## Syllabus

**Basics of Cyber Forensics**

Unit 1: Digital Investigation - Digital Evidence and Computer Crime - History and Terminology of Computer Crime Investigation - Technology and Law - The Investigative Process -Investigative Reconstruction - Modus Operandi, Motive and Technology -Digital Evidence in the Courtroom.

Unit 2: Understanding information - Methods of storing data: number systems, character codes, record structures, file formats and file signatures - Word processing and graphic file formats - Structure and Analysis of Optical Media Disk Formats - Recognition of file formats and internal buffers - Extraction of forensic artifacts– understanding the dimensions of other latest storage devices – SSD Devices.

Unit 3: Computer Basics for Digital Investigators - Computer Forensic Fundamentals - Applying Forensic Science to computers - Computer Forensic Services - Benefits of Professional Forensic Methodology -Steps taken by computer forensic specialists.

Unit 4: Standards, Guidelines and Best Practices- Handling the Digital Crime Scene - Digital Evidence Examination Guidelines –ACPO – IOCE – SWGDE -DFRWS – IACIS – HTCIA - ISO 27037

Unit 5: Types of Computer Forensics Tools and Technology -Tools and Types of Military Computer Forensics Technology -Tools and Types of Law Enforcement Computer Forensic Technology -Tools and Types of Business Computer Forensic Technology

**Networking and Communication Protocols**

Unit 1 Networking models- OSI Layered model - TCP/IP Model - MAC Address representation - Organisationally Unique Identifier - Internet Protocol - Versions and Header lengths - IP Identification - IP Flags - IP fragmentation and reassembly structure - Transport Layer protocols - Port numbers - TCP Flags - Segmentation - TCP 3 way handshake and Options - encapsulation and De-encapsulation - Payload.

Unit 2 Static and Dynamic Routing - IP Routing Protocols - Classful and Classless Routing - RIPv1 - RIPv2, Broadcast and Multicast domains - OSPF, EIGRP - Network Address Translation - IP Classes - Private IP - Public IP - Reserved IP - APIPA.

Unit 3 Subnetting IP network - Class A, B, C subnetting - Classless Inter-domain Routing (CIDR) - Subnet mask - Wild card mask - WAN Technologies - Frame Relay - Data link Connection Identifiers (DLCI) - Committed Information Rate (CIR) - Permanent Virtual Circuits (PVCs) - Multiprotocol Label Switching (MPLS) - Edge Routers - Label Switching - CE and PE Routers - Data Terminal Equipment (DTE) - Data Communication Equipment (DCE) - Clock speed.

Unit 4 Virutal LANs - Access links and Trunk links - Switchport modes - Vlan Trunking - Server, Client and Transparent modes - VTP Domain - Configuration Revision numbers - Inter Vlan Communications - Broadcast domain - Collision Domain

Unit 5 Communication protocols - Address Resolution Protocol (ARP) - Reverse Address Resolution Protocol (RARP) - Internet Control Message Protocol (ICMP) - Internet Protocol (IP) - Transmission Control Protocol (TCP) - User Datagram Protocol (UDP) - American Standard Code for Information Interchange (ASCII) - Hypertext Transfer Protocol (HTTP) - File Transfer Protocol (FTP) - Simple Mail Transfer Protocol (SMTP) - Telnet - Trivial File Transfer Protocol (TFTP) - Post Office Protocol version 3 (POP3) - Internet Message Access Protocol (IMAP) - Simple Network Management Protocol (SNMP) - Domain Name System (DNS) - DNS Flags - Dynamic Host Configuration Protocol (DHCP).

