SYLLLABUS: Junior Scientific Assistant (Cyber Forensic) in FSL

1. **Basics of Computers**: Definition, evolution, types of computers, components of a computer, Primary and secondary Storage Devices, Input and Output (I/O) devices, Understanding Disk, Volume, and Partition, HDD and SSD Structures, Number Systems and Logical Operations, Operating System, Boot Process, Process and Memory Management, Windows OS Architecture - FAT and NTFS File Systems. Understanding and Analysing FAT and NTFS File Systems, registry and log-based Forensic analysis, concept of Event log analysis.

2. **Cyber crimes and related offences and penalties**: Introduction to Cybercrimes, Classification of cybercrimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Kinds of cyber crimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; Spamming, Phishing, Privacy and National Security in Cyberspace, Cyber Defamation and hate speech, computer vandalism etc. Provisions in Indian Laws in dealing with Cyber Crimes and its critical analysis, Information Technology Act, 2000, Penalties under IT Act, Offences under IT Act, Offences and Analysis related with Digital Signature and Electronic Signature under IT Act, Statutory Provisions, Establishment of Authorities under IT Act and their functions, powers. Cyber crimes under BNS.

3. **Digital Forensics**: Branches of Digital Forensics, Investigation of digital crime scenes, maintaining proper documentation, and chain of custody. Standard Operating Procedures for Handling,

Preservation, Acquisition, packaging, labeling & Transpiration of electronic evidence, digital data acquisition tools, identifying and collecting data from relevant digital sources such as hard drives, mobile devices, network logs, cloud storage, or email servers, hash value generation, Methods of Data Recovery and Carving, analytical techniques for analyzing digital data such as metadata examination, keyword searches, timeline creation, log correlation, or pattern analysis using specialized software. Tools used for analysis and evaluation of digital evidences.

4. **Memory Forensics:** Acquisition, analysis, and interpretation of volatile memory (RAM), overview of memory structures, types of data stored in RAM, and the significance of memory analysis in identifying malware, running processes, network connections and system artifacts, memory acquisition tools and techniques, extraction of encryption keys. Challenges and legal considerations in memory forensics.

5. **Computer forensics and DVR Forensic:** Basics of computer forensics, acquisition methods, image format (Raw, DD, SMART, AFF, E01 etc.), disk and file encryption techniques, file signature analysis, windows registry analysis, artifacts recognition from slack space and unallocated space, metadata analysis. Basics of DVR and NVR, Types of CCTV camera and their characteristics, Operating Systems. Overview of Computer and DVR forensics software and tools: write blockers, imaging, and cloning devices.

6. **Mobile Forensics:** Basics of mobile devices, motile communications, challenges, resource constraints and types of acquisitions, rooting & system, app permissions, jail-breaking. Android OS architecture and file logging mechanism in Android-phone, types of artefacts, tools and technologies for Android Forensics, challenges & limitations of Android forensics, IOS: iPhone OS (iOS) architecture, iOS file system, iOS app permissions, logging in IOS, tools & technologies for iOS forensics, challenges & limitations of iOS forensics, forensic analysis of Pagers, Wearable devices and other smart gadgets, CDR (Call Details) Analysis.

7. **Information Security:** Confidentiality, Integrity, and Availability (CIA) Triad, Authentication, Authorization, Non-repudiation, concepts of Cryptography & Steganography, Symmetric and Asymmetric algorithms, Hashing Algorithms, Cryptanalysis, Digital Signature, Digital A Certificate, Certifying Authorities (CA). steganalysis and its challenges. Vulnerability Assessment and Penetration Testing (VAPT), vulnerability v/s weakness, types of U, vulnerabilities. Common Vulnerabilities and Exposures (CVEs), Common Vulnerability Scoring System (CVSS), vulnerability assessment tools and techniques, penetration testing and its methods/tools.

8. **Introduction to malware analysis and ransomware analysis:** Introductory Malware Analysis: Malware, viruses, and worms, Importance of Malware Analysis, Importance of Ransom ware Analysis.

9. **Data and Signals**: Analog and Digital Data, Analog and Digital Signals, Periodic and No periodic, Periodic Analog signals, Time and Frequency Domains, Composite Signals, Bandwidth, Digital Signals, Bit Rate, Digital Signal as a Composite Analog Signal, Transmission of Digital and Analog Signals, Transmission Impairment, Attenuation, Distortion, Noise, Data rate limits, Data Flow-Simplex, Half Duplex, Full Duplex.

10. **Semiconductors**: General properties and band structure, carrier statistics, impurities, intrinsic and extrinsic semiconductors, p-n junction, forward biasing & reverse biasing, drift and diffusion currents, mobility, Hall Effect.

11. **Introduction to Forensic Science**: Branches of Forensic Science, Locard's Exchange Principle, Court Evidence, Scene of Crime Examination.