TCCI COURSE MODULES

TCCI COURSE MODULES

Chapter I: Introduction to Cyber Crimes and Initiatives

- Overview of Cyber Crimes
- Indian Scenario
- Government and Law Enforcement Initiatives
- NASSCOM – DSCI Initiatives

Chapter II: Understanding Cyber Crimes

- Definitions
- Tools and Techniques Used to Commit Cyber Crimes
- Types of Cyber Crimes
    - Crimes targeting computer systems
    - Crimes in which computer systems are used as tools/instruments
- What is Digital Evidence and the Nature of Digital Evidence
- Digital Devices – Sources for Digital Evidence
- Cyber Forensics
    - Definition
    - Classification of Cyber Forensics
    - What Cyber Forensics Can Reveal

    - What can the IO expect from Cyber Forensic Analysis

Chapter III: Application of Law

- Cyber Crimes and Information Technology Act
- Cyber Crimes Mapping with ITAA 2008, IPC and Special & Local Laws.
- Laws / Guidelines Relating To International Investigations
    - Legal procedure to gather information from outside India
    - Procedure for Sending Letter Rogatory

Chapter IV: Pre-Investigation Assessment

- Doing the Basics Right
- Is it a crime (as per ITAA2008) in the first place?
- Preliminary Review of the Scene of Offence
    - Evaluating the Scene of Offence
    - Preliminary Interviews at the Scene of Offence
- Pre-Investigation Technical Assessment
- Issuance of preservation notice
- Containment of the incident / Offence

Chapter V: Standard Operating Procedures for Investigations

- Importance of SOPs in the Investigation
- Standard Operating Procedures – A Flow Chart
- Crime Scene Investigation: Search and Seizure
    - Steps in Crime Scene Investigation
    - Panchanama (Seizure Memo) and Seizure Proceedings
- Chain of Custody and Digital Evidence Collection Form
    - Chain of custody
    - Digital Evidence Collection (DEC) form

- Forensic Collection of Digital Media
    - Identifying/Seizing the devices that need to be forensically imaged for analysis
    - Investigative Tools and Equipment
- Collection of Digital Evidence
    - Procedure for gathering evidence from switched-off systems
    - Procedure for gathering evidence from live systems (Switched-on Systems)
    - Procedure for gathering evidence from Mobile Phones
- Forensic Duplication – A Technical Introduction
- Network Drives Imaging and Logical File Collection
- Conducting Interviews
- Packaging and labeling of the evidence
- Transportation of the evidence
- Legal procedure to be followed post-seizure of evidence
- Expert Opinion from the Forensic Examiner
- Analyzing External / Third-party information
    - Time Zone Conversion
    - Email Headers
    - Cases where the Subject Mail Is Not Available
- Gathering information from external agencies/companies
    - Availability of information and format from ISPs
    - Information from email services
    - Information from Mobile service providers
    - Information from Social networking sites
    - Information from Financial institutions/Internet banking institutions
    - Information from Website domain/hosting providers
    - Information from VoIP service providers
    - Analyzing and handling the external data
- Correlating the external data with lab findings

Chapter VI: Investigation of Offences - Scenario Based

- Case Scenarios
    - Preparation of Forged Counterfeits using Computers /Printers/Scanners
    - Phishing Frauds
    - Obscene Profile on a Social Networking Site
    - Data Theft
    - Blocking of Websites
    - Kidnapping Case of a Minor Girl
    - Hacking using Keylogger
- Guidelines to prepare a charge sheet
- Tips to Preserve the Seized Digital Media
- Tips to prepare for deposition of evidence in the court

Chapter VII: Advanced Forensics Modules

- Windows Forensics
    - Windows Operating System Internals
    - Techniques for Investigating Windows Systems
    - Analyzing Windows Logs and Artifacts
- Linux Forensics
    - Linux Operating System Internals
    - Techniques for Investigating Linux Systems
    - Analyzing Linux Logs and Artifacts

Chapter VIII: Advanced OSINT Modules

- Advanced OSINT Techniques
    - Deep and Dark Web Investigations
    - Advanced Image OSINT and Geolocation Techniques
    - Social Media OSINT: Deep Dive into Platforms

- OSINT Virtual Machines (VMs)
    - Setting Up and Configuring OSINT VMs
    - Enhancing Anonymity and Security in OSINT Operations
- OSINT Tools and Frameworks
    - Utilization of Cutting-Edge OSINT Tools
    - Case Studies on Advanced OSINT Applications