Course Name: Computer and Mobile Forensics for Belarus Officials

Dates: 23.09.2024 to 04.10.2024

Duration: 2 Week

Mode: Physical mode at NFSU, Gandhinagar Campus

Objectives of the course:

- This course presents an overview of the principles and practices of various digital investigation techniques related to mobile forensics.
- The objective of this program is to emphasize the fundamentals and importance of cyber forensics.
- Participants will learn different techniques and procedures that enable them to perform a cybercrime investigation.
- This course focuses mainly on the analysis of physical storage media and volume analysis of the storage devices.
- It covers the major phases of digital investigation such as preservation, analysis and acquisition of artifacts that reside in various digital devices.
- The objective of this program is to emphasize the importance of computer & mobile forensics and to
- prepare participants to conduct a digital device-based investigation in an organized and systematic way.
- This course will provide theoretical and practical knowledge, as well as current research on Cyber Forensics and investigation.
- Upon completion of the course, participants can apply open-source forensics tools to perform digital investigation and understand the underlying theory behind these tools.

Contents:

- Emerging trends & techniques in cyber security & digital crimes
- Roles of computers in crime & other misconduct
- Introduction & Identification of Digital Evidence
- Search and Seizure Process of Digital Evidence
- Forensic Duplication Process & Authentication and Verification of Digital evidence
- Digital Evidence Acquisition Techniques
- Types of potential digital evidence that can be created by an Operating System
- Computer Forensic Analysis platforms, tools & Techniques
- Deep diving and data mining from the computer forensic perspective
- Data Recovery & Data Carving fundamentals
- Acquisition of data from running servers, Accessing /Preservation of data from routers / Wifi Access Points
- Useful Commands & Techniques to lead the investigation process
- Packet Capturing and Analysis
- Firewalls, IDS & IPS, Content Security & Log analysis
- Email and Internet Frauds and Investigation Techniques
- Introduction to dark web & understanding the functioning of cryptocurrency
- Fundamentals of OSINT
- Overview of IT Act 2000 & Its Amendment in 2008 and Special & Local Laws
- Emerging trends & techniques in Cyber Forensics
- Basics of Mobile Telecommunication Technology & Mobile Storage Fundamentals
- Introduction & Identification of Digital Evidence

- Search and Seizure Process of Digital Evidence and investigation officer roles & responsibilities
- Mobile Phone Acquisition Techniques for Android Devices Using commercial grade forensic tool sets
- Mobile Phone Acquisition Techniques for Apple Devices Using commercial grade forensic tool sets
- Fundamentals of SQLite Databases & importance in mobile forensic
- Mobile device Data Analysis Technique Using Commercial Grade Toolset
- Custom filters, Encrypted Data interpretation & Data normalization techniques using Commercial Grade Toolset
- Open Source Tools & Techniques to lead the mobile investigation techniques
- Mobile Device 3rd party Application Analysis
- Fundamentals of Mobile Malware & mobile malware analysis techniques
- Admissibility of Mobile Evidences & role of service providers
- Introduction to dark web & understanding the functioning of cryptocurrency
- Fundamentals of ASINT
- Overview of IT Act 2000 & Its Amendment in 2008 and Special & Local Law