Course Name: Cyber Crime Investigation for the Officers of Tanzania
Dates: 17.02.2025 to 28.02.2025
Duration: 2 Week
Mode: Physical mode at NFSU, Gandhinagar Campus

Objectives of the course:

- To learn the fundamentals and importance of cybercrime.
- To learn different techniques and procedures that enable trainees to perform a digital investigation.
- To carry out analysis of physical storage media.
- To prepare trainees to conduct a digital investigation in an organized and systematic way.
- To learn use of open-source forensics tools to perform digital investigation and understand the underlying theory behind these tools.

Contents:

- Emerging Trends & Techniques in Cyber Crime Investigation Techniques.
- Basics of Computer & Storage Fundamentals.
- Basics of Internet -IP Address, Mac Address, Domain Name System & URLs.
- Useful Commands & Techniques to lead the investigation process.
- Introduction & Identification of Digital Evidence.
- Search and Seizure Process of Digital Evidence.
- Digital Evidence Acquisition Techniques.
- Data Recovery from Various Repositories using freeware & open source tools & technologies.
- Mobile Device Acquisition & Analysis techniques.
- Acquisition of data from running servers, Accessing /Preservation of data from routers / Wifi Access Points.
- Email and Internet Frauds and Investigation Techniques.
- Leveraging Social Media Intelligence Gathering/Cyber Patrolling.
- Admissibility of Digital Evidences & role of service providers.
- Introduction to dark web & understanding the functioning of cryptocurrency.
- OSINT Fundamentals.
- Overview of IT Laws & Its Amendment, Governance & Policies.
- Financial Frauds Overview & Investigation Techniques.
- Cryptocurrency-based crime & Investigation techniques.
- Roles of computers in crime & other misconduct.
- Digital Evidence Acquisition Techniques (Lab).
- Types of potential digital evidence that can be created by an OS.
- Details of common file systems & partitioning Fundamentals.
- OS-specific data hiding & restoration techniques.
- Computer Forensic Analysis platforms, tools & Techniques (Lab).
- Mobile phone Acquisition Techniques.
- Mobile OS Fundamentals & Common File Systems.
- Various data extraction & Data Processing Techniques for hand held devices.
- Mobile Phone Analysis Techniques (Lab).
- Network components that may be of evidentiary significance.
- Network packet filtering & analysis Firewalls, IDS & IPS, Content Security & Log analysis.
- Packet Capturing and Analysis (Lab).
- Emerging trend in social media crimes, Information Gathering/Cyber Patrolling.
- Drafting of Subpoena requests, Preservation letter, Emergency Disclosure Request Form, COC (Chain of Custody) Form.