**Introduction to Information Security**

Unit 1: Overview of Information Security - What is Information and why should be protect it? - Information Security - Threats - Frauds, Thefts, Malicious Hackers, Malicious Code, Denial-of-Services Attacks and Social Engineering - Vulnerability – Types - Risk – an introduction - Business Requirements - Information Security Definitions - Security Policies - Tier1 (Origination-Level), Tier2 (Function Level), Tier3 (Application/Device Level) – Procedures - Standards - Guidelines

Unit 2: Information Asset Classification - Why should we classify information? - Information Asset – Owner, Custodian, User - Information Classification - Secret, Confidential, Private and Public – Methodology - Declassification or Reclassification - Retention and Disposal of Information Assets - Provide Authorization for Access – Owner, Custodian, User

Unit 3: Risk Analysis & Risk Management - Risk Analysis Process - Asset Definition - Threat Identification - Determine Probability of Occurrence - Determine the Impact of the Threat - Controls Recommended - Risk Mitigation - Control Types/Categories - Cost/Benefit Analysis

Unit 4: Access Control - User Identity and Access Management - Account Authorization - Access and Privilege Management - System and Network Access Control - Operating Systems Access Controls - Monitoring Systems Access Controls - Intrusion Detection System - Event Logging - Cryptography

Unit 5: Physical Security - Identify Assets to be Protected - Perimeter Security - Fire Prevention and Detection - Safe Disposal of Physical Assets.

IT Infrastructure and Cloud Computing

Unit 1: Computer Hardware Basics

- Basics of Motherboard including CMOS and BIOS
- Working of processors and types of processors
- System memory
- Introduction to RAM
- System storage devices
    - Types of hard disks - FAT, NTFS, RAID etc.
    - Optical drives

    - Removable storage devices
    - Tape drives and backup systems
- Common computer ports – Serial – Parallel - USB ports etc.
- Different input systems - Key Board - Mouse etc.
- Display arrays – VGA – SVGA – AGP
- Additional display cards
- Monitors and their types
- Printers and their types

Unit 2: Operating Systems

- Operating system basics
    - Functions of operating system
    - Functions of Client Operating System
    - Functions of Server operating system
    - Introduction to Command line operation
- Basics on files and directories
- Details about system files and boot process
- Introduction to device drivers

Unit 3: Computer Principles and a Back Box Model of the PC

- Memory and processor
- Address and data buses
- Stored program concept
- Physical components of the PC and how they fit together and interact
- Basic electrical safety
- Motherboards and the design of the PC
- Dismantling and re-building PCs
- Power On Self Test and boot sequence
    - Architecture of real mode o Interrupts
    - Start of boot sequence
    - Power On Self Test (POST)

Unit 4: Enterprise and Active Directory Infrastructure

- Overview of Enterprise Infrastructure Integration
- Requirement to understand the Enterprise Infrastructure 5
- Enterprise Infrastructure Architecture and it's components
- Overview of Active Directory (AD)
- Kerberos
- LDAP
- Ticket Granting Ticket {TGT}
- Forest

- Domain
- Organization Unit (OU)
- Site Topology of a Forest
- Trust Relationships
- Object – Creation, Modification, Management and Deletion
    - User
    - Group
    - Computer
    - OU
    - Domain
- Group Policy (GPO) Management
    - Structure of GPO
    - Permissions and Privileges
    - GPO Security Settings Password Settings Account Lockout Settings Account Timeout Settings USB Enable/ Disable Settings Screen Saver Settings Audit Logging Settings Windows Update Settings User Restriction Settings
    - Creation of GPO
    - Linking a GPO
    - Application of GPO Linking a GPO Enforcing a GPO GPO Status Inclusion / Exclusion of Users/ Groups in a GPO
    - Precedence of GPO
    - Loopback Processing of GPO
    - Fine-Grain Policy / Fine-Grain Password Policy
- Addition of Windows Workstations to Domain and Group Policy Synchronisation
- Addition of Non-Windows Workstations in AD Environment
- Integrating Finger-Print, Smart Card, RSA or secondary authentication source to Active Directory
- Single-Sign On Integration
- Active Directory Hardening Guidelines

Unit 5: Cloud Computing

- Concept – Fundamentals of Cloud Computing
- Types of clouds
- Security Design and Architecture
- Cloud Computing Service Models
- The Characteristics of Cloud Computing
- Multi Tenancy Model
- Cloud Security Reference Model
- Cloud Computing Deploying Models
- Cloud Identity and Access Management
    - Identity Provisioning – Authentication

- Key Management for Access Control – Authorization
- Infrastructure and Virtualization Security
- Hypervisor Architecture Concerns.

