BUREAU OF POLICE RESEARCH & DEVELOPMENT

Modernization Division

NATIONAL CYBER RESEARCH AND INNOVATION CENTRE

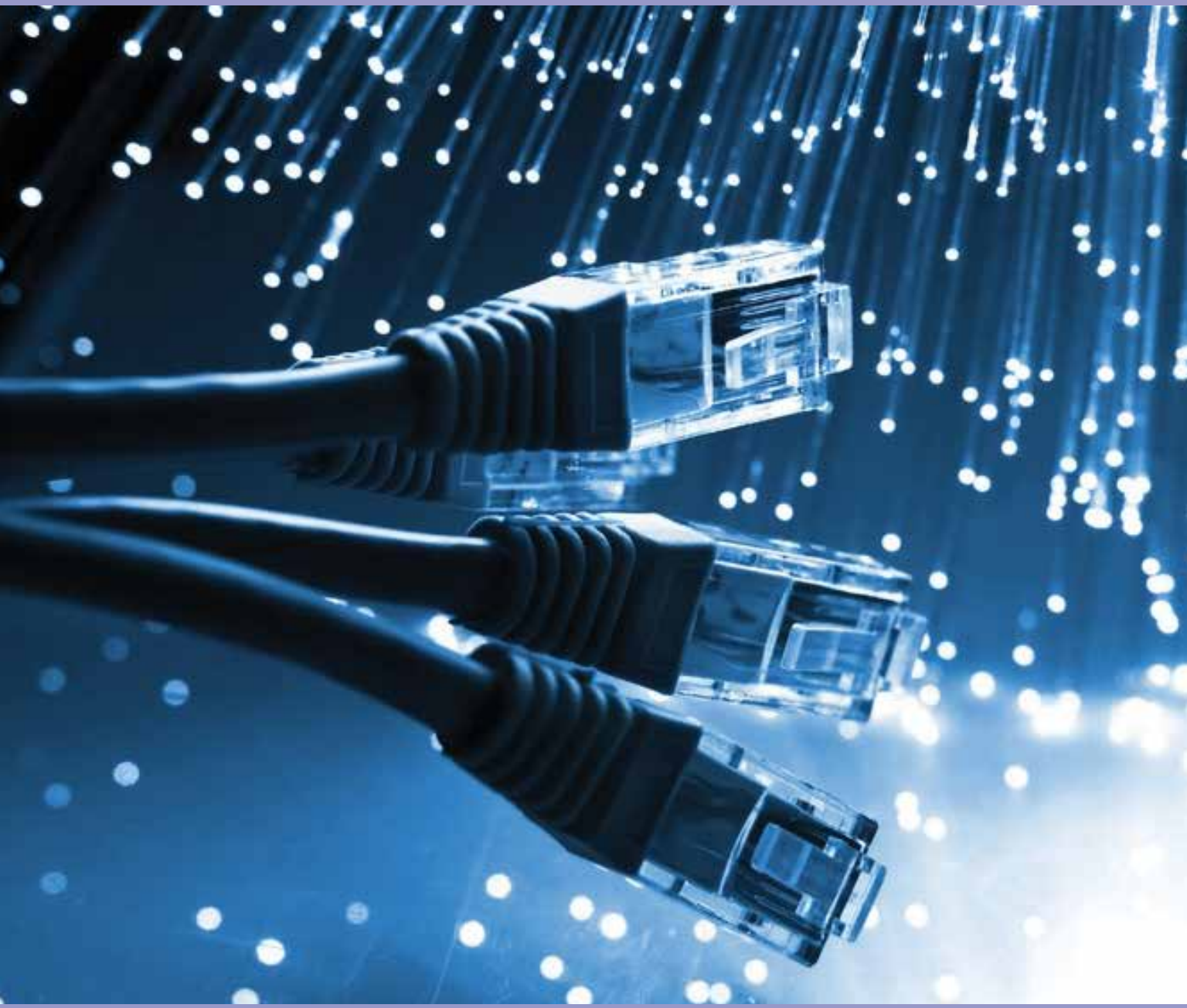
Training Curriculum- Cyber Crime Investigation & Digital Forensics

MODULE - I

Basic Course

(One Week)

INVESTIGATION OF CYBER CRIME CASES



1 UNDERSTANDING OF COMPUTER SYSTEMS – LAW ENFORCEMENT AGENCY (LEA) PERSPECTIVE

- Classification of computers and their features. Specifications of various computer generations and various functionalities of computers - data processing and storage.
- How computer systems process instructions.
- Various parts of a computer.
- Computer softwares - system software, application software, operating systems.
- Basic operations of a computer system :
  - Computer hardware - input & output devices.
  - Binary and hexadecimal representation of data.
- Memory devices and storage mechanism.
- Volatile and non-volatile memories.
- How data is written on and retrieved from the Hard Disk Drive (HDD).
- Formatting of HDD – New Technology File System, File Allocation Table, Extended File System, Hierarchical File System.
- Various hardware components and their uses.
- Introduction to types of computing devices – desktops, laptops, MacBook, iMac, all in one Computers, tablets, wearable devices (smart watches, smart bands).
- Different operating systems and their relevance to law enforcement officers.
- Introduction to system and application software.
- Demonstration of disassembling a computer and showing various components and peripherals.
- Types of data storage – primary and, secondary (internal and external storage devices).
- Types of storage device technologies – magnetic tapes, flash (semiconductor memories), difference between mobile phone storage and computer storage etc.
- HDD overview – physical and logical structure.
- Types of HDD interfaces – Serial Advanced Technology Attachment,

Integrated Development Environment, Small Computer System Interface Solid State Disks etc.

- Parts of HDD–spindle, disk.
- Structure of HDD – sector, track, cluster size etc.
- HDD data addressing, metadata, disk capacity, calculation and measuring performance of HDD.
- Partitioning and formatting of HDD – low level and high level formatting.
- Boot process – Master Boot Record of different operating systems, file systems, understanding file system, shared disk file systems, special purpose file systems, etc.
- CD-ROM/DVD file systems – Compact Disc File System, ISO, Joliet, and Universal Disk File Format.

2 UNDERSTANDING OF COMPUTER NETWORK AND ITS IMPORTANCE IN INVESTIGATION

- Fundamentals of computer networking and its needs.
- Different types of computer network.
- Standalone vs network systems.
- Client vs server systems.
- Bluetooth technology, Wi-Fi technology, wireless fidelity, WiMAX technology.
- Home Area Network (HAN), Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area network (MAN), Wide Area network (WAN), Near Field Communication (NFC).
- Network architecture and topologies.
- Local Area Network vs. Virtual Local Area Network.
- Internet service providers and their roles in the network.
- How internet works, Internet Protocol (IP) addresses, Domain Name System (DNS), country list, components of the internet (world wide web, email,File Transfer Protocol (FTP), Instant messaging, social networking), web browsers and servers, search engines.
- Networking devices – firewalls, hubs, bridges, switches, routers, intrusion detection systems and intrusion prevention systems etc.
- Concept of physical addressing system.

- Identification of MAC addresses.
- Concept of logical addressing system
- Introduction to Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP).
- Types of IP addresses – static, dynamic, public and private.
- Concept of IP address assignment – Dynamic Host Configuration Protocol, Static and Dynamic IP Address.
- Types of IP address versions - IPV4, IPV6 and differences between them.
- Intranet vs Internet vs Extranet.
- Introduction to Network Address Translation (NAT).
- Concept of website, DNS and Uniform Resource Locators (URLs).
- Identification of IP address of a user device or website.
- Proxy Network vs Virtual Private Network (VPN).

3 INTRODUCTION TO CYBER CRIMES AND CYBER CRIMES INVESTIGATION

- Understanding cyber-crime.
- Cyber crime - scope, characteristics and landscape over the years and current trends in cyber space.
- Development of cyber crime.
- Classification of cyber crime.
- Cyber criminals – individual criminals / organized criminals / sponsored criminals / hired criminals.
- Various types of cyber crimes and understanding their modus operandi for predictive policing.
- Challenges in investigations.
- Countering cyber crimes and best practices for the same.
- Investigation of the most common cyber crimes reported to LEAs.
- Emerging trends in cyber crime.
- Do's and Dont's while investigating cyber crime complaints.
- Difference between investigation of traditional crime and cyber crime.
- Common mistakes committed by Investigating Officers (crime scene, search and seizure, transportation, labeling.

