systematic physical searches and utilize forensic sketching and high-resolution photography to document incident scenes in situ.
   - Implement rigorous chain of custody protocols and evidence labelling compliant with the Bharatiya Sakshya Adhiniyam (BSA) 2023.
   - Secure and package various forms of physical and digital evidence to prevent contamination or data loss during transit.
2. **Digital & Mobile Data Acquisition and Analysis**
   - Perform bit-stream imaging and physical block-level acquisition of HDDs and SSDs using the Tableau TX1 to ensure 1:1 forensic integrity.
   - Utilize Oxygen Forensic Detective and iMazing to conduct logical and physical extractions from Android and iOS devices, including smartwatches.
   - Recover "deleted" media fragments and extract database artifacts from encrypted applications like WhatsApp and Telegram.
   - Identify Indicators of Compromise (IoCs)–including malicious file hashes, suspicious domains, and C2 traffic–using tools like iMazing, Console, Activity Monitor, Wireshark, VirusTotal and YARA to detect system-level breaches.
   - Investigate Cloud Artifacts and token-based access for Google and iCloud accounts to recover synchronized backups, photos, and location history.
3. **Advanced Multimedia Analysis**
   - Detect pixel-level tampering and image cloning in Amped Authenticate using Error Level Analysis (ELA) and PRNU sensor fingerprinting.
   - Execute non-destructive video and image enhancement within the Amped FIVE workflow.
   - Apply super-resolution and frame averaging to clarify obscured details such as license plates or facial features in low-quality CCTV footage.
   - Execute acoustic signal processing and phonetic analysis of formants (F1,F2,F3) to verify vocal identities and detect audio edits.
4. **Metadata and Hex Analysis**
   - Perform manual Hex analysis and signature inspection of file headers to identify masked file types or manual data splicing.
   - Map GPS coordinates and device signatures from extracted EXIF and XMP metadata to establish spatial-temporal correlations.
5. **Technical Surveillance**
   - Conduct professional sweeps to detect hidden microphones and cameras using Spectrum Analyzers, NLJDs, and Thermal Imagers.
6. **Questioned Documents Analysis**
   - Examine and compare Handwriting and signature samples with questioned samples.
   - Validate security features in high-value instruments like Banknotes and Passports by inspecting watermarks, microtext, and UV-reactive elements.
   - Analyse printing mechanisms, ink discharge patterns, and paper fibre compositions using microscopic techniques and Alternate Light Sources.
   - Detect document alteration and decipher indentation marks on documents
   - Digital documents, digitally captured signature and handwriting analysis.
7. **Fingerprint Impression Analysis**
   - Identification of latent fingerprint using alternate light sources.
   - Development, lifting and analysis of fingerprint pattern.
   - Development of fingerprint from wet surfaces using SPR technique.
8. **Legal Documentation & Courtroom Skills**
   - Synthesize multi-domain technical findings into a unified, court-ready expert report and defend the methodology in mock courtroom trials.

Programme Details

- Duration: 2 Months.
- Mode: Offline (Hands-on Lab training).

Advance Training Certification in

COMPUTER FORENSICS AND INVESTIGATION

Our course, Advance Training Certification in Computer Forensic Investigation, provides a comprehensive understanding of how to identify, collect, preserve and analyze digital evidence from storage devices such as hard drives, SSDs and external media. The course focuses on the principles of forensic imaging, data recovery and analysis of file systems, while maintaining the integrity of evidence. Students will gain practical experience in using professional forensic tools to recover deleted, hidden, or encrypted data and to interpret digital traces relevant to investigations. Emphasis is placed on the legal and ethical standards that guide digital evidence handling and reporting in forensic examinations.

