SYLLABUS FOR THE POST OF SCIENTIFIC OFFICER-
AUDIO-VIDEO FORENSICS SECTION
FORENSIC SCIENCE LABORATORY-POLICE DEPARTMENT

1 Digital Forensic and Cyber Crime

Understanding Cyber Crime: Indian IT Act 2008 and amendments, categories of cyber crimes ie., unauthorized access and hacking, virus, worms & Trojan attacks, E-mail related crimes, Internet relay, chat relating crimes, sale of illegal articles, online gambling, phishing, Intellectual property crimes, web defacement, DOS attack, cyber stalking etc.,

2 Working with Windows and DOS Systems

Understanding File Systems, Exploring Microsoft File Structures, Examining NTFS Disks, Understanding Whole Disk Encryption, Understanding the Windows Registry, Understanding Microsoft Startup Tasks, Understanding MS-DOS Startup Tasks, and Understanding Virtual Machines. Macintosh and Linux Boot Processes and File Systems: Understanding the Macintosh File Structure and Boot Process, Examining UNIX and Linux Disk Structures and Boot Processes, Understanding Other Disk Structures. Free space Management Bit-Vector Linked List Grouping Counting Efficiency & Performance Recovery Physical Damage Physical Damage Recovery Logical Damage Logical, Damage Recovery.

3 Current Computer Forensics Tools:

Evaluating Computer Forensic Tool Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating and Testing Forensics Software. Data Acquisition: Understanding Storage Formats for Digital Evidence, Determining the best Acquisition Method, Validating Data Acquisitions, Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, Performing Remote Acquisitions. Performing RAID Data Acquisitions, Using Remote Network Acquisition Tools, and Using Other Forensic Acquisition Tools. Recovering Graphics Files: Recognizing a Graphics File, Understanding Data Compression, Locating and Recovering Graphics Files, Identifying Unknown File Formats, Understanding Copyright Issues with Graphics.

4. Audio /video forensics:

Spectrography – Conversion of different voice file formats in to forensic voice module formats. Various types of spectrograms, spectrographic cues for vowels and consonants. Speech analysis in forensic sciences. Speech synthesis by analysis, Speech recognition and speaker identification. Fundamentals of Digital Signal processing and communication system. Analogue and digital systems, Analogue signal and digital signals, Analogue to digital and digital to analogue converters, need and advantages of digital systems and digital signal processing. Forensic extraction of video files from DVR and other storage media. Forensic examination of DVR containing video footages, its frame analysis. Forensic examination and authentication of meta data present in video/audio files. Enhancement of video/ Photo and its comparison/authentication.

5. Computer hardware/Software :

Hardware: Basic PC Components, Monitors, Keyboard, Storage devices :Hard Disk ; Storage related simple problems, CD, Mother-board, Printers its classification etc, OCR, OMR, BAR Code etc. Memory Hierarchies : Basics of Semiconductor Memories, ROM Cells & Circuits, Address Decoding, Access Time, Examples of Integrated Circuit ROMs, PROMs, EPROMs, EEPROM, Static Read/Write (RAM) Memory.CPU ;ALU, Components of CPU ; Register, Accumulator, IR, etc. Software System- application Software and their Examples in real life. Operating System and their usage. Multitasking –Multiprogramming- Multiprocessing Operating System.

6. NON LINEAR DATA STRUCTURES AND HASH TABLES

Introduction- Definition and Basic terminologies of trees and binary trees. Hash Tables: Introduction- Hash Tables- Hash Functions and its applications. HASH FUNCTIONS AND DIGITAL SIGNATURES-Authentication functions-Message authentication codes-Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm)-Digital signatures (Authentication protocols, Digital signature Standard).

7. Mobile phone forensics:

mobile phone data acquisition through logical, physical and file system techniques, forensic procedures, device data, external memory dump, evidences from memory card, Android forensics: Procedures for handling an android device, imaging android USB mass storage devices. Decrypting of encrypted files, analysis of .db files. Recovering of files, Voice.

8. Escalating privileges-

Hiding Files- Steganography technologies- Countermeasures. Ethical Hacking terminology

9. Foot printing & Social engineering

Information gathering methodologies- Competitive Intelligence- DNS Enumerations-Social Engineering attacks. Analysis of Deep web/ dark web and silk road analysis.