- Understanding Cloud Security
  - Securing the Cloud
  - The security boundary
  - Security service boundary
  - Security mapping
  - Securing Data
  - Brokered cloud storage access
  - Storage location and tenancy
  - Encryption
  - Auditing and compliance
  - Establishing Identity and Presence
  - Identity protocol standards

**Forms of Cyber Crime**

Unit 1: Cyber Crime – Introduction – History and Development – Definition, Nature and Extent of Cyber Crimes in India and other countries - Classification of Cyber Crimes – - Trends in Cyber Crimes across the world.

Unit 2 : Forms of Cyber Crimes , Frauds – hacking , cracking, DoS – viruses, works, bombs, logical bombs, time bombs, email bombing, data diddling, salami attacks, phishing, stegnography, cyber stalking, spoofing, pornography, defamation, computer vandalism, cyber terrorism, cyber warfare, crimes in social media, malwares, adware, scareware, ransomware, social engineering, credit card frauds & financial frauds, telecom frauds. Cloud based crimes – understanding fraudulent behaviour, fraud triangle, fraud detection techniques, Intellectual Property Rights and Violation of Intellectual Property rights, Ecommerce Frauds and other forms.

Unit 3 : Modus Operandi of various cybercrimes and frauds – Definition of various types of cyber frauds – Modus Operandi - Fraud triangle – fraud detection techniques including data mining and statistical references - countermeasures.

Unit 4: Profile of Cyber criminals – Cyber Crime Psychology – Psychological theories dealing with cyber criminals

Unit 5: Impact of cybercrimes – to the individual, to the corporate and companies, to government and the nation.

**Network Security and Cryptography**

Unit 1 Network Security - The CIA Triad - DAD - Internet Key Exchange (IKE) - Internet Protocol Security (IPSec) - AH and ESP Header - Security Associations - Transport Layer Security (TLS) - Secure Electronic Transaction (SET) - Extensible Authentication Protocol (EAP) - Protected Extensible Authentication Protocol (PEAP) - Lightweight Extensible

Authentication Protocol (LEAP) - Secure Multipurpose Internet Mail Extensions (S/MIME) - Pretty Good Privacy (PGP).

Unit 2 Point-to-Point Protocol (PPP) - Challenge Handshake Authentication Protocol (CHAP) - Password Authentication Protocol (PAP) - High Level Data link Control (HDLC) - Remote Authentication Dial-In User Service (RADIUS) - Terminal Access Controller Access-Control System (TACACS+) - Tunneling Protocols in the Data Link Layer - Layer 2 Forwarding (L2F) - Layer 2 Tunneling Protocol (L2TP) - Point-to-Point Tunneling Protocol (PPTP)

Unit 3 Security Threats and Vulnerabilities - Virus - Trojan - Rootkits - Backdoors - Botnets - Man in the middle attack - Dos and DDos - Replay attack - Spoofing - Spam - Phishing - privilege escalation - DNS poisoning - Brute force - Dictionary attack - Cross-site scripting - SQL injection - Zero-day attack - Session hijacking - Vulnerability scanning vs Port Scanning - Honeypots - Banner grabbing - Social Engineering.

Unit 4 Cryptology - Cryptosystems - Symmetric vs asymmetric cryptosystem, Goals of Cryptographhy - Confidentiality, Integrity and Non-repudiation - Ciphers, (Block ciphers and stream ciphers), Transposition Ciphers - Substitution Ciphers - One-Time Pads - Codes vs. Ciphers - Cryptographic keys, - Hashing Algorithms - IPSec - AH and ESP - Security Associations - ISAKMP. Wireless Network security, WEP, WPA, WPA2, TKIP - CCMP.