Topics covered

- Introduction to Computer Forensics and its importance in real-life investigations.
- Different types of storage media and their types
- How HDD, SSD & Hybrid drives work and their parts
- Different types of disk interfaces and their connectors
- Understanding Disk Structure and File Systems
- Types of data & how data is stored in a device
- Introduction to the operating system
- Seizures of digital evidence and detailing
- Collection of evidence by disassembling
- Collection of evidence from running machine – RAM capturing
- Examination of Encrypted and Protected Volumes
- Introduction to Malware, rootkit & spyware
- Standard procedure for handling disk evidence
- Introduction to write blockers and their types
- Forensic Imaging and Evidence Acquisition
- Data Integrity Verification and Hashing Techniques
- Recovery of Deleted, Hidden, and Encrypted Data
- Metadata and File Signature Analysis
- Law related to Computer Forensics
- Chain of Custody and Evidence Management
- Forensic Report Preparation and Documentation
- Practical Case Study and Investigation Simulation

Hands-on Training

- **Components of disks:** Identify HDD and SSD components and their functions.
- **RAM:** Locate and explain pagefile.sys and hiberfil. sys and where to check them.
- **Registry:** Show where to find important registry values and how to view them.
- **SOPs:** Write standard operating procedures covering the entire workflow up to courtroom presentation.
- **Crime-scene photography:** Document proper crime-scene photography techniques and forensic investigative steps.
- **Laptop disassembly:** Safely disassemble laptops and extract internal drives for analysis.
- **Live forensics:** Detect whether a disk is encrypted and use an Encrypted Disk Detector (EDD).
- **Live forensics:** Capture RAM correctly and preserve volatile evidence.
- **Virus Total:** Use VirusTotal for online malware scanning and interpreting results.
- **Hashing:** Calculate and verify hash values using tools like Hash My Files and AccuHash.
- **FTK - RAM Capture:** Hands-on practice creating forensically sound images and RAM captures.
- **Volatility & CAINE:** Hands-on use of Volatility and CAINE for memory and system analysis.
- **Data recovery:** Recover data from HDDs, SSDs, memory cards and USB drives, including common failure scenarios.
- **TX1 procedures:** Perform TX1 tasks: hashing, secure wiping, recovery of formatted drives, full/partial / logical/physical imaging, and document each step.
- **FTK tool kit:** Investigation procedure.
- **Windows & Mac:** Forensic Investigation
- **Reporting:** Prepare detailed forensic reports using Autopsy and FTK Toolkit with clear findings, methodology, and exhibits.

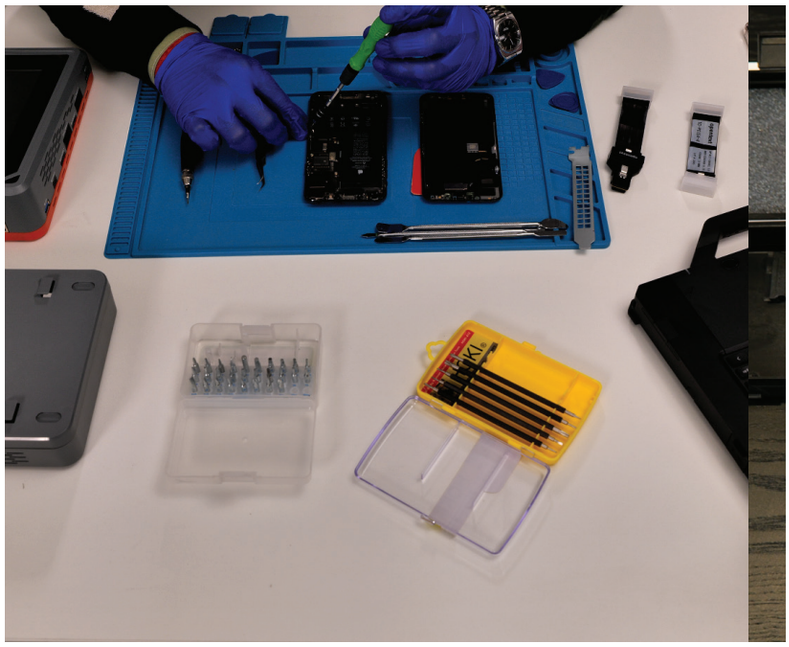
Programme Details

- Duration: 1 Months.
- Mode: Offline (Hands-on Lab training).

Advance Training Certification in

ADVANCE TRAINING CERTIFICATION IN MOBILE FORENSIC INVESTIGATION

Our course, Advance Training Certification in Mobile Forensic Investigation, is designed to equip participants with comprehensive skills in mobile device forensics and in identifying Indicators of Compromise (IoCs). The course covers foundational mobile architecture, acquisition techniques, Investigation methodologies, artifact analysis, and advanced threat detection methods. Learners will explore forensic methodologies for Android, iOS, smartwatches, and encrypted apps, and gain hands-on experience with tools such as FTK, Tableau TX1, iMazing, iConsole, Activity Monitor, and Oxygen Forensic Detective. Topics include network and email forensics, malware behaviour, cloud investigations, and mobile threat landscapes. The program culminates with a capstone case and a mock courtroom presentation to simulate real-world investigation and reporting.



Topics covered

- Introduction to Mobile Platforms (Android & iOS) and Device Architecture
- Mobile Forensics Fundamentals, Evidence Handling & Hashing Techniques
- Laws related to mobile forensics
- Mobile Chipsets, Boot Process, File Access & OS Security Features
- Data Acquisition Techniques: Logical, File System & Physical Extraction
- Hands-on Extraction on Oxygen Detective.
- Hands-on FTK and its use in mobile forensics
- Forensic Analysis using Oxygen Forensic Detective (OFD)
- Rooting, Jailbreaking, Device Modes (ADB, DFU, Recovery, EDL)
- Smartwatch Forensics and Artifact Extraction
- Geolocation Forensics: GPS, EXIF Data, KML Plotting with QGIS
- Indicators of Compromise (IoCs): Types, Detection & Forensic Relevance
- Mobile Threat Landscape, Attacks, IMSI/TMSI Analysis & Rogue Towers
- Threat Hunting using FTK, VirusTotal, and YARA
- Objective-based mobile phone investigation.
- WhatsApp, FaceTime, Telegram, call history extraction and reconstruction.
- IOC Correlation & Reporting Best Practices
- Network Forensics: C2 Traffic, DNS Tunnelling, Proxy/VPN Artifacts
- Encrypted Traffic, Beaconing & Anomaly Detection
- Email Forensics: Protocols, Header Analysis, System & Application Logs
- Advanced Detection Techniques: Malware, Lateral Movement, Privilege Escalation
- Use of iMazing, iConsole, IDS/IPS & Thermal Imaging in Forensics
- Cloud Artifact Investigation (Google/iCloud), Token-Based Access
- End-to-End Investigation, Report Submission & Mock Courtroom Presentation

Programme Details

- Duration: 1 Months.
- Mode: Offline (Hands-on Lab training).

