

**SYLLABUS FOR THE POST OF SCIENTIFIC OFFICERS-  
COMPUTER FORENSIC/MOBILE FORNSIC/AUDIO-VIDEO FORENSIC  
SECTIONS  
FORENSIC SCIENCE LABORATORY-POLICE DEPARTMENT**

**1. Digital Forensic and Cyber Crime:**

Understanding Cyber Crime: Indian IT Act 2008 and amendments, categories of Cyber crimesie., 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. Number Systems and Codes:**

Basic Rules of Binary , Binary Number System, Octal Number System, Hexadecimal Number System, Bits and Bytes , 1's and 2's Complements, Decimal –to- Binary Conversion, Decimal-to- Octal Conversion, Decimal –to-Hexadecimal Conversion, Binary –octal and Octal – Binary Conversions , Hexadecimal – Binary and Binary –Hexadecimal Conversion, Hexadecimal –Octal and Octal –Hexadecimal Conversion.

**3. Boolean algebra and Logic Circuits:**

Definitions, Theorems and Properties of Boolean algebra, Boolean functions, canonical and standard forms, the map method of simplification of boolean functions. Two-Three-Four variable maps, product of Sum simplification, NAND and NOR implementation, don't care conditions, The Tabulation Method, determination and selection of prime implicants

Introduction, design procedure, Adders – binary parallel adder, decimal adder, Subtractor, Code conversion, decoders and multiplexers; Flip Flops, types-SR, JK, D & T, triggering of Flip Flops, Flip flop excitation tables, Registers and types, Counters, Synchronous and Asynchronous Counters

**4. Computer Hardware and Memories:**

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.

**5. Overview of Programming Languages:**

Introduction to programming logic, algorithm, simple types of real integer variables in C. Mathematical representations of C functions. C++ class overview-class definition-objects-class members- access control- constructors and destructors-parameter passing methods-dynamic memory allocation and de-allocation-Function overloading. Introduction to Interpreted Languages and Python - Data Types and variables - Operators and Expressions - Program Structure and Control - Functions and Functional Programming - Classes, Objects and other OOPS concepts

## **6. Working with different kinds of Operating Systems:**

Understanding File Systems, Exploring Microsoft File Structures, Examining NTFS Disks, 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.

## **7. TCP/IP:**

The Internet Protocol (IP), IP packet, IP addressing, subnet mask, classless interdomain routing (CIDR), address resolution, reverse address resolution, IP fragmentation and reassembly, ICMP, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), TCP reliable stream services, TCP operation, TCP protocol, Dynamic Host Configuration Protocol (DHCP), mobile IP, IPv6, Internet routing protocols, routing information protocols, open shortest path first protocol, border gateway protocol, multicast routing, reverse path broadcasting, internet group management protocol, reverse path multicasting, distance vector multicast routing protocol. File system, accessing the world wide web-File systems, hypertext markup language, wireless application protocol, wireless data gram protocol, wireless transaction protocol.

## **8. 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).

## **9. Computer Forensics:**

Evaluating Computer Forensic Tools 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, Hiding Files- Steganography technologies- Countermeasures. Principles of public key cryptosystems-The RSA algorithm-Key management.

## **10. Mobile Phone Forensics:**

Mobile phone data acquisition through logical, physical and file system techniques, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- 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, Mobile application security. Voice, SMS and Identification data interception in GSM, Mobile system architectures.

## **11. Audio/Video Forensics:**

Spectrography – Conversion of different audio 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.

## **12. Ethical Hacking terminology, Foot printing and social engineering:**

Five stages of hacking- Vulnerability Research- Legal implication of hacking- Impact of hacking. System Hacking-Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures. Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks. Analysis of Deep web/ dark web and Silk Road analysis.