Unit 5 Symmetric Key Algorithms - Data Encryption Standard (DES) - DES Keys - DES Algorithm - Electronic Codebook Mode - Cipher Block Chaining Mode - Cipher Feedback Mode - Output Feedback Mode - Counter Mode - Triple DES (3DES) - DES Variants - DES-EEE3 - DES-EDE3 - DES-EEE2 - DES-EDE2 - International Data Encryption Algorithm (IDEA) - Blowfish - Skipjack - Advanced Encryption Standard (AES) - CAST - Password hashes and Salting - Asymmetric Key Algorithms - RSA - Diffie-Hellman - Private key and Public key - Digital Signature - Public Key Infrastructure (PKI) - Certificate Authorities - Certification Revocation List (CRL) - Digital Signature.

**Advanced Cyber Forensics**

Unit 1: Windows Forensics

- Volatile Data Collection
    - Memory Dump
    - System Time
    - Logged On Users
    - Open Files
    - Network Information (Cached NetBIOS Name Table)
    - Network Connections
    - Process Information
    - Process-to-Port Mapping
    - Process Memory
    - Network Status
    - Clipboard Contents

    - Service / Driver Information
    - Command History
    - Mapped Drives
    - Shares
- Non-Volatile Data Collection
    - Disk Imaging (External Storage such as USB and Native Hard Disk)
    - Registry Dump
    - Event Logs
    - Devices and Other Information
    - Files Extraction
    - Write-Blocking port
- Registry Analysis
- Browser Usage
- Hibernation File Analysis
- Crash Dump Analysis
- File System Analysis
- File Metadata and Timestamp Analysis
- Event Viewer Log Analysis
- Timeline Creation
- Evidence Collection in Linux and Mac Operating system

Unit 2: Network Forensics

- Understanding Protocols with Wireshark
    - TCP
    - UDP
    - HTTP(S)
    - SSH
    - Telnet
    - SMTP
    - POP / POP3
    - IMAP o
    - FTP
    - SFTP
    - ARP
- Packet Capture using Wireshark, tshark and tcpdump
- Packet Filtering
- Extraction of Data from PCAP file
- Netflow vs Wireshark
- Analysis of logs
    - CISCO logs
    - Apache Logs
    - IIS Logs
    - Other System Logs

Unit 3: Memory Forensics

- History of Memory Forensics
- x86/x64 architecture
- Data structures
- Volatility Framework & plugins
- Memory acquisition
- File Formats – PE/ELF/Mach-O
- Processes and process injection
- Windows registry
- Command execution and User activity
- Networking; sockets, DNS and Internet history
- File system artifacts including $MFT, shellbags, paged memory and advanced registry artifacts
- Related tools – Bulk Extractor and YARA
- Timelining memory
- Recovering and tracking user activity
- Recovering attacker activity from memory
- Advanced Actor Intrusions

Unit 4: Virtual Machine Forensics

- Types of Hypervisors
- Hypervisor Files and Formats
- Use and Implementation of Virtual Machines in Forensic Analysis
- Use of VMware to establish working version of suspect's machine
- Networking and virtual networks within Virtual Machine
- Forensic Analysis of a Virtual Machine
    - Imaging of a VM
    - Identification and Extraction of supporting VM files in the host system
    - VM Snapshots
    - Mounting Image
    - Searching for evidence

Unit 5: Cloud Forensics

- Introduction to Cloud computing
- Challenges faced by Law enforcement and government agencies
- Cloud Storage Forensic Framework
    - Evidence Source Identification and preservation in the cloud storage o
    - Collection of Evidence from cloud storage services
    - Examination and analysis of collected data Cloud Storage Forensic Analysis Evidence Source Identification and Preservation Collection of evidence from cloud storage devices Examination and analysis of collected data
- Dropbox analysis:
    - Data remnants on user machines

- Evidence source identification and analysis - Collection of evidence from cloud storage services
- Examination and analysis of collected data –

- Google Drive:
  - Forensic analysis of Cloud storage and data remnants
  - Evidence source identification and analysis - Collection of evidence from cloud storage services
  - Examination and analysis of collected data –
  - Issues in cloud forensics.

**Cyber Laws and Intellectual Property Rights**

Unit 1: Fundamentals of Cyber Law

- Introduction on cyber space
- Jurisprudence of Cyber Law
- Scope of Cyber Law
- Cyber law in India with special reference to Information Technology Act, 2000 (as amended) and Information Technology Act, 2008.