- Documentation and its importance – incorrect entries in seizure memo, irregularities in seizure memo, irrelevant or vague questions in forwarding note to Forensic Science Laboratory.

4 CALL BASED CRIMES INVESTIGATION USING CDR AND TDR ANALYSIS BY EXCEL/SPREAD SHEETS

- Introduction to various types of calls eg. PSTN calls
- Mobile phone CDR analysis - (concepts & demo using MS Excel)
- Basics of CDR
- Understanding of CDR columns (called number, calling number, cell IDs, IMSI, IMEI etc.)
- Basics of MS Excel filter, sorting, advanced filter
- Things to be looked into for CDR analysis in investigation and detection of crimes.
- How to find out frequently dialed and received call numbers.
- Tools used for analysis of CDR
- Checklist for ideal analysis of CDR
- BTS cell sites dump and its significance and analysis
- Evidentiary value of CDR analysis and processing citing such evidences during case trial & its admissibility
- Tower dump analysis
- Basic concept of BTS cell sites
- Finding out the cell ID of 2G/3G/4G towers
- Collection of data's from different service provider
- Things to be looked in to for Tower dump analysis in investigation and detection of crimes
- Introduction to investigation of calls – PSTN calls, No number calls, below 10 digit calls, above 10 digit calls, same number or dual victim calls
- Introduction to call detail record (CDR)
- Types of CDRs
- Requesting a CDR / TDR
- Responsibilities of intermediaries
- CDR analysis using Excel
- TDR analysis using Excel
- Guidelines of DOT / TRAI / TERM

5 INTRODUCTION TO DIGITAL EVIDENCE AND FORENSIC TECHNOLOGIES WITH BEST PRACTICES

- Digital evidence – definition, characteristics, types, source of digital evidence etc.
- Classification of digital evidence – user created, user protected and system created.
- Difference between volatile and non-volatile memory.
- Rules of evidence – best evidence rule, hearsay evidence etc.
- Traditional forensic evidence vs digital evidence.
- Cyber forensics – definition, classification.
- Cyber forensics v/s traditional forensics – Locard's exchange principle, Daubert's rule, repeatability and reproducibility, peer review techniques.
- Doctrine of evidence gathering.
- Understand pre-requisite for search & seizure and first responder kits.
- Basic do's and don'ts during search.
- Identifying and securing the crime scene.
- Documentation of scene of crime including initial documentation of scene.
- Collection of evidence from switched off system.
- Collection of evidence of live system.
- Collection of evidence from mobile phones.
- Use of Faraday bag.
- Forensic duplication.
- Conducting interviews.
- Seizure memo and seizure proceedings.
- Maintain chain of custody.
- Model digital evidence collection form.
- Handling, labelling, packaging transportation and storage of digital evidence.
- Best practices for seizure of electronic evidences.
- Introduction to forensic tools, techniques and technology. Discussion on its application

to computer systems, network, communication devices, volatile memory, storage systems, internet data, cloud, Supervisory Control and Data Acquisition (SCADA) systems and databases.

- Authentication of data in storage device including hands on hashing techniques and tools.
- Integration and authentication of various storage devices.
- Concept of hashing and hash value - use of write blockers for authentication of data (Demo).
- How to collect evidence from various repositories and develop hash value using authentic free ware.
- Anti-forensics - data hiding techniques.
- Doctrine of evidence gathering.
- Understanding pre-requisite for search & seizure and first responder kits.
- Basic do's and don'ts during search.
- Identifying and securing the crime scene.
- Documentation of scene of crime including initial documentation of scene hashing – importance, process, algorithm and tools.
- Best practices – ACPO, Interpol, STCIA, DOJ guidelines and best practices in Indian environment.
- Responsive toolkit – preparation, portable software tools, validation of tools and things to carry.
- Cyber forensics process – Identify, preview, acquire, authenticate, analyze and document.
- Areas to search – active files, deleted files, slack space, unallocated space, hibernation file, page file, metadata and registry etc.
- Steps in crime scene investigation – securing crime scene, interviews, shutdown process, collecting evidence, packaging and transportation.
- Process model – triage process, dual process model and its utility.
- Collection of important data – tools and techniques for collecting volatile data from RAM from a live system.
- Introduction to digital signatures, understanding how digital signature work and various techniques to combat crimes related to fraudulent digital signatures.
- Smart card devices (RFID / QR Codes / barcode scanner code).

- Imaging the drive at scene of crime using various tools and techniques – Use of write blocker devices, imaging, cloning, hashing, authentication of evidence, CRC, tools for hashing.
- Volatile data capture and analysis – capturing system information and network information.
- Packaging, transportation and preservation of data.
- Documentation – seizure memo, chain of custody, forwarding note to FSL, 65 B, etc.

6 INTRODUCTION TO MOBILE DEVICES – MOBILE DEVICE AS EVIDENCE

- Basics of mobile phone & communications: types of cellular networks (CDMA / GSM).
- Introduction to different mobile devices, hardware and software characteristics of mobile devices.
- Mobile operating systems (MOS): classification of MOS (WebOS, Symbian OS, Android OS, RIM, BlackBerry OS, Windows Phone 7, Apple iOS).
- Difference between Desktop Operating System (DOS) and MOS.
- Mobile Forensics - Definition.
  - Information available in mobile phones, memory considerations in mobiles.
  - Subscriber Identity Module (SIM), SIM File System.
  - Integrated Circuit Card Identification (ICCID) and International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI) and Electronic Serial Number (ESN).
  - Difference between mobile forensics and computer forensics.
- Identification and isolation of mobile devices. Search and seizure of mobile devices and acquisition methods (physical, logical, file system, JTAG, Chip off).
- Analysis of mobile images, understanding a mobile forensic report.
- SIM & SIM-less devices.

7 UNDERSTANDING OF WEBSITE WORKING PROCEDURE AND WEBSITE BASED CRIMES AND ITS INVESTIGATIONS

- Introduction to websites & social media websites (working procedure of protocols and functions).
- Handling complaints related to website crimes.
- Identifying a fake website.
- Identification of IP address of the website.
- Gathering information related to a website ownership.
- Collection of evidence (live, archival).
- Website defacement investigation.
- IPR Infringement Issues.
- Responsibilities of intermediaries.
- Acquaints website investigation.
- Deleted website investigation.
- Website specific content removal.
- Web attack investigation.
- Data and document forgery.
- Notice process to over the top – OTTs (WSP-ESP-instant message applications)- ISP-MSP (web service provider, email service provider, internet service provider, mobile service provider).
- Challenges involved - Proxy or VPN involvement in website investigation.
- Relevant sections of IT Act & IPC laws for FIR registration.
- SoPs for investigating website related crimes.

8 INTRODUCTION TO IT ACT AND IT ACT AMENDMENTS & INDIAN TELEGRAPH ACT

- Introduction to cyber crime and cyber law.
- Cyber space and information technology.

- Nature and scope of cybercrime and fundamentals on its jurisdiction.
- Cyber crimes and their respective sections.
- Overview of amended laws by the IT Act 2000: The Indian Penal Code (IPC) 1860, The Indian Evidence Act 1872, The Banker's book evidence Act 1891, The Reserve Bank of India Act 1934 and the Indian Telegraph Act 1885 and relevant case laws.
- Digital signature and certificate issues and their legal implications.
- Section 79, and the Government Examiner of Digital Evidence.
- Requirement of certification under different sections.
- Understanding the report given by cyber forensics.
- Relevant sections of the Indian Evidence Act.
- Admissibility of electronic evidences.
- Framing proper notice with clauses.
- IPC and cyber crime classifications.
- Code of Criminal Procedure 1973 – search and seizure provisions, examination of witnesses through audio and video by police.
- Section 46 the role of Adj. Officer - IT Act.
- Difference between 79 3B IT, 91 Cr.P.C and 149 Cr.P.C.
- Surveillance and interception of mobile and internet communications.
- Lawful interception and authorization – legal provisions as per Indian Telegraph Act Section 5(2) rules 419, 419A.
- Rules 69 of IT Act.
- Section 91 Cr.P.C.
- What is lawful interception.
- Procedure and documentation for legal interception.
- Liaising with the service providers for monitoring suspect activities.
- Contacting CERT.IN, MEITY, TERM, TRAI, ICANN/IANA etc.

