Post: Senior Scientific Assistant
Division: Cyber Forensic
Syllabus

1. Computer Fundamental, Operating System and File System

Computer System History and development, Computer Organization and Architecture: Cache memory. Primary and Secondary Storage devices, Input- Output device.
Operating System and File System- Operating system, layered architecture/logical structure of operating system, Types of OS, virtual machine, OS services, Process management, Memory management, Virtual Memory. Overview of operating system in Linux & windows.

File System concepts, naming, attributes, operations, types, structure, file organization & access (Sequential, Direct, Index Sequential) methods, memory mapped files, directory structures.

2. Computer Network and Internet concepts

Introduction of computer networks, Network architecture, Introduction to TCP/IP Model, compare TCP/IP to (OSI) reference model, Network protocol: FTP, Telnet, DNS, DHCP, SNMP, SMTP, POP3 etc. Basic Mobile communication network Model, Wi-Fi network, Bluetooth, Broadband and optical fibre.

Concept of IP address and their version IPv4 and IPv6, Web Hosting Concepts and Domain name Registration Process.

3. Cloud Technology and Cyber Security

Introduction to cloud technology, secure cloud bases services, Cloud based Applications: Facebook, Instagram, Telegram, WhatsApp, Facebook Messenger.

Monitoring computer networks and activities, live packet capturing, network intrusion detection, Types of Network Attack. searching and collection of digital evidence from the network.

Information security concepts, Overview: Background and current scenario, types of attacks, goals for security, E-commerce security, steganography

Security threats and vulnerabilities, overview of security threats, weak/strong passwords, insecure network connections, malicious code, programming bugs, cybercrime and cyber terrorism, information warfare and surveillance, virus, Trojan, worms, botnet, ransomware, shells.

4. Database Management System and Security

Contents of the Subject Introduction: Overview of DBMS, Advantages of DBMS, Basic DBMS terminology,

Data modeling using the Entity Relationship Model: mapping constraints, Generalization, Aggregation, Specialization, Extended ER model, relationships of higher degree

Relational model: Storage Organizations for Relations, Relational Algebra, Set Operations, Relational Calculus, Concepts of Alternate key, candidate key, primary key, Foreign key, Integrity Rules, Data Dictionary.

Normalization: Functional dependencies, normal forms, first, second, third normal forms, BCNF, inclusion dependencies, loss less join decompositions,

Data security policy: database security risks; database security testing; database auditing models and tools; user management strategies; maintenance policy, assessment and (counter) measures.

5. Information System Security and Cryptography

Cryptographic System, Classification of Cryptographic System, Substitution-Permutation Network, Feistel structure, Block Ciphers: DES, Double DES, AES, Stream Ciphers: LFSR, RC4.

Public Key Cryptography, RSA, Discrete Logarithm Problems, Diffie-Hellman, DSA, PKI.

Data Integrity, Hash Functions: MD5, SHA, Message Authentication Codes.

Emerging Application: Email Security, SSL/TLS, Web Security, Access Controls, Malwares, Firewalls, and Intruders. Digital Signature, User authentication - Token based, Biometric, Remote user authentication, Intrusion detection systems, honey pots, Denial of Service.

6. Foundation to Multimedia Forensic and Image Processing

Introduction to digital signals: audio, image and video; Digitization process: sampling and quantization; Image Enhancement Techniques: Spatial and frequency domain; Image Compression Techniques: Introduction, lossy and lossless compression, Run length coding, scalar and vector quantization, JPEG and JPEG 2000 compression techniques; Image description and representation techniques: Introduction, boundary descriptor: chain code and shape number, regional descriptor: color and texture descriptors ; Introduction to pattern clustering and classification.

Basics of Multimedia; Devices for capturing image and video: digital camera and its components, acquisition process of digital image and video; Standards for video transmission; NTSC and PAL.

Image Enhancement in the Spatial Domain: Some Basic Gray Level Transformations, Histogram Processing, Enhancement Using Arithmetic/Logic Operations, Basics of Spatial Filtering, Smoothing

Spatial Filters, Sharpening Spatial Filters, Combining Spatial Enhancement Methods. Image Restoration Filtering, Inverse Filtering ,

Color Fundamentals: Color Models, Pseudo color Image Processing, Basics of Full-Color Image Processing, Color Transformations, Smoothing and Sharpening, Color Segmentation, Noise in Color Images, Color Image Compression.

7. Modern Digital devices and Digital Technologies

Modern digital Devices: Computer, Laptop, tablet, Mobile Phones, POS, ATM machine, Smart watch, Drone, IoT devices.

Crypto Currency, Blockchain Technologies, Cloud computing, Artificial Intelligence, Machine learning, Big Data Analysis, Deep fake video technology, Dark Web, Anonymous browsing techniques.

8. 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, enhancement of video and Authentication of video.

Overview of Computer and DVR forensics software and tools: write blockers, imaging, and cloning devices.

9. Mobile forensics and Mobile technology: H]istory of mobile phones, types of mobile phones, basics of mobile phones and their components, identification of mobile phones, operating systems.

Post: Senior Scientific Assistant
Division: Cyber Forensic

Syllabus

Mobile phone technology: e.g. asynchronous transfer mode (ATM), wireless applications protocols (WAP), advanced mobile phone system (AMPS), time division multiple access (TDMA), Code Division Multiple Access (CDMA) cellular networks: GSM, GPRS, EDGE, UMTS, LTE, VoLTE.

Mobile phone data acquisition by manual, logical, file system extraction and physical, Advanced Acquisition techniques. Overview of mobile forensic software.

10. Cyber Crimes & IT Act:

Cyber space, cyber-crimes and types of cyber-crimes Social media-use and misuse, hacking, unauthorized access, spoofing, phishing, cyber terrorism, cyber stalking, social engineering, DOS and DDOS attack, skimming, financial crimes, identity theft, Trojans, viruses, logic bombs, malware attack.

The Information technology Act 2000 and its amendments. Related and relevant section of IPC, Indian Evidence Act, Indian Telegraph Act.

Search, seizure and Collection of digital evidence, Significance of hash value, chain of custody.

Cell Site Analysis, CDR Analysis, Tower Dump, IP tracing, web domains analysis, IPDR Analysis, Mobile Phone tracing, Email Tracing.