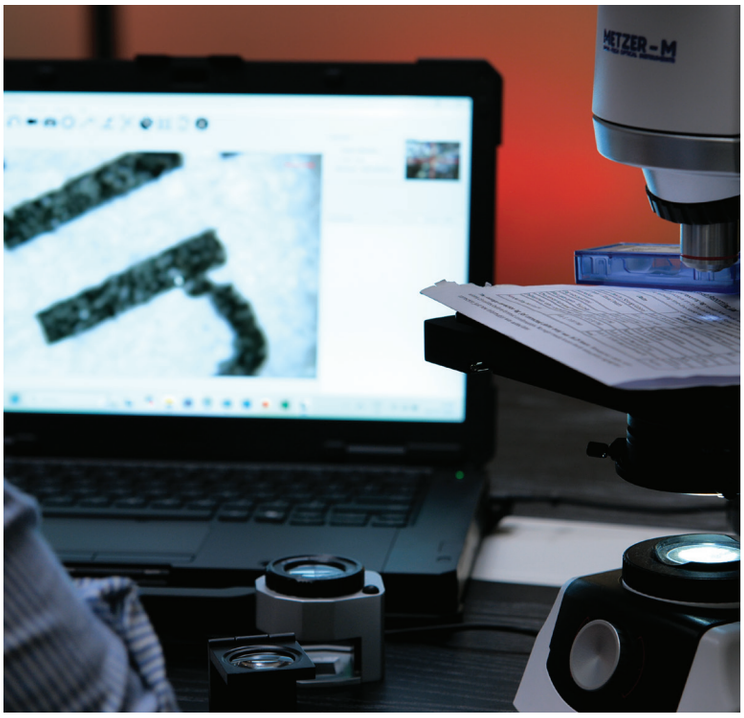
Hands-on Training

- Learn to disassemble mobile devices and identify key internal components.
- Practice securing electronic evidence using Faraday bags.
- Perform cryptographic hashing (MD5, SHA1, SHA256) to ensure data integrity.
- Acquire data from SD cards and USB drives using Tableau TX1 forensic imager.
- Verify image integrity using hash comparison.
- Practice data wiping procedures and understand their forensic implications.
- Conduct logical and physical acquisition using Oxygen forensic detective.
- Live demo of Oxygen Forensic Detective (OFD) and explore supported data extraction.
- Gain hands-on experience with rooting (Android) and jailbreaking (iOS) devices.
- Work with device modes such as ADB, DFU, Recovery, and EDL for data access.
- Extract GPS/EXIF geolocation metadata and visualize it using Google Earth and QGIS.
- Use VirusTotal and YARA rules to validate malware indicators.
- Practice correlating indicators across tools and documenting findings using standardized formats.
- Analyze network traffic for indicators of C2 communication, DNS tunneling, and VPN/proxy artifacts.
- Data packet analysis.
- Conduct system-level and application-level analysis to uncover signs of compromise.
- Detect advanced signs of compromise like lateral movement and privilege escalation.
- Use tools like iMazing, Activity Monitor, and iConsole for in-depth iOS analysis.
- Explore the use of IDS/IPS in mobile environments.
- Perform thermal diagnostics using Thermal Imaging Cameras.
- Extract and investigate cloud artifacts using token-based access for Google and iCloud accounts.
- Complete a real-world case simulation with a test device/image containing hidden evidence.
- Acquire, validate, and analyse data using TX1, Oxygen Forensic Detective, FTK, and Autopsy.
- Identify Indicators of Compromise and document findings in a comprehensive forensic report.
- Legal framework in the mobile forensic domain in India.
- Complete a capstone investigation project with evidence acquisition, analysis, reporting, and a mock courtroom presentatio.

Advance Training Certification in

ADVANCE TRAINING CERTIFICATION IN QUESTIONED DOCUMENT EXAMINATION

Our course, Advance Training Certification in Questioned Document Examination, provides an in-depth understanding of the scientific methods used in the examination and analysis of questioned documents. It covers handwriting and signature verification, detection of forgeries, alterations, and counterfeiting, along with the instrumental and microscopic analysis of inks, papers, and printed materials. Learners gain practical exposure to advanced forensic tools such as UV–IR examination systems, stereomicroscopes, and compound microscopes, and VSC. The course emphasises analytical precision, legal relevance, and report formulation to prepare students for professional roles in forensic laboratories and investigative agencies.



Topics covered

- Introduction to questioned documents – its legal importance
- Workflow and protocol followed in laboratories
- Class, characteristics, natural variations, and factors affecting handwritten documents.
- Digital camera – introduction, parts, working and applications in forensics
- Stereomicroscope – introduction, parts, working and applications in forensic analysis
- Compound microscope – introduction, parts, working and application in forensic.
- Electrostatic detection apparatus – introduction, parts, working and application
- VSC – introduction, parts, working, and applications.
- Document Alteration Detection- Mechanical/ Chemical Erasure methods and Addition identification, detection, and analysis
- Charred, printed, and photocopied documents – introduction, preservation, reconstruction, and recovery techniques
- Types of printers, ink, and printing methodologies to identify printers.
- Fiber analysis of printed/photocopied documents – types of paper used in printing and photocopying, procedure of making paper, fiber patterns, analysis procedure
- Font analysis of printed/photocopied documents - parameters for analysis
- Indentation Examination in Questioned Documents
- Security features - bank notes, cheques, passport, PAN card, Aadhar card
- Forensic Comparison and Analysis of Digitally Captured Signatures and Handwriting
- Digital documents – PDF basic structure and architecture
- Fundamentals of Kali-Linux
- Use of amped authentication in questioned documents
- Legal laws associated with documents and digital records
- Legal report making

