Course Name: Digital Forensics and Cyber Security for the Officials of Malaysia.
Dates: 19/05/2025 to 30/05/2025 (2 weeks)
Duration: 2 Weeks
Mode: Physical mode at NFSU, Gandhinagar Campus, Gujarat State.

Objectives of the course:

- This course presents an overview of the principles and practices of various digital investigation techniques related to digital forensics.
- The objective of this program is to emphasize the fundamentals and importance of cyber security forensics.
- Participants will learn different techniques and procedures that enable them to perform a cyber security investigation.
- It covers the major phases of digital investigation such as preservation, analysis and acquisition of artifacts that reside in various digital devices.
- It provides exposures on various tools and techniques used in Cyber Security.

Contents:

- Emerging trends & techniques in cyber security & digital forensics
- 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.
- Network components that may be of evidentiary significance.
- Network packet filtering & analysis Firewalls, IDS & IPS, Content Security & Log analysis.
- Leveraging Social Media Intelligence Gathering/Cyber Patrolling.
- Types of potential digital evidence that can be created by an OS.
- 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).