Course Contents for the ITEC Training Program on Digital Forensics and Cyber Security

Day: -1

- Brief about NFSU
- Emerging trends & techniques in cyber security & digital crimes
- Search and Seizure of Digital Devices-Standard Operating Procedures & best Practices.
- Visit to various Center of Excellences.

Day: -2

- Concept of disk duplication, write blocker, and Hash value
- Identification of potential digital evidence
- Computer Forensic Tools & Investigation Tactics
- Computer Data Acquisition & Analysis

Day: -3

- Advance Computer Forensics Investigation (Volatile Memory Forensics)
- Incident Response and Malware Analysis
- Cyber Kill Chain & Ransomware Investigation
- Handling, Collection & preservation of multimedia exhibits for analysis

Day: -4

- Detecting the origin of the multimedia files, digital water marking & confirming the integrity of the file
- Surveillance & AI: Transforming predictive policing with CCTV technology
- Deep Fake Investigation – Identification, detection and analysis techniques
- Enhancement and Authentication of video / image

Day: -5

- Cyber Crime Investigation - Case Studies
- Network Forensics-Packet Capturing and Analysis
- Cloud Forensics
- Investigating Email and Internet Fraud: Techniques for Tracing Cybercriminals

Day: -6

- Fundamentals of Mobile Security 3rd party Application Security
- Introduction to SOC: Role & Functions
- Advanced Threat Detection and Incident Response
- Hands on CoE-Cyber Security

Day: -7

- Introduction to the Email Security and Analysis
- Fundamentals of IoT Security
- Phishing Detection using AI/ML Fundamentals
- Fundamentals of IRM

Day: -8

- Advancement in IoT: Security and Forensics
- Fundamentals of Web Application Security
- Cyber Security Challenges in OT Environment
- Blockchain Fundamentals: An Approach to Data Security

Day: -9

- Operating System Security & Patch Management
- Smart Contract Exploits and Forensics
- Advanced VPN and Proxy Technologies: Strengthening Privacy and Anonymity
- Hands-on at CoE Digital Forensics.

Day: -10

- Forensic Acquisition of Data from IoT Devices.
- OSINT tools and techniques
- Assessment
- Valedictory.