Unit 2: E- Governance and E – Commerce

- Electronic Governance
- Procedures in India
- Essentials & System of Digital Signatures
- The Role and Function of Certifying Authorities
- Digital contracts
- UNCITRAL Model law on Electronic Commerce
- Cryptography – Encryption and decryption

Unit 3: Cyber Crimes Investigation

- Investigation related issues
- Issues relating to Jurisdiction
- Relevant provisions under Information Technology Act, Evidence Act

Unit 4: Trademark, Copyright and Patent laws

- Definitions and concepts
- Trademark
  - Introduction to Trademarks
  - Functions and types of Trademarks
  - Madrid Agreements
  - Trademarks Law Treaty (Geneva)
  - Indian Trademark Act
  - Registration of Trademarks
  - Rights conferred by Registration of Trademarks
  - Infringement of Registered Trademark
  - Defenses

- Trademarks dilution
- International Applications and Case Studies

- Copyright
  - Basics
  - Copyright Law
  - Terms of Copyright
  - Registration of Copyrights
  - Transfer of Ownership of Copyright
  - Infringement Liability Exemptions Defenses Case Studies Copyrights Laws in India

**Application Security**

Unit 1: Application Types

- Client/Server Applications
- Components of Client/Server Applications (Logical & Physical Architecture)
- Web Applications
  - About Web Applications
  - Technologies used to create Web Applications
  - Components of Web Application Architecture
- Data Warehouse Applications
  - About DW Applications
  - Uses
  - Physical & Logical Architecture
- Management Information Systems

Unit 2: Web application security

- Introduction to web application
  - Primer
  - OWASP Top 10 vulnerabilities
  - Mitigation techniques
- Web Application Security Fundamentals
  - What Do We Mean By Security?
  - The Foundations of Security
  - Threats, Vulnerabilities, and Attacks Defined
  - How to Build a Secure Web Application
- Secure Your Network, Host, and Application
  - Securing Your Network
  - Network Component Categories
  - Securing Your Host
  - Host Configuration Categories
- Securing Your Application
  - Application Vulnerability Categories
  - Security Principles

Unit 3: Threats and Countermeasures

- Overview : Anatomy of an Attack
  - Survey and Assess
  - Exploit and Penetrate
  - Escalate Privileges
  - Maintain Access
  - Deny Service
- Understanding Threat Categories
  - STRIDE
  - STRIDE Threats and Countermeasures
- Network Threats and Countermeasures
  - Information Gathering
  - Sniffing
  - Spoofing
  - Session Hijacking
  - Denial of Service
- Host Threats and Countermeasures
  - Viruses, Trojan Horses, and Worms
  - Foot printing
  - Password Cracking
  - Denial of Service
  - Arbitrary Code Execution
  - Unauthorized Access
- Application Threats and Countermeasures
  - Input Validation
  - Buffer Overflows
  - Cross-Site Scripting
  - SQL Injection
  - Canonicalization
- Authentication
  - Network Eavesdropping
  - Brute Force Attacks
  - Dictionary Attacks
  - Cookie Replay Attacks
  - Credential Theft
- Authorization
  - Elevation of Privilege
  - Disclosure of Confidential Data
  - Data Tampering
  - Luring Attacks
- Configuration Management
  - Unauthorized Access to Administration Interfaces
  - Unauthorized Access to Configuration Stores

    - Retrieval of Plaintext Configuration Secrets
    - Lack of Individual Accountability
    - Over-privileged Application and Service Accounts
- Sensitive Data
    - Access to Sensitive Data in Storage
    - Network Eavesdropping
    - Data Tampering
- Session Management
    - Session Hijacking
    - Session Replay
    - Man in the Middle Attacks
- Cryptography
    - Poor Key Generation or Key Management
    - Weak or Custom Encryption
    - Checksum Spoofing
- Parameter Manipulation
    - Query String Manipulation
    - Form Field Manipulation
    - Cookie Manipulation
    - HTTP Header Manipulation
- Exception Management
    - Attacker Reveals Implementation Details
    - Denial of Service
- Auditing and Logging
    - User Denies Performing an Operation
    - Attackers Exploit an Application Without Leaving a Trace
    - Attackers Cover Their Tracks

Unit 4: Mobile application security

- Mobile Platforms
    - Top issues facing mobile devices
    - Secure Mobile application development
    - Android security
    - iOS Security
    - Windows, Blackberry & Java Mobile Security
    - Symbian OS security
    - Web OS security
    - WAP and mobile HTML Security
    - Blue tooth security
    - SMS Security
    - Mobile Geo location
    - Enterprise Security on Mobile OS
    - Mobile Malwares
    - Mobile security penetration security

- Encryption and authentications
- Mobile privacy concerns

Unit 5: Threat Modeling

- Overview
- Threat Modeling Principles
  - The Process
  - The Output
- Step 1. Identify Assets
- Step 2. Create an Architecture Overview
  - Identify What the Application Does
  - Create an Architecture Diagram
  - Identify the Technologies
- Step 3. Decompose the Application
  - Identify Trust Boundaries
  - Identify Data Flow
  - Identify Entry Points
  - Identify Privileged Code
  - Document the Security Profile
- Step 4. Identify the Threats
  - Identify Network Threats
  - Identify Host Threats
  - Identify Application Threats
  - Using Attack Trees and Attack Patterns
- Step 5. Document the Threats
- Step 6. Rate the Threats
  - Risk = Probability * Damage Potential
  - High, Medium, and Low Ratings
  - DREAD

Unit 6: Application security standards and checklist

- Application security checklist NIST
- OWASP security checklist
- OWASP Application Security Verification Standard

**Introduction to Data Privacy**

Unit 1: Introduction to Privacy Data Protection & Privacy Terminologies - Data Protection Principles and Approaches to Privacy - Code for protection of Personal Information - Information Life Cycle -Data Security Threats and Mitigation - Data Storage Security Issues in Cloud Computing

Unit 2: Data protection principles and Safeguards Data protection principles - Subject access request Damage or distress - Preventing direct marketing Automated decision taking - Correcting inaccurate personal data - Compensation, Exemptions & Complaints - Big data -

CCTV & Data sharing - Online & apps Privacy by design - Guidance Note on Protecting the confidentiality of Personal Data - Safeguarding Personal Information - Using Personal Information on Websites and with Other Internet related Technologies - Privacy considerations for sensitive online information, including policies and notices, access, security, authentication identification and data collection. - Data Privacy in online data collection, email, searches, online marketing and advertising, social media, online assurance, cloud computing and mobile devices.

Unit 3: Data Privacy Management Data Privacy Management controls & Plan - Data Privacy Management Reference Model – ISTPA - Data Protection in the context of Police and Criminal Justice - Cross Border data transfer - Do not Track Privacy Policy - Developing Privacy Management Tools - Information security practices for data privacy - Developing a privacy management plan - Rights of the Data Subject - Documenting the privacy baseline of the organization - Data processors and third-party vendor assessments - Physical assessments; mergers, acquisitions and divestures - Privacy threshold analysis; privacy impact assessments - Privacy Monitoring and Incident Management (MIM) - Auditing your privacy program; creating awareness of the organization's privacy program; Compliance monitoring; handling information requests; and handling privacy incidents.

Unit 4: Privacy Program Governance and Compliance and Legal Framework Privacy Organization and Relationship (POR) - Privacy Policy and Processes (PPP) - Regulatory Compliance Intelligence (RCI) - Privacy legislations - applicability and interpretation - Privacy Awareness and Training (PAT) – Legal Framework for Data protection, Security and Privacy Norms

Unit 5: Privacy in cloud computing and IOT Privacy in Cloud _ Introduction to Privacy in cloud computing - Cloud computing paradigm and privacy - Challenges to privacy in cloud computing - Privacy in IoT - IoT Governance - IoT Security & Privacy Issues - IoT Privacy challenges - IoT