Hands-on Training

- Identifying and categorizing the class and individual characteristics of an individual based on his handwriting
- Detection of forged signatures through analysis and forensic examination of handwriting characteristics and stroke patterns
- Examination and identification of disguised handwriting through analysis of writing habits and intentional alterations
- Identification and classification of various types of handwriting forgeries, including traced, simulated, and freehand forgeries
- Analysis of class and individual characteristics in printed and photocopied documents for source determination and authenticity verification
- Toner analysis for differentiation of printed documents and determination of printing technology or source
- Fiber analysis of paper materials to determine origin, composition, and authenticity of questioned documents
- Detection and decipherment of obliterated writings using advanced forensic techniques such as infrared and ultraviolet examination
- Identification of multiple inks through visual and instrumental methods (UV–IR, compound and stereo microscopy) to distinguish ink types and sequence of entries
- Examination and decipherment of Indented writing using Oblique lighting of Alternate Light Sources.
- Forensic Comparison and Analysis of Digitally Captured Signatures and Handwriting
  - » Questioned Digitally captured signatures/ handwriting Vs Digitally captured signatures/ handwriting Reference
  - » Questioned Digitally captured signatures/ handwriting Vs Conventional Document Reference
  - » Questioned Conventional Document Vs Digitally captured signatures/handwriting Reference
- Examination of security features in identity and financial instruments to detect counterfeits and alterations:
  - » Bank notes - validation of watermarks, security threads, holograms, microtext, and intaglio printing
  - » Cheques - verification of cheque-paper, security fibres, MICR line, and anti-tamper features
  - » Passport - inspection of laminates, UV-reactive elements, MRZ data, and polycarbonate security features
  - » Aadhar card - checking holograms, QR code integrity, and print substrate for authenticity
  - » Pan card - verification of printed security elements, lamination, and card stock characteristics
  - » Credit cards - an assessment of embossing, magnetic stripe/chip data integrity, and tamper signs
- Operation of a digital camera for forensic documentation: correct settings, evidence photography standards, scale and lighting control, and chain-of-custody imaging
- Use of a stereo microscope for low-magnification examination of documents, inks, fibres, and surface features
- Operation of a compound microscope for high-magnification analysis of inks, paper fibres, and microscopic trace evidence
- Installing and downloading Kali Linux and analyzing an evidence file in Kali Linux.
- Detection and verification of PDF tampering and manipulation, using metadata analysis, file structure inspection, and forensic tools to identify edits, redactions, and forged contents

Programme Details

- Duration: 1 Months.
- Mode: Offline (Hands-on Lab training).

Advance Training Certification in

ADVANCE TRAINING CERTIFICATION IN MULTIMEDIA FORENSICS

In a digital era where pixels and sound waves serve as the primary records of truth, Multimedia Forensics stands as the vanguard of modern investigation. As digital manipulation becomes increasingly sophisticated, the ability to distinguish authentic data from fabricated content is critical to the integrity of the justice system.

This certification program empowers participants to master the rigorous science of extracting, authenticating, and enhancing digital evidence with surgical precision. Through a deep dive into the technical architecture of images, audio, and video, you will learn to uncover hidden patterns, verify origins, and transform raw data into scientifically validated evidence suitable for the highest levels of legal scrutiny.

Topics covered

- Detailed study of multimedia files, including Audio, Video, Photo, and their properties, including sampling rates, bit depth, and the structural differences between various file containers and compression codecs.
- Implementation of the chain of custody and cryptographic hashing, with a primary focus on SHA-1 for legal compliance and SHA-256 for cross-validation.
- Hands-on acquisition and bit-for-bit imaging of source media using professional hardware and software like Tableau TX1 and FTK Imager.
- Advanced extraction of forensic artifacts from encrypted mobile applications and mobile devices using Oxygen Forensic Detective.
- Extraction and mapping of metadata, including EXIF and GPS coordinates, to establish the time and location of a captured file.
- Manual hex analysis of file headers and footers to detect hidden file types, masking, or manual splicing.
- Application of scientific enhancement workflows to stabilize shaky footage and correct lens distortions from wide-angle CCTV cameras.
- Utilization of super-resolution and frame averaging to reduce sensor noise and reveal critical details like license plates or faces.
- Detection of video tampering, including frame duplication or deletion, through frame-by-frame analysis, motion vector analysis, Group of Pictures (GOP) analysis, etc.
- Synchronising multiple video feeds for chronological event reconstruction and timeline-based analysis.
- Authentication techniques to identify image cloning, retouching, and manipulations.
- Implementation of Error Level Analysis (ELA) and quantisation table inspection to detect inconsistencies caused by double compression.
- Scientific linking of a questioned image to a specific physical camera sensor using PRNU “fingerprint” analysis.
- Analysis of JPEG Huffman tables and quantization data to identify if an image has been edited and resaved.
- Forensic cleaning of background environmental noise and electrical hums to clarify vocal signals while maintaining evidentiary integrity.
- Detection of splicing or manipulation in audio files.
- Phonetic and biometric analysis of voice samples, measuring pitch and formant patterns to verify speaker identity.
- Advanced signal processing and spectrum analysis to compare suspect voice samples against evidentiary recordings using biometric markers.

Programme Details

- Duration: 1 Months.
- Mode: Offline (Hands-on Lab training).

Hands-on Training

1. Evidence Acquisition and Integrity
    - Execute bit-stream imaging and physical block-level acquisition using Tableau TX1 to ensure 1:1 forensic copy without metadata alteration.
    - Perform logical and physical extractions via Oxygen Forensic Detective to recover multimedia artifacts and deleted fragments from encrypted applications.
    - Master the generation and verification of SHA-1 hash values to maintain a legally defensible chain of custody for all digital evidence.
2. Multimedia Authentication
    - Use HxD Hex Editor for manual signature analysis and ExifTool for deep extraction of metadata timestamps to detect file-type masking or temporal manipulation.
    - Detect pixel-level tampering and cloning in Amped Authenticate using Error Level Analysis (ELA) to identify inconsistencies in compression.
    - Utilize Amped FIVE and VideoCleaner to analyze GOP (Group of Pictures) structures and frame rates to detect frame duplication, deletion, or insertion.
3. Multimedia Enhancement
    - Execute non-destructive video stabilization, motion deblurring, and perspective correction in Amped FIVE while maintaining a scientific log for reproducibility.
    - Leverage Final Cut Pro for comparative visual editing and high-fidelity restoration of low-quality forensic footage.
    - Implement spectral subtraction and advanced signal processing in Audacity and Logic Pro to clarify weak vocal signals and reduce environmental noise.
4. Speaker Identification
    - Perform waveform and spectrographic analysis in Praat to identify background discontinuities or hidden edits in audio recordings.
    - Conduct forensic phonetic analysis by tracking Formants (, ,), pitch, and fundamental frequency to verify identities through biometric markers.
5. Source Identification
    - Scientifically link a questioned image to a specific physical camera sensor using PRNU (Photo Response Non-Uniformity) fingerprinting.
    - Analyze JPEG Quantization and Huffman tables to identify the specific software or device settings used during the creation of a file.
6. Reporting & Mock Court
    - Compile all technical findings into a legally defensible forensic report strictly aligned with the Bharatiya Sakshya Adhiniyam (BSA) 2023.
    - Present findings in a mock courtroom scenario to practice defending scientific methodologies and expert opinions under cross-examination.