9 COMMON CYBER CRIMES SCENARIO BASED EXERCISES (DEMO/HANDS-ON) EXAMPLE: LIVE WEBSITES, DELETED WEBSITES, DE-ACTIVE WEBSITE, AND DEFACED WEBSITE

10 PRE & POST COURSE ASSESSMENT

MODULE - II

Intermediate Course

(One Week)

INVESTIGATION OF CYBER CRIME CASES

Refresh session on topics covered in basic course and connectivity to intermediate course.

1 UNDERSTATING OF EMAIL & EMAIL ENABLED CRIMES AND ITS INVESTIGATION

- Working of email service.
- Types of email configurations – SMTP/ IMAP / POP protocols.
- Concept of tracing email related crimes.
- Extraction of email headers (brief and full header) and deriving vital information from the same.
- Steps to trace details from various email clients such as – Gmail, Rediffmail, Yahoomail, Hotmail, NIC mail etc. :
  - Finding full header of received mail
  - Finding sender email address (server IP).
  - Finder senders IP address.
  - Finding message ID.
  - Finding ISP of source IP Address including physical address of ISP.
- Email tracking via Rednotify/ Getnotify tools etc.
- Tracking of IP address using IPlogger/ Grabify techniques etc.
- Collection of evidences for tracing of admissible evidences from emails.
- Identifying malicious emails such as phishing email, malicious content mail and suspicious and harmful attachments in emails.
- Requesting details from intermediaries.
- Collection of email as an evidence – single email, multiple emails, entire mailbox etc.
- Collection of emails and other relevant data from various cloud services such as Google Takeout etc.
- Presentation of email details and the technical information from emails as an evidence in court.
- Restoring deleted emails from web and app.

- Challenges such as proxy and VPN.
- Regaining access to hacked email IDs.
- Email tracking through lawful interception under 91 Cr.P.C
- Lawful interception of emails.
- Tracing the email artifacts on drive / cloud storage.

2 FORENSIC IMAGING PROCEDURE & ANALYSIS OF HDD IMAGE.

- Practical scenarios on imaging & analysis of data using freewares.
- Concepts of sterile media and imaging.
- The significance of imaging of the drive.
- Forensic cleaning of media.
- Creating an image of the drive/media.
- Steps for imaging, cleaning and its documentation.
- Practical demonstration of imaging the media.
- Acquiring data from volatile memory and demonstration of relevant tools for the same.
- Practical demonstration of about medias.
- Imaging of a memory card/SIM card.
- Do's and Don'ts while imaging cell phone memory.
- Physical and logical mounting of files.
- Metadata analysis.
- File carving.
- File signature mismatch Analysis.
- Keyword searching and indexing of artefacts.
- Recovery of deleted data (within the slack, partition and unused memory).
- Registry analysis.
- Windows forensics and analysis of artefacts.
- Limitations of computer forensics.
- Generating reports on the findings.
- Windows forensic analysis - window artifacts, evidence volatility, system time, logged on user(s), open files, MRUs, network information, process information, service information, windows registry, startup tasks, memory dumping.

- Document forensics- PDF structure, PDF analysis, MS Office document structure and analysis, macros, Windows thumbnails, Android thumbnails.

3 INTRODUCTION TO INCIDENT RESPONSE, LIVE FORENSICS & ANALYSIS OF VOLATILE MEMORY

- Understanding volatile data.
- Traditional Forensics vs Live Forensics.
- The live response process and the best evidence rule.
- Differences between volatile data from various OS sources.
- Various destination options of the acquired data.
- Acquisition of network data.
- Attached devices.
- Integrity checks.
- Acquisition in a live environment.
- System impact.
- Procedure for acquiring physical memory data.
- API calls vs RAM acquisition.
- Challenges in acquiring data from RAM for the following OS (Windows/ Linux/Mac).
- Volatile data collection using APIs.
- Acquire volatile data.
- Best practices for imaging conditions in a live environment.
- Encrypted volumes.
- Dynamic disk imaging - RAID.
- Identifying passwords.
- Capturing recently visited URLs, bookmarks etc.
- Cached memory.
- Deriving relevant information from browsing history.
- Network information - collection of network logs from routers, and open WiFi / hotspots etc.

4 INTRODUCTION TO EMERGING TECHNOLOGY DRIVEN FORENSICS

- Emerging technologies and its impact on cyber crimes.
- Drones driven crimes and drone forensics.
- Smart vehicles and usage of vehicle forensics to derive potential evidences from the same.
- IOT Devices in smart cities - IOT forensics.
- Deep, dark-net crimes and crypto currency forensics.
- Cyber physical device forensics (Smart Devices like Apple Watch, Fitness Tracking Devices, Alexa, Siri, Google Asst etc.).
- Cloud network, servers at abroad & cloud forensics.

5 HANDLING CCTV RELATED CRIMES & ITS INVESTIGATION PROCEDURE

- What is CCTV & types of CCTV cameras.
- Handling complaints related to CCTV investigations.
- Step by step action guide on handling CCTV / DVR / NVR data.
- Search and seizure of CCTV / DVR / NVR data.
- Collection of evidence pertaining to CCTV/DVR/NVR data.
- Introduction to Chinese CCTV OS.
- Various challenges faced during investigation of CCTV footage.
- Documentation process of case diary, seizure memo, chain of custody, forwarding note to FSL and 65B certificate).

6 HANDLING ANTI-FORENSIC ENABLED MEDIA

- Handling of encrypted devices (file/ folder/drive) or enciphered data using decryption data.
- Handling of content/file hiding using steganography. Deciphering/ unhiding procedure.
- Detection of hidden Key loggers / Screen recorders applications from the suspect system.
- Recovery of deleted data from HDD/ multimedia cards including other storage devices. Demo recovery of deleted data from multimedia cards with using different tools.
- Wiping- how to recover formatted/ deleted/wiped data from suspect device.
- Anti-forensics – motivation, applications, outcomes.
- Introduction to malware analysis - cases related to ransomware, and other malware, APT, concept of IoCs, domain fast fluxing.

7 INTRODUCTION TO VOIP CALL CRIMES & INVESTIGATIONS USING IPDR ANALYSIS

- Introduction to VoIP calls.
- Introduction to investigation of calls –Web Calls, App Calls, Prank Calls.
- Concept of VOIP.
- Types of VOIP Services.
- Steps involved in tracing of VOIP calls.
- Tracing of fake phone call social engineering.
- Tracing of spoof/fake calls.
- VOIP Call Packet Analysis.
- Requesting a IPDR / IP (CDR) / GPRS Data.
- Tracking & tracing of suspect using IPDR analysis by Excel.
- Guidelines of DOT / TRAI / TERM.

8 GATHERING INFORMATION THROUGH CYBER SPACE USING (OSINT-SOCMINT-SIGINT)

- Gathering information of a user / organization using open space.
- Search operators.
- Google vs Bing.
- Carrot search.
- Image lookups.
- Information available on Government websites.
- Mobile number lookups.
- Mobile network information.
- Social media analytics for gathering of information about target suspect/ accused/offender by using crime input such as:
  - Name
  - Email ID
  - Photo
  - Video etc.,
- Introduction to cloud services.
- Cloud artifacts and their evidentiary value.

9 INTERNATIONAL IT LAWS AND THEIR PROCEDURES

- Mutual Legal Assistance Treaty, Letter Rogatory.
- Procedural aspects of law.
- Federal laws, GDPR, TRIPS and other global law practices related to IT Act.

10 SCENARIO BASED EXERCISES

11 PRE & POST ASSESSMENT

Note: Tools to be covered: Encase, UFED, FTK Imager, Magnet Acquire, Bulk Extractor, Volatility, Recon–ng and any other free / open source tools available.

MODULE - III

Advanced Course

(Two Weeks)

SOCIAL MEDIA AND OTHER DIGITAL TOOLS INVESTIGATION

1 INTRODUCTION TO SOCIAL MEDIA CRIMES & RELATED INVESTIGATIONS

Refresh session on topics covered in basic course and intermediate course and their connectivity to intermediate course.

2 FACEBOOK RELATED INVESTIGATIONS:

- Identity theft related cases.
- Different types of cyber crime associated (cyber stalking / bullying / harassment).
- Content investigation (obscenity / nudity / defamatory related cases).
- Content removal.
- FB live stream blocking methods.
- Accused character estimation through FB.
- Missing people/human trafficking surveillance in FB.
- FB posts share-tag-comment-like related offences.
- Facebook analytics.
- Downloading complete profile from Facebook.
- Facebook for law enforcements.
- Collection, preservation of digital evidences, presentation in the court of law.

3 TWITTER RELATED INVESTIGATIONS:

- Identity theft related cases.
- Types of associated cyber crimes (cyber stalking / bullying / harassment).
- Content investigation (obscenity / nudity / defamatory related cases).
- Content removal.
- Investigation on tweet, retweet, tags, Handlers.
- Twitter analytics.
- Web patrolling using Twitter.

- Downloading complete tweets from a profile, keyword etc.
- Sentiment analysis.
- Collection, preservation of digital evidences, presentation in the court of law.

4 INSTAGRAM RELATED INVESTIGATIONS:

- Identity theft related cases.
- Different types of cyber crime associated (cyber stalking / bullying / harassment).
- Content investigation (obscenity / nudity / defamatory related cases).
- Content removal.
- Downloading complete content.
- Instagram for law enforcement.
- Collection, preservation of digital evidences, presentation in the court of law.

5 LINKEDIN RELATED INVESTIGATIONS:

- Identity theft related cases.
- Cyber stalking / harassment.
- Content investigation.
- Content removal.
- Job frauds.
- Downloading complete user data.
- Collection, preservation of digital evidences, presentation in the court of law.

6 SNAPCHAT RELATED INVESTIGATIONS:

- Identity theft related cases.
- Cyber stalking / Cyber Bullying / Harassment.
- Content investigation (obscenity/ nudity / defamatory).
- Content removal.
- Downloading complete user data.
- Collection, preservation of digital evidence, presentation in the court of law.

7 YOUTUBE RELATED INVESTIGATIONS:

- Content investigation (obscenity / nudity / defamatory related cases).
- Copyright infringement related cases.
- YouTube Video content removal.
- Youtube tracing video uploaded user details.
- Youtube video comment analysis.
- Youtube video tracking through geo-location/geo-tagging.
- Collection, preservation of digital evidences, presentation in the court of law.

8 MATRIMONIAL / DATING / ADULTERY RELATED INVESTIGATIONS:

- Content investigation (obscenity/ nudity / defamatory).
- Tinder/Happn/Locanto/Tagged/ Escort service related apps & websites.
- Collection, preservation of digital evidence, presentation in the court of law.

9 OTHER SOCIAL MEDIA APPS / WEBSITES RELATED INVESTIGATIONS:

- Tiktok / Sharechat / Musically.
- Games related investigations – Blue Whale, PubG, Fortnite, MoMo Games.
- Advisory content for cyber safety awareness.

10 INVESTIGATION OF FIN-TECH RELATED CASES:

- Various kinds of Fin-Tech options available in India.
- Common misconceptions.
- Investigating e-wallets.
- Investigating ATM related frauds.
- Investigating OTP related frauds, NO OTP based frauds.
- OLX frauds.
- Skimming frauds.
- Link click based frauds.
- UPI based frauds.
- QR code driven frauds.
- Toll-free number based frauds.
- Bulk SMS based frauds.
- Investigating payment gateways.
- Investigating identity theft related cases.
- Database forensics.
- Job frauds, gambling, betting, financial transactions for illegal activities.
- Advanced - malware analysis - cases related to ransomware, and other malware(s).
- Investigation of software piracy cases - Intellectual Property Rights (IPRs)-
- Collection of information from complainant.
- Registration of FIR.
- Understanding modus operandi and technology involved.
- Tracking of criminal - collection of third party information.
- Search, seizure and collection of digital evidence.
- Document to be collected from banks.
- Request to FSL for report.
- Collection of third party information / certificates for proving the case.
- Guidelines to prepare charge sheet.

11 UNDERSTANDING OF LOCATION / CLOUD BASED INVESTIGATIONS(TRACKING & TRACING OF SUSPECT USING NAVIGATION DEVICES, WEBSITE/CLOUD DATA INPUTS)

- Introduction to location based services.
- Types of location based services.
- Triangulation and GPS techniques to pin point the actual location.
- Locating the suspect / accused / missing person based on mobile, internet communication including social media and tracing of missing / stolen mobile phones:
  - By using CDR and Cell ID.
  - By using Triangulation techniques.
  - By using WhatsApp, Facebook, Viber etc.
- Google dash board.
- Android device manager.
- By using GPS tagging on photographs.
- Tracing using Google Goggles.
- Tracing missing/stolen mobile by using MAC Number.
- Tracing missing/stolen mobile by using IMEI number.
- Gathering data created using various Google services
- Requesting details from Google via legal approach.
- Retrieval of data from Google / iCloud /Microsoft cloud services.
- Tracing missing/stolen mobile by using IMEI No.
- Tracing missing/stolen mobile by using MAC No.

12 INVESTIGATION OF WHATSAPP/TELEGRAM RELATED CASES

- Live WhatsApp / Telegram investigation-digital foot prints.
- Deleted WhatsApp/Telegram chat retrieving methods.
- WhatsApp-cloud chatting extraction methods.
- WhatsApp/Telegram image or video offences related investigation.

- Cyber harassment through WhatsApp/Telegram.
- Investigation on WhatsApp/Telegram groups.
- Monitoring of WhatsApp/Telegram groups through masking methods.
- How to request details from WhatsApp/Telegram via legal route.
- Originator of post (content, image, video).
- WhatsApp / Telegram call investigations (audio, video).
- Notice and responses under Section 91 of Cr.P.C & Mutual Legal Assistance Treaty (MLAT).

13 INTRODUCTION TO DARK WEB INVESTIGATIONS

- Introduction of Deep & Dark Net.
- Surface Internet vs Deep Internet.
- Indexed Website vs non Indexed Websites.
- Red Rooms, Galaxy, Hidden WIKI, Wiki leaks, Silk Road, Pandora other Onion links.
- Modus operandi of cyber-crimes committed using Dark Web.
- Working principle of Block Chain.
- Concepts of crypto currencies and mechanisms behind it.
- Wallet tracking, Public Key vs Private Key (in the context of crypto currencies).
- Introduction to track cryptocurrencies.
- Challenges in investigations.

14 CYBER TERRORISM THREAT GRAVITY ON REAL & DIGITAL WORD

- Cyber terrorism new paradigm.
- Misuse of internet by terrorists.
- Introduction to Botnet.
- Recruitment, spread of propaganda on internet.
- Phony websites & cyber herding.

- Web crawlers and use of data mining.
- Proactive measures to combat misuse of internet by terrorists.
- Cyber terrorism & international conventions.

15 NETWORK FORENSIC & INVESTIGATION ANALYSIS

- Network forensics basics.
- Strategies.
- Evidence gathering.
- Software-defined nets.
- Introduction to network protocols.
- Network evidence types and sources – switch, firewall, IDS / IPS, router.
- Network packet capture.
- Types of attacks.
- Web/host attacks.
- Routers/switches attacks.
- Device-based attacks.
- Network forensics tools.
- Wired/wireless access.
- Session reconstruction for protocols – TCP and HTTP.
- Log collection, aggregation, and analysis.
- Wireless packet analysis.
- Challenges - encoding, encryption, VPN.
- MITM - Man-In-The-Middle methods/ tools.
- Acquisition of data from running servers – accessing/preservation of data from routers/ Wi-Fi access points – hacking.
- Gather information from server.
- Secure Wi-Fi or routers from UN-authorize access.
- Know the seriousness of Wi-Fi security.
- Work on router configuration.
- Know the security risks based on Wi-Fi/router.
- Defining servers.
- Analyzing server logs.
- Router and its configuration.
- Mistakes during setting up routers.
- Risks of insecure router.
- Analyzing router logs.

- Case studies related to hacking of computer system.

