NOTICE

Syllabi for recruitment to the posts of Supervisor Level-I, Expert Level-II and Scientific Examiner in CID, West Bengal for contractual basis.

(Ref. Advertisement No.15/CID/GL-I dated 18/10/2022)

Syllabus for the Interview

1	Supervisor Level - I	**Section (A)** 1. General Aptitude 2. Comprehension **Section (B)** 3. DBMS/RDBMS 4. OS (Windows/Linux) 5. Algorithm / Data Structure 6. Javascript, J-Query, AJAX, JSON 7. HTML 5.0 8. MySQL/PostGreSQL/MongoDB **Section (C)** (Any two of the following) 1. Java (Core Java/Advanced Java/FX/Hibernate/Spring) / Android App development / iOS App Development 2. PHP (CI/Laravel) /Node JS /React JS, CSS 3 3. VB DOT NET / C# 4. Cyber Security (Nmap, Burpsuite, SQL Map, Netstat, Reverse Engg. etc.) / Python, Machine Learning / Digital Forensics 5. Cloud Server Management (AWS, GoDaddy) / Big Data Analysis & Optimisation
2	Expert Level - II	**Section (A)** 1. General Aptitude 2. Comprehension **Section (B)** 3. DBMS/RDBMS 4. OS (Windows/Linux) 5. Algorithm / Data Structure 6. Javascript, J-Query, AJAX, JSON 7. HTML 5.0 8. MySQL/PostGreSQL **Section (C)** (Any two of the following) 1. Java (Core Java/Advanced Java/FX/Hibernate/Spring) / Android App development / iOS App Development

	2. PHP (CI/Laravel) /Node JS /React JS, CSS 3 3. VB DOT NET / C# 4. Cyber Security (Nmap, Burpsuite, SQL Map, Netstat, Reverse Engg. etc.) / VPN / Proxy/ Python, Machine Learning / Digital Forensics 9. Cloud Server Management (AWS, GoDaddy) / Big Data Analysis & Optimisation / Data Centre Management 5. Electronics / Robotics / Mobile Technology

Syllabus on Digital Forensic for selection of "Scientific Examiner"

1. COMPUTER FORENSICS

(a) Introduction to Computer Hardware - Various Components of a Computer, Motherboard, Processor, Memory, Storage Devices and Networking components. Understanding Computer Operating Systems (OS), Booting process of computers. Introduction to File Systems and types of File System.

(b) Cyber Crime- Form of Cyber Crime, Internal and External Attacks, Crimes related to Social Media, ATM and Banking Frauds,Packet sniffing, Spoofing, Web security

(c) First responder - role and toolkit. Procedure for search and seizure of digital evidences. Search and Seizure of Volatile and Non-volatile Digital Evidence. Imaging and Hashing Digital Evidence. Analyzing and Recovery of Deleted, Hidden and Altered files.

(d) Windows Systems Artifacts: File Systems, Registry, Event logs, Shortcut files, Executable. Alternate Data Streams (ADS), Hidden files, Slack Space. Linux System and Artifacts: Linux file system: Ownership and Permissions, Hidden Files, User Accounts and Logs. Mac OS X systems and Artifacts: System Startup and Services, Network Configuration, Hidden Directories, System Logs and User Artifacts

(e) Web Browsers: Cookies, Favourites or Bookmarks, Cache, Session Data and Plugins. Email: Types of Email and Protocols. Analysing the Header details and tracking the email, Spoofed Mails. Virtual Machine and Cloud Technology Forensics.

2. NETWORK FORENSICS

(a) Computer Networking- Digital and Analog Signaling Methods, Network Types and Topologies, Overview of OSI Model and TCP/IP Protocol. Different types of IP Addresses and Classes, Subnet Masks, Sub-netting and Supernetting. Network Hardware Devices and Client/Server Computing. Types of Networks - LAN, MAN and WAN. Routers and Routing Protocols.