Advance Training Certification in

ADVANCE TRAINING CERTIFICATION IN TECHNICAL SURVEILLANCE COUNTER MEASURES (TSCM)

This course focuses on the principles and practices of detecting, locating, and neutralising electronic surveillance threats. It provides hands-on training in identifying hidden audio, video, GPS, and data transmission devices through advanced TSCM equipment such as spectrum analysers, non-linear junction detectors, RF scanners, and thermal imagers. Learners develop the ability to conduct technical sweeps, analyse radio frequency environments, and secure communication channels against espionage and data leaks. The program bridges theoretical knowledge with field applications, preparing professionals for operational roles in security agencies, corporate intelligence, and counter-espionage units.

Topics covered

- Introduction to TSCM and its importance
- Role of forensics in TSCM
- Difference between cybersecurity and TSCM
- Categorization of surveillance threats
- Types of surveillance devices used in audio transmission, video transmission, location and GPS tracking, telephone and communication, cyber and electronic
- Types of bugs
- Surveillance detection theories
- Principles and tools used in TSCM
- Non-linear junction detector – fundamentals, parts, working, applications
- Radio frequency and Cellular Signals
- Mobility enhancer spectrum analyzer – fundamentals, parts, working and applications
- Thermal imager – parts, working and applications
- Inspection protocol and procedure
- Roles and responsibilities of the Searching Authority
- Relevant Laws and Procedures to Crime Scene Management and Surveillance Devices.
- Crime Scene Photography and Sketching
- Crime scene searching methods of investigation
- Vehicle sweep procedure
- Electronic Evidence Seizure, Packaging and Transportation Protocols
- Guidelines and ethical boundaries in TSCM
- Legal report making and formation

Programme Details

- Duration: 1 Months.
- Mode: Offline (Hands-on Lab training).

Hands-on Training

1. **Working and procedural understanding of non-linear junction detectors**
   - Detection of hidden semiconductors through harmonic signals
   - Any hidden physical device transmitter
   - Localisation of real electronic circuits and hardware embedded within walls, furniture, or vehicles
   - Identification of concealed transmitters, microphones, GPS trackers, and data-collection devices
2. **Principle working and searching procedure using spectrum analyzers**
   - Working principles of spectrum analysers, including frequency range, resolution bandwidth, and signal amplitude interpretation
   - Detection of transient, continuous, and burst RF signals used in covert communications
   - Signal characterization and demodulation to differentiate between legitimate and malicious transmissions
   - Waterfall analysis techniques for tracking intermittent or frequency-hopping signals
   - Integration of spectrum analysers with other TSCM tools like directional antennas, MCP probes, and RF detectors for precise localization of threats
3. **Fundamental usage procedure of thermal imagers**
   - Detection of concealed devices, such as transmitters, cameras, and GPS trackers, based on emitted heat patterns
   - Identification of live electrical or electronic circuits, recently operated systems, and powered-on components behind walls, furniture, or vehicles
   - Working principles of thermal imaging technology, including infrared radiation detection and image interpretation
4. **Inspection Protocol & Legal Framework**
   - Crime Scene Sketching and High-Resolution Photography to record scene overview and device locations in situ before retrieval.
   - Understanding DPDP Act, Bharatiya Sakshya Adhiniyam (BSA), IT Act and other Indian Laws to ensure technical sweeps respect privacy laws and government mandates.
   - Ensuring all findings and Evidence Handling Protocols to ensure evidence integrity and admissibility in the court of law.
5. **Roles & Responsibilities of the Searching Authority**
   - Establishing a “sterile” perimeter and controlling access to prevent the remote triggering or removal of hidden devices.
   - Maintaining a rigorous audit trail from the moment of detection through specialised seizure and forensic laboratory submission.
   - Generating comprehensive forensic reports that detail the methodology, device functionality, and identified security breaches.

Advance Training Certification in

ADVANCE TRAINING CERTIFICATION IN FORENSIC JOURNALISM

This course provides an in-depth understanding of the principles and practices of Forensic Journalism, focusing on the integration of investigative reporting with forensic science. It covers evidence-based news investigation, digital and data verification, forensic interviewing, and the analysis of crime, corruption, and misinformation. Learners gain practical exposure to investigative tools and digital forensic techniques used in uncovering and authenticating information. The course emphasises accuracy, ethical integrity, and legal compliance, preparing students for professional roles in investigative journalism, media analysis, and forensic communication.

Programme Details

- Duration: 1 Months.
- Mode: Offline (Hands-on Lab training).

Topics covered

- Introduction to forensic journalism and its aspects
- Crime Scene Management- procedures involved in crime scene investigation and management, Reconstruction of crime scene.
- Role of questioned documents in media – introduction, alterations, indentations, psychological profiling of author through different parameters of handwriting (linguistic, text, document, emotional)
- Cyber forensics in journalism – network traffic analysis, log files and stamps, user account activity, e-mail header analysis, cache, file metadata, social media activities, communication patterns and VPN logs, malware artifacts.
- Physical Forensic – Introduction, projectile: its direction and determination, impact patterns, glass fractures (radial, concentric), different tool marks, skid and tyre marks: their examination, analysis of bloodstain patterns (diameter, angle, directionality), fire patterns (origin and lightning conditions)
- Forensic chemistry and media - introduction, usage of odour and smell, colour changes, livor mortis and marbling of body, changes in body colour with time, staining and discolouration of materials (blood, seminal fluid, saliva, steel component), analysis of powder and crystals, analysis of obliterated marks and their restorations, fumes and vapours, analysis of unusual residue on objects, examination of packaging materials
- Forensic biology and medicine - introduction, analysis of bloodstains, examination of hair, bodily fluids, types of injuries, physical injuries (abrasions, contusions, lacerations), examination of the victim's procedure, evidence in sexual assault cases, analysis of ligature marks
- Forensic taphonomy – study of post-mortem changes (immediate, early and late changes)
- Forensic psychology – introduction, importance in criminal investigations, behavioral analysis (ritual and signature), evaluation of victim and witness statements, communication style interpretation, staging and manipulation analysis, geographical profile analysis, victimology, psychological autopsy, criminal profiling, eyewitness memory and identification, psychological assessment of suspect, interrogation and interviewing techniques, criminal competency and insanity

Hands-on Training

- Forensic-mock reporting
- Dummy crime scene reconstruction and reporting
- Practical application of forensic skill on forensic journalist reporting
- Application of observational methods of forensics in mock cases
- Application of forensic psychology on journalist interviews
- Application of questioned document forensics on document-based reporting
- Application of victimology in media reporting
- Studying and interpreting fractures formed in glasses
- Identification, analysis, and examination of tool marks to determine the type of instrument used, its unique characteristics, and possible linkage to the crime or suspect
- Examination and analysis of bloodstains to determine, pattern, and distribution for reconstructing crime scene events
- Practical examination and analysis of skid and tyre marks to determine vehicle speed, direction, braking/acceleration events, and aid in collision reconstruction through measurement and pattern comparison
- Microscopic and comparative analysis of hair evidence for species identification, root and cuticle morphology, treatment/damage assessment, and trace-evidence testing
- Analysis of email headers to identify the origin, transmission route, and authenticity of electronic communications
- File metadata analysis to extract creation/modification timestamps, authorship, and system traces
- Cache examination to recover transient data, deleted content, and browser artifacts
- Social media activity forensic review to collect posts, message metadata, geolocation, and interaction patterns

Laxhar Institute of Forensic Excellence

A Knowledge initiative of Laxhar Evidence Labs Pvt. Ltd.

A-525 & 527, Anthurium Tower, Sector-73, Noida, UP. 201301

+91 88007 92002 support@laxhar.com

www.laxhar.com **CIN:** U80300UP2024PTC214190

Follow us: