SYLLABUS FOR THE POST OF SCIENTIFIC OFFICER-
MOBILE 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.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.

3. 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:

4. Mobile Banking

Mobile Banking Technologies, Mobile Banking services, Applications, Mobile payments –types of mobile payments –mobile phone based, SIM card based, WAP based, mobile wallet, USSD, SEOMPS, Mobile payment service providers –paypal Here, Square, Google wallet, Isis, M-Pesa, MobiPay, NTT DoCoMo (Osaifu-Keitai), Reliance m-pay. Finance and Accounting Mobile Apps –Mint, Expense Manager, Money Lover, ToshI Finance Budget & Expense.

5. REVIEW OF CELLULAR SCHEMES

Model and methodology, mobile computing topologies, networks and protocols, gsm/gprs/3g system architecture, network and switching subsystem, operation subsystem, radio interface, logical channels and frame hierarchy, handover, authentication, encryption , hscsd, umts and imt-2000, umts basic architecture, utra fod mode, utra tdd mode, SDMA, FDMA, TDMA.

6. 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 Data gram Protocol (UDR), 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, wsp/b over wtp, wsp/b as connectionless session service, wireless markup language, WTP class 0, WMLScript

7. INTRODUCTION TO NETWORK SECURITY

Networking Devices (Layer1,2,3)- Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trials) – IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based).VIRTUAL PRIVATE NETWORKS -VPN and its types –Tunneling Protocols – Tunnel and Transport Mode – Authentication Header-Encapsulation Security Payload (ESP)- IPSEC Protocol Suite – IKE PHASE 1, II – Generic Routing Encapsulation(GRE). WAN Topologies- Standard IP based Switching – CEF based Multi-Layer switching-MPLS Characteristics- Frame Mode MPLS Operation – MPLS VPN.

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. NEXT GENERATION INTERNET PROTOCOL

Introduction to IPv6 – IPv6 Advanced Features –V4 and V6 header comparison – V6 Address types –Stateless auto configuration – IPv6 routing protocols – IPv4-V6 Tunnelingand Translation Techniques.

10. Ethical Hacking terminology

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.

11. Foot printing & Social engineering

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

12. PUBLIC KEY CRYPTOGRAPHY

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman, Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography.