

Course Contents for the ITEC Training Program on Computer and Mobile Forensics

Day: -1

- Emerging trends & techniques in cyber security & digital crimes.
- Introduction & Identification of Digital Evidence.
- Search and Seizure Process of Digital Evidence. (Hands On)
- Visit to various Center of Excellence.

Day: -2

- Forensic Duplication Process & Authentication and Verification of Digital evidence.
- Digital Evidence Acquisition Techniques. (Hands On)
- Data Recovery & Data Carving fundamentals.

Day: -3

- Deep diving and data mining from the computer forensic perspective.
- Types of potential digital evidence that can be created by an Operating System.
- Computer Forensic Analysis platforms, tools & Techniques. (Hands On)

Day: -4

- Acquisition of data from running servers, Accessing /Preservation of data from routers / Wifi Access Points.
- Useful Commands & Techniques to lead the investigation process (Hands On)
- Packet Capturing and Analysis. (Hands On)

Day: -5

- Firewalls, IDS & IPS, Content Security & Log analysis. (Hands On)
- Introduction to dark web & understanding the functioning of cryptocurrency.
- Introduction to internet-based crime.
- Drone technology in today's world in combating terror.

Day: -6

- Crime Scene Management Hands on Exercise.
- Emerging trends & techniques in Mobile Forensics technologies.
- Fundamentals of mobile forensics & Acquisition Techniques.
- Fundamentals of Mobile Forensics & Analysis Techniques.

Day: -7

- Mobile device 3rd party application analysis techniques.
- Mobile Cloud & Cloud Data Extraction.
- Digital Forensics for detection of multimedia frauds & digital crimes.
- Introduction to multimedia evidence, multimedia forensics.

Day: -8

- Handling, Collection and preservation of Multimedia exhibits for analysis.
- Types and components of CCTV architecture.
- Detecting the origin of multimedia files, digital watermarking, confirming the integrity of the files.

Day: -9

- Enhancement and authentication of video / Image.
- Hands on training tools for authentication of Video / Image Files.
- Overview of Deepfake – an introduction & forensic analysis.
- Fundamentals of OSINT.

Day: -10

- Deep Fake identification, detection and Analysis techniques.
- Artificial Intelligence based Big Data Analytics for Cyber Terrorism Case Investigation.
- Assessment.
- Valedictory.