(b) Network threat and vulnerabilities, Types of network attacks- eavesdropping, spoofing, modification, Cross-site scripting, DNS Spoofing, Routing Table Page 15 of 48 Poisoning, ARP Poisoning, Web Jacking. Attacks on Wireless Networks. Social Engineering Attacks and its types. Packet Sniffing, Types of authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots.

Syllabus on Digital Forensic for selection of "Scientific Examiner"

(c) IP security architecture, Security protocols, IPSec, Web Security - Firewalls, IDS, IDPS. Network Security Applications, Authentication Mechanisms: Passwords, Cryptographic authentication protocol, Kerberos, X.509 LDAP Directory. Digital Signatures. Web Security: Secure Socket Layer (SSL) Encryption, Transport Layer Security (TLS), Secure Electronic Transaction (SET) and Virtual Private Networks (VPN).

(d) Monitoring of computer network and activities, Live Packet Capturing and Analysis. Searching and collection of evidences from the network. Network Intrusion Detection and Analysis. SQL Injection, Event Log analysis- tools and techniques. Investigating network attacks. Evidence collection from Routers other networking devices.

(e) Cloud Technology and its various components - private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Role of virtualization in enabling the cloud. Technologies and the processes required when deploying web services. Cloud Security Architecture, Secure Cloud based service, Identity and Access Management, Encryption and Key Management. Cloud Forensic - collection and analysis of evidence.

3. MOBILE AND WIRELESS DEVICE FORENSICS

(a) Introduction to Mobile Technologies - Asynchronous Transfer Mode (ATM), Wireless Application Protocol (WAP). Cellular technologies - Advanced Mobile Phone System (AMPS), i-Mode, Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) and relative strengths. Subscriber Identity Module (SIM), International Mobile Equipment Identity (IMEI).

(b) Various Generation of Mobile Phone Technologies. Understanding of the mobile phone operating systems - Android, iOS, Windows. Understanding of SQLite Databases.

(c) Overview of Mobile Forensics, Seizure and Preservation of mobile phones and PDA. Types of Evidence present in mobile phones - Files present in SIM card, external memory dump, and evidences in memory card. Mobile phone evidence extraction process, Data Acquisition Methods - Physical, File System, Logical and Manual Acquisition. Mobile Forensic Investigation Toolkit. Tracking of mobile phone location.

4. SOCIAL MEDIA FORENSICS

(a) Introduction to Social Media, Security Issues in Social Media, Types of crimes of Social Media - Cyberbullying, Online Grooming, Cyberstalking. Emerging Trends in social media,

Syllabus on Digital Forensic for selection of "Scientific Examiner"

(b) Sources for social media evidence, Types of Data Available on Social Networking Sites, Different evidence collection methods from social networking sites, Intelligence gathering from Social Media- Tools and technique for intelligence gathering- indirect method, direct method with login, direct method without login.

5. CRYPTOGRAPHY

(a) Introduction to Cryptography, Symmetric and Asymmetric Cryptosystem Encryption Techniques- Substitutional Cipher and Transpositional Ciphers. Types of keys - Public Key and Private Key. Advanced Encryption Techniques and Security Issues. Various types of attacks including Cipher Text-Only attack, Known-Plaintext Attack, Chosen-Plaintext Attack, Chosen-Cipher text Attack.

(b) Symmetric Cryptosystem - AES, DES, RC4, Blowfish. Asymmetric Cryptosystems - RSA, DSA, Elliptic Curve cryptography. Introduction to Cryptanalysis - Differential and Linear Cryptanalysis. Hashing Algorithms - MD5, SHA-1, SHA-2, SHA-3, One-Way Hash, Hash Message Authentication Code.

6. DIGITAL FORENSIC TOOLS & ITS PROCESS

(a) Phases of Digital Forensics (IPAAD): Identification,Preservation, Acquisition, Authentication, Documentation

(b) Digital evidence & Analysis of Digital Evidence: Preserving the integrity of digital evidence, Admissibility of digital evidence in court of law, Maintaining the chain of custody

(c) Understanding and mastering Forensic tools

(d) Writing an examination report

--------- END ------

29/11/2022