16 MALWARE ANALYSIS

- What is malware & understanding of malware workflow.
- How malware is used for committing the cyber crime.
- Goals of malware analysis, AV scanning, hashing, finding strings, packing and obfuscation, PE file format, static/linked libraries and functions.
- Static analysis tools, virtual machines and their usage in malware analysis, sand boxing, basic dynamic analysis, malware execution, process monitoring, viewing processes, registry snapshots, creating fake networks.
- Live malware analysis, dead malware analysis, analyzing traces of Malware, System Calls, API Calls, Registries, and Network Activities.
- Android malware analysis: Android architecture, App development cycle, APKTool, APK Inspector, static and dynamic Analysis, case studies.

17 INVESTIGATION OF CRITICAL INFRASTRUCTURE RELATED CRIMES

- Understanding of critical infrastructure.
- What is a SCADA network.
- Railway networks.
- Power Grid networks.
- Water Grid networks.
- Nuclear power plants.
- Indian SCADA systems – digitalization perspective.
- Case studies from famous attacks on

SCADA or critical infrastructure.

- NCIIPC role.

18 CCTV FOOTAGE FORENSICS (IMAGE ENHANCEMENT & ANALYSIS)

- Introduction to the forensic video analysis and workflow concepts.
- Understanding video formats.
- Digital video recovery & playback.
- Intro to video processing.
- Video enhancement.
- Demultiplexing.
- Footage restoration.
- Visual authentication.
- Enhancement & speed correction.
- Format conversion.
- Audio enhancement.
- Tampering investigations.

19 CYBER SECURITY PRACTICES- CYBER AUDIT PROCEDURE

- Pillars of cyber security – Confidentiality, Integrity, Availability.
- Data File Directory, System, Network, Internet Security.
- Web security, data security, network security.
- VAPT / OWASP top 10 attacks.
- IDS, IPS, Firewall's.
- Data encryption.
- Business continuity & disaster recovery.
- Standards- ISO 27001; NIST framework.
- Emerging threats due to advancement in technology.
- Threats to system.
- Online threats.
- Countermeasures.
- Defining cyber threats.
- Types of cyber threats.
- Offline and online threats.
- Advance technologies which can be

used by criminals.
- Countermeasures.
- Introduction to Kali / DEFT / Paladin

20 PRACTICAL INVESTIGATION ON CULPRIT SYSTEMS & NETWORKS

- Foot printing and reconnaissance on culprit systems & networks.
- Scanning culprit networks.
- Enumeration.
- Vulnerability analysis.
- System hacking.
- Malware threats.
- Sniffing.
- Social engineering.
- Denial-of-service
- Session hijacking.
- Evading IDS, Firewalls and Honeypots
- Hacking web servers.
- Hacking web applications.
- SQL injection.
- Penetration on wireless networks.
- Penetration on mobile platforms.

21 CYBER SAFETY & AWARENESS PRACTICES

- Computer safety.
- Mobile safety.
- Network safety.
- Parental control systems.
- Awareness to the society for cyber safety.
- Cyber Swachhta Kendra.
- Cyber patrolling.
- MHA-IB- initiative cyber peace.
- Cyber security measures for the police officers.

22 NODAL AGENCIES AND RESPONSIBILITIES

- CERT-In, RBI, SEBI, NCIIPC, Sectoral CERTs, MHA-CIS (Cyber & Information Security).
- MSP/ISP/OTTs.
- MHA-I4C.
- MHA-Cyber Crime Reporting Portal.
- MHA-IB- Cycord.
- FIU-RBI.
- NPCI.
- RBI-Financial Intelligence Unit (FIU).
- Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism.

23 SCENARIO BASED INVESTIGATIONS ON ABOVE CRIME MODUS BY TRAINEES

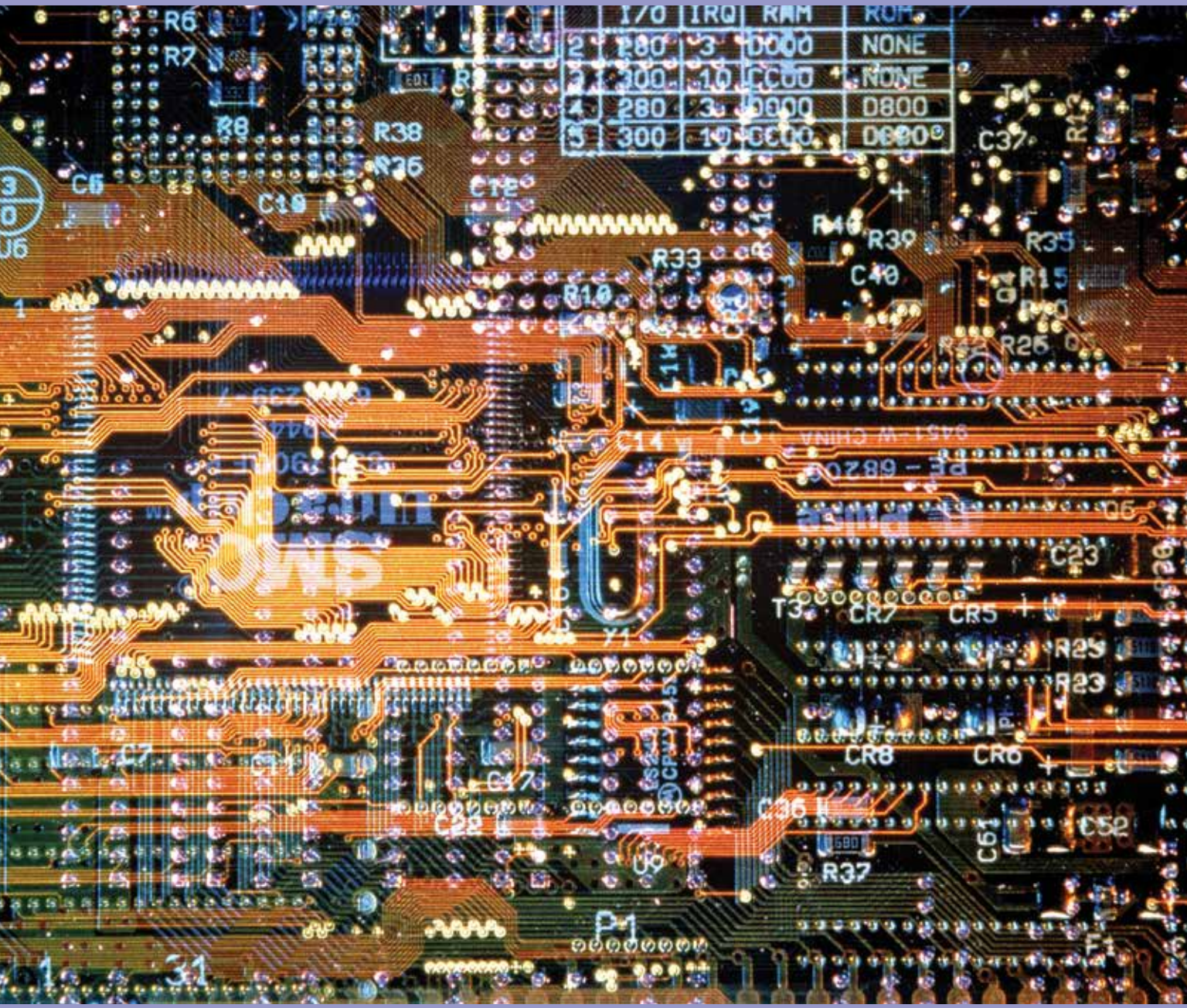
24 PRE & POST ASSESSMENTS

MODULE - IV

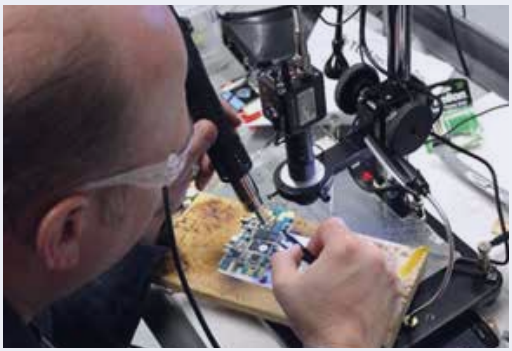
Special Advanced Course

(Two Weeks)

ADVANCED EVIDENCE EXTRACTION TECHNIQUES USING JTAG-CHIP OFF-ISP


I/O
IRQ
RAM
ROM
2 280 3 D000 NONE
3 300 10 CC00 NONE
4 280 3 D000 D800
5 300 10 CC00 D800
R6
R7
R8
R38
R36
C6
C19
C37
R40
R39
R33
C40
R35
R15
R10
R32
R26
C23
T3
CR7
CR5
R25
R23
CR8
CR6
C7
C17
C28
C36
C52
C61
R37
P1
31

LEA officers shall acquire the data recovery skills at chip level using JTAG, Chip-off & ISP Training using dedicated hardware and software capability.



S.No	Day	Course Content
1	Day - I	● Introduction to networks ● Intro to SIM cards and mobile devices ● SIM cloning & handset extractions ● Intro to location data ● Common challenges with devices ● Searching & exporting
2	Day – II	● Day 1 Review ● Intro to smartphones ● Android basics ● iDevice basics ● Windows phone basics ● BlackBerry basics ● Assessment exercise

S.No	Day	Course Content
3	Day – III	● Different extraction types ● Android logical extractions ● Next Level Logical Extractions ● GPS devices & locations ● Connection types & passcodes ● Dumping and decoding feature phones ● Non-standard mobile devices
4	Day – IV	● Introduction to HEX ● File systems & memory cards ● HEX searching & file signatures ● Data hashing
5	Day – V	● RAM disk & bootloaders ● Dumping & decoding smartphones ● Import & Export ● P-Lists & SQL databases ● Investigating apps ● Support tools ● Assessment
6	Day -VI	● Course introduction ● Device disassembly and reassembly ● Applying the JTAG technique properly to acquire data ● Obtaining a physical image from a locked/USB debugging disabled android phone, determining the password and then recovering the user data using your forensic tools ● Advanced extraction methods ● JTAG extraction practical

S.No	Day	Course Content
7	Day - VII	● Health & safety ● Memory chip knowledge ● Properly removing a BGA chip from a device ● Handling and preparing the chip to be read ● Reading the chip to acquire the data ● Applying tools and techniques to decode the data ● Hands-on lessons using password protected Blackberry devices, and utilizing forensic software to recover the data ● Intro to eMMC ● Chip-off equipment ● USB eMMC Chip-off practical ● Handset eMMC chip off practical
8	Day - VIII	● Importing data dumps ● Working with data dumps ● Partition & File systems
9	Day - IX	● Android & ADB ● Rooting ● Swipe PIN decoding ● USB disabled devices ● DD & Nanddump ● Encryption schemes ● Decryption android user data partition
10	Day - X	● App programming languages ● Decompiling APK files ● Reverse engineering apps - Android ● Decrypting apps ● Assessment & closure


F3
F4
F5
@
2
#
3
$
4
%
5
W
E
R
S
D
F
T
6
Y
X
C
V
G
H
B
N

MODULE - I

Basic Course

(One Week)

INVESTIGATION OF CYBER CRIME CASES

AIM

To create awareness & investigation capability among the participants about the importance of Cyber Forensics in investigation of Cyber Crimes and to know the technique of investigation of various Cyber Crimes including collection, preservation and seizure of digital evidence and forwarding them to the Forensic experts for connecting the culprits with the crime.

OBJECTIVES

At the end of the training the participants will be able to:

- Identify various Modus Operandi in Cyber Crimes
- Understand the importance and various aspects of cyber forensics in the investigation of Cyber Crimes
- Get exposure to the Indian IT Act/Cyber Laws and its interpretation in Cyber Crimes
- Define the roles and responsibilities of the IO and the cyber expert in the investigation of Cyber Crimes
- Follow best practices in collection, preservation and seizure of digital evidence and forwarding the same to forensic labs

(1st Week)

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
1	Registration (Formal inauguration by course coordinator) Ice breaking session followed by pre-course test	T E A	Understanding computer systems and components - LEA perspective	Understanding computer systems and components - LEA perspective	L U N C H	Demo of a computer system and components/ peripherals – A crime scene management perspective	T E A	Assembling & dissembling of a computer system and various components/ peripherals - Hands-on practice by trainees
2	Introduction to computer network and its importance in cyber crime incidents as digital evidence **Note:** trainer shall demonstrate with network devices & connectors	T E A	Introduction to Mobile Devices and their importance in Cyber Crime incidents as Digital Evidence **Note:** Trainer shall demonstrate Mobile Devices (2G, 3G/4G & Different Mobile Sets)	Introduction to Cyber Crimes and the Cyber Crime Investigation. Recent Trends & Emerging Crimes in Cyber Space **Note:** Trainer shall demonstrate with Sets of Live Cases	L U N C H	Introduction to PSTN call based investigation; CDR and TDR Analysis using Excel Sheet **Note:** Trainer shall showcase different scenarios with sample CDR/ TDR Excel/CSV Sheets	T E A	CDR & TDR Hands-on Practice by trainees with multiple case scenarios

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
3	**Understating of Digital Evidence and Forensic Technologies** - Computer System as Evidence	TEA	**Introduction to Digital Evidence and Forensic Technologies** - Mobile Device as Evidence	**Introduction to Digital Evidence and Forensic Technologies** - Other Digital Gadgets/ Peripherals as Evidence	LUNCH	**Live Simulation of Crime Scene Management** -Search & Seizure, Evidence Packing Procedure, CoC Formalities, FSL Forwarding Note	TEA	**Live Simulation of Crime Scene Management** ... Contd
4	**Introduction to website, its working and Investigation of web related Crimes**	TEA	**Practical Demonstration on website Investigation** (Live, Deleted, Deactivated & Defaced Websites and Specific Offensive Content, their removal including Website Evidence Extraction & Preservation Procedures)		LUNCH	**Website Investigation** - Hands-on by Trainees with Simulated Cases	TEA	**Website Investigation** - Hands-on by Trainees with Simulated Cases followed by Group Presentation
5	**Introduction to the IT Act, IT Act Amendments & the Indian Evidence Act**	TEA	**Introduction to the IT Act, IT Act Amendments & the Indian Evidence Act**		LUNCH	**Common Cyber Crime scenarios based exercises**	TEA	**Group Presentation on Live Cases, Oral & Written Feedback** -Followed by Valedictory

Note: BPR&D to provide Computer Systems, Network Connectivity, Investigative Free/Open Source Tools and facilities in an integrated Lab Environment.

MODULE - II

Intermediate Course

(One Week)

INVESTIGATION OF CYBER CRIME CASES

AIM

To create better understanding amongst participants about the importance of Cyber Forensics in Investigation of Cyber Crimes and to train them for technical investigation of crimes related to Emails, Internet Calls and other modus operandi. Trainees would be able to understand different techniques of CCTV Footage Analysis and Live Forensics. The training shall also focus on MLAT, Letter Rogatory, International Laws and Effective Witness Procedure.

OBJECTIVES

At the end of the training the participants will be able to:

- Identify various Modus Operandi in Cyber Crimes with emphasis on Email, VOIP Call, Social Media Investigation
- Understand the importance of Cyber Forensics (Imaging & Analysis) in the investigation of Cyber Crimes.
- Understand the Effective Witness Procedures and International Laws
- Define the roles and responsibilities of the IO and cyber expert in investigation of Cyber Crimes
- Understand collection, preservation and seizure of digital evidence and forwarding the same to Forensic Lab.

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
1	Registration (Formal Inauguration by Course Coordinator) ICE Breaking Session followed by Pre Course Test on Basic Module	T E A	Recap session of topics covered in basic course and connectivity to intermediate course.	Introduction to Email Working Procedure - LEA Perspective	L U N C H	Introduction to Email Crimes & its Modus Operandi. Practical Demo on Email Investigation (Web/App Based Emails, Spoof/ Proxy Emails etc.)	T E A	Demo on Email Investigation with Email Evidence Preservation Procedure, Header Analysis etc. –Followed by Hands-On Practice by Trainees
2	Introduction to Forensic Image Procedure. Note: Trainer shall demonstrate different scenarios using Disk/Pen Drive as evidence and imaging procedure steps for the same including Hash Calculation. Free Tools: FTK Imager/Encase Imager etc. may use for Imaging	T E A	Analysis of Forensic Image. Note: Trainer shall demonstrate with Disk/ Pen Drive Image Creation, Image Mounting, Carving and Signature Analysis procedure steps. Premium Tools: FTK/Encase/ Prodiscover etc. may be used for the demonstration. Free Tools: Autopsy Forensic Tool etc.		L U N C H	Forensic Imaging & Hash Analysis Hands-On Practice by Trainees with multiple case scenarios	T E A	Forensic Image and Analysis Hands-On Practice by Trainees with multiple case scenarios... Contd.

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
3	Introduction to Live Forensics (analysis of Volatile memory) - Identifying Passwords - Capturing recently visited URL's, Bookmarks - Cached memory - Browsing history – Search history, form data etc. – - Network information, Collection of Network Logs from Routers, and open WiFi / hotspots etc.	T E A	Introduction to Live Forensics (analysis of Volatile memory) ... Contd.		L U N C H	Introduction to Emerging Technology Driven Forensics	T E A	Simulation on Live Forensic Techniques - Analysis of Volatile memory by Trainees with multiple case scenarios
4	Handling CCTV related Crime & investigations Procedure - Special focus on Search & Seizure Procedure of DVR/NVR	T E A	Working with Encrypted/ Protected Devices/Data (Screen Locker-Computer/ Mobile, Degausser, Cryptography, Encryption, Steganography identification of Keyloggers / Screen recorders, Data Hiding, Wiping Defeating a forensic expert, Anti-forensics methods)		L U N C H	Introduction to VoIP Call Crimes & its investigation procedure with IPDR/IPCDR Analysis	T E A	**Practical Demonstration on IPDR Analysis with live Simulated Cases followed by Group Presentation**

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
5	Introduction to Gathering of useful information through cyber space using OSINT, SOCMINT, SIGINT techniques Note: Trainer would use different websites, frameworks, OS enabled tools and free/open source tools and utilities.	T E A	Hands-on Session on Gathering information through cyber space using OSINT, SOCMINT, SIGMINT techniques followed by live cases		L U N C H	Becoming an effective witness - Role of witness (79 A and 45 B Section of IT Act) - Scope of witness - Types of witness - Process followed during investigation. - Report preparation for court - General ethics for a witness - International laws	T E A	Group Presentation on Live Cases Oral & Written Feedback Followed by Valedictory

Note: BPR&D shall facilitate Computer Systems, Network Connectivity and Investigative Tools -Premium, Free/Open Source Tools and facilities in an integrated Lab Environment.


CYBER CRIME CYBER CRIME CYBER CRIME
CYBER CRIME CYBER CRIME

MODULE - III

Advanced Course

(Two Weeks)

INVESTIGATION OF CYBER CRIME CASES

AIM

To create in depth knowledge amongst the participants on Advanced Cyber Forensic Investigation Techniques and to get exposure in combating emerging Cyber Crimes. Trainees would have a better understanding of collection, preservation and seizure techniques of digital evidence especially related to Social Media. This module of the training shall also focus on International laws and Effective Witness Procedure.

OBJECTIVES

At the end of the training the participants will be able to:

- Understand different techniques to combat Social Media related crimes.
- Understand the importance of cyber-attacks & Network forensics in the investigation of cyber crimes.
- Identify the various Modus Operandi in Cyber Crimes with emphasis on Cyber Terrorism & Dark net crimes
- Learn various CCTV Video Enhancement techniques in crime detection
- Understand collection, preservation and seizure of digital evidence and forwarding the same to Forensic Lab

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
1	Registration (Formal Inauguration by Course Coordinator) ICE Breaking Session followed by Pre-Course Test on Intermediate Module	T E A	Recap Session on topics covered in Basic, Intermediate course and introduction to Advanced course.	Introduction to Social Media and Social Networking related Crimes & Investigation Procedures	L U N C H	Live Demo on Facebook related crimes investigation: Cyber stalking, Bullying , Harassment, Content investigation (obscenity / nudity /fake profile/fake news spreading/ defamatory related cases)	T E A	Hands-on Practice by trainees with multiple case scenarios related to FB crimes
2	Understanding of Twitter related crimes & its investigations: - What is twitter - Twitter functions & Features - Identity theft related cases on Twitter - Content removal from Twitter - Investigation on Tweet, Retweet, Tags, Handlers - Twitter Analytics - Web patrolling using Twitter - Downloading complete tweets from a profile, keyword etc. - Sentiment analysis - Collection, preservation of digital evidences and presentation in the court of law	T E A	Practical demo on Twitter related investigations with Live and Simulated Cases:		L U N C H	Instagram related Investigations: - Identifying theft related cases - Different type of Cyber Crime associated (Cyber stalking / Bullying / Harassment) - Instagram related cases - Content investigation (obscenity / nudity / defamatory related cases) - Content removal - Downloading complete content	T E A	Hands-on Practice by trainees related to Twitter, Instagram Cases

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
3	**Youtube related investigations:** - Content investigation (obscenity / nudity / defamation related cases) - Copyright infringement related cases. - Youtube Video content removal procedure - Tracing user details of offenders on youtube - Youtube video tracking through geolocation/geotagging - Collection, preservation of digital evidences, presentation of the same in the court of law.	T E A	**Matrimonial / Dating / Adultery related investigations:** - Content investigation (obscenity / nudity / defamatory related cases) - Tinder / Happn / Locanto / Tagged/ Escort Services Related Apps/ Websites - Collection, preservation of digital evidences, presentation in the court of law		L U N C H	**Other social media Apps / Websites related investigations:** - Tiktok / Sharechat / Musically - Games Related Investigations (Blue Whale, PubG, Fortnite, MoMo Games)	T E A	**Hands-on practice by trainees on cases related to Youtube, Tiktok, Matrimonial sites etc.**

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
4	**Investigation of Fin-Tech related cases:** - Various kinds of Fin-Tech options available in India - Common misconceptions - Investigating e-wallets related frauds - Investigating ATM related frauds - Investigating OTP related frauds - Investigating Payment gateways - Investigating identity theft related cases - Job frauds, Gambling, Betting, Financial transactions for illegal activities - Advanced (Malware analysis and cases related to ransomware, and other malwares)	T E A	**Handling of Cyber Fraud Cases With Practical Case Studies** - Net banking Frauds - Debit/Credit Card Frauds - E-Wallet Frauds - OTP Frauds - Skimming/Cloning Frauds - OLX Frauds - Job Frauds (Website, Email, SMS, Instant Message as a Crime Channel) **Investigation Procedure on Above Case Scenarios**		L U N C H	Handling of Cyber Fraud cases with practical case studies	T E A	Hands-on Exercise on Cyber Fraud Cases with live Simulated Environment followed by Group Presentation
5	Advanced Training Test	T E A	Field Visit of Cert-In NCIIPC GOVT/Private -SOC/SIEM CCTNS Network SCADA Networks		L U N C H	Field Visit Cert-In NCIIPC GOVT/Private -SOC/SIEM CCTN Networks SCADA Networks	T E A	Field Visit Oral & Written Feedback followed by Valediction and Distribution of Certificates

Note: BPR&D shall facilitate Computer Systems, Network Connectivity, Investigative Tools -Premium, Free/Open Source Tools and facilities in an integrated Lab Environment.

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
6	**Importance of Network Forensics in Cyber Attack Investigation** - Introduction to Network Protocols - Network Evidence types and Sources – Switch, Firewall, IDS / IPS, Router - Network Packet Capture PCAP - Encapsulation and DE capsulation methods - Session reconstruction for protocols TCP and HTTP - Log collection, aggregation, and analysis - Wireless Packet Analysis - Different Challenges faced during handling Encoding, Encryption, VPN issues including MITM - Man-in-the-Middle Methods.	T E A	**Practical Session on Network Forensics using Wireshark / Network miner tools etc.** - Hands-On Practice by Trainees with multiple network investigation scenarios		L U N C H	**Practical Investigation on Penetration of Culprit Systems & Network using Kali Linux & other free software** - Foot printing and Reconnaissance on culprit Systems & Networks - Scanning Culprit Networks - Enumeration - Vulnerability Analysis - Understanding of System Hacking - Malware Threats - Sniffing - Social Engineering	T E A	**Practical Investigation on Penetration of Culprit Systems & Networks using Kali Linux & other free software** - Denial-of-Service - Session Hijacking - Evading IDS, Firewalls, and Honeypots -Understanding of Hacking Web Servers -Understanding of Hacking Web Applications -Understanding of SQL Injection -Understanding of Hacking Wireless Networks -Understanding of Hacking Mobile Platforms -Understanding of IoT Hacking

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
7	**Introduction to location / cloud based investigations** - Introduction to Location Based Services. - Types of Location Based Services. - Triangulation and GPS Techniques to pin point the actual location of the criminals by using Triangulation techniques. - By using GPS tagging on photographs by using Google photos and other cloud based APIs and by using WhatsApp, Facebook, Viber etc. - Retrieval of data from Google / iCloud /Microsoft cloud services. -Tracing missing/stolen mobile By Using IMEI No. - Tracing missing/stolen mobile By Using MAC No.	T E A	**Hands on session on cloud based investigations**		L U N C H	**WhatsApp/ Telegram and other social media apps investigations & Forensics Examination** - Live WhatsApp/ Telegram investigation using digital foot prints - Retrieval of Deleted WhatsApp/ Telegram chat messages - WhatsApp/ Telegram image or video offences related investigation - Examination of Cyber harassment through WhatsApp/ Telegram - Investigation of WhatsApp and other group messaging services. - Monitoring techniques of WhatsApp/Telegram groups through masking methods	T E A	**Hands-on exercise on location tracing & WhatsApp Forensics** **Followed by Advanced Training Grand Test & Oral/Written Feedback**

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
		T E A			L U N C H	- Legal approach to request details from WhatsApp and other messaging service providers - How to identify Originator of post (Content, Image, Video) - WhatsApp Call Investigations (Audio, Video)	T E A	

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
8	**CCTV Footage Enhancement & Video Forensics** - Understanding of CCTV Network - Understanding of DVR & NVR - Video Enhancement techniques and tools - Demultiplexing - Footage Restoration - Visual Authentication - Enhancement & Speed Correction - Format Conversion - Audio Enhancement - Investigation of tampered footages, audio files etc.	T E A	**Practical demo on CCTV Forensics using Open Source & Premium Tools** Hands-On Practice by Trainees with multiple case scenarios on CCTV Footage related Cases		L U N C H	**Practical demo on Malware Analysis** - What is Malware - How malwares are used by cyber criminals for intrusion - Understanding of malware analysis - AV Scanning, Hashing, Finding Strings, Packing and Obfuscation, PE file format, Static, Linked Libraries and Functions. - Static Analysis tools, Virtual Machines and their usage in malware analysis, Sandboxing. - Basic dynamic analysis, Malware execution process Monitoring, Viewing processes, Registry snapshots, creating fake networks.	T E A	**Practical demo on Malware Analysis** - Hands-On Practice by Trainees With multiple case scenarios related to Malware Cases

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
9	**The Role of Cyber Terrorism in Digital Space** - Misuse of Internet by terrorist organizations - Introduction to Botnet - Recruitment, spread of propaganda on Internet - Phony websites & Cyber Herding - Web crawlers and use of data mining - Proactive measures to combat misuse of Internet by the terrorists	T E A	**Introduction to Dark Web investigations** - Introduction of Deep & Dark Net - Surface Internet vs Deep Internet - Indexed Website vs Non-Indexed Websites - Red Rooms, Galaxy, Hidden Wiki, Wiki leaks, Silk Road, Pandora and other Onion links - Modus operandi of cyber-crimes committed using Dark Web - Working principle of Block Chain - Concepts of Crypto currencies and mechanism behind it - Wallet Tracking, Public Key vs Private Key (w.r.t. Crypto Currencies) - Introduction to track crypto currencies and challenges in investigations.		L U N C H	**Investigation of critical infrastructure related crimes** - SCADA Networks - Railway Networks - Power Grid Networks - Water Grid Networks - Nuclear Power Plants - Maharashtra State SCADA systems – Digitalization perspective - Case studies from famous attacks on scada or Critical infra	T E A	**Other Social Media Apps / Websites related investigations:** - Tiktok / Sharechat / Musically - Games Related Investigations (Blue Whale, PubG, Fortnite, MoMo etc. Games) - Live Simulation on Snapchat, YOutube, Tiktok etc.

Day	09:30-10:30		11:00-12:00	12:00-13:00		14:00-15:00		15:30-17:30
10	**Cyber Security Practices** - Pillars of Cyber Security, Confidentiality, Integrity, Availability. - Web security, data security and network security - VAPT / OWASP top 10 attacks - IDS, IPS, Firewalls - Data Encryption - Standards- ISO 27001; NIST framework - Emerging threats due to advancement in technology - Threats to system - Online threats - Countermeasures - Defining Cyber threats - Types of Cyber threats - Offline and Online threats	T E A	**Cyber Security Practices in** - Organizational networks - Government Network Infrastructure - Critical Network Infrastructure - Security Audit - ISO/IEC & MEITY Guidelines etc.		L U N C H	**Cyber Safety Practices** - Computer Safety guidelines - Mobile Safety guidelines - Network Safety guidelines - Parental control systems - Awareness to the society for Cyber Safety - Cyber Swachta Kendra - Cyber Patrolling - Cyber Security measures for the police officers	T E A	**Hands-on Exercise on Cyber Security & Safety Practices**

MODULE - IV

Special Advanced Course

(Two Weeks)

INVESTIGATION OF CYBER CRIME CASES

AIM

To learn innovative ways in extracting data from different Digital Devices employed in various Cyber Crime. It would help IOs to learn different techniques to extract data from mobile devices when traditional forensic tools are no longer an option. It would take trainees to the next level of knowledge and understanding of mobile forensics. This course would focus on the extraction and recovery of data via JTAG and Chip Off/ISP methods. Trainees will also be receiving de-soldering practical experience to learn how to extract components from a device for Advance Forensics.

OBJECTIVES

At the end of the training the participants will be able to:

- Understand the importance of advanced Cyber Forensics in the investigation of Cyber Crimes.
- Identify the various Modus Operandi in damaged digital devices in Cyber Crimes/traditional crimes
- Understand and learn upcoming trends in Cyber Crime and their combat mechanisms

Day	Course Content
I	• Introduction to Networks • Introduction to SIM Cards and Mobile Devices • SIM Cloning & Handset Data extractions • Introduction to Location Data • Common Challenges with Devices • Searching & Exporting
II	• Day 1 Review • Intro to Smartphones • Android Basics • Apple devices Basics • Windows Phone Basics • BlackBerry devices Basics • Assessment Exercise
III	• Different data Extraction Types • Android data Logical Extractions • Next Level Logical data Extractions • GPS Devices & Locations • Connection Types & Passcodes • Dumping and Decoding Feature Phones • Non-Standard Mobile Devices
IV	• Introduction to HEX • File Systems & Memory Cards • HEX Searching & File Signatures • Data Hashing

Day	Course Content
V	• RAM Disk & bootloaders • Dumping & decoding smartphones • Import & export • PLists & SQL databases • Investigating apps • Support tools • Assessment
VI	• Course introduction • Disassembling and reassembling of device components • Using JTAG technique properly to acquire data • Obtaining a physical image from a locked/USB Debugging disabled Android phone, determining the password and then recovering the user data using forensic tools • Advanced extraction methods • JTAG extraction (Practical Session)
VII	• Health & Safety • Memory chip knowledge • Properly removing a BGA chip from a device • Handling and preparing the chip to be read • Reading the chip to acquire the data • Applying tools and techniques to decode the data • Blackberry devices, and utilizing forensic software to recover the data • Introduction to eMMC • Introduction chip-off equipment • USB eMMC Chip-off practical • Handset eMMC chip off (Practical Session)
VIII	• Importing data dumps • Working with data dumps • Partitioning of RAW disk & File Systems

Day	Course Content
IX	• Android & ADB • Rooting various operating systems on electronic devices • Swipe PIN decoding • USB disabled devices • DD & Nand dump • Encryption schemes • Decryption of Android user data partition
X	• App programming languages • Decompiling APK files • Reverse engineering Apps - Android • Decrypting apps • Assessment & closure

Note: BPR&D shall facilitate Computer Systems, Network Connectivity, JTAG, Chip-off, ISP toolkits and sample mobile devices with multiple OEMs and versions.

Notes

Notes

BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037

officialBPRDIndia BPRDIndia Bureau of Police Research & Development India bprdindia www.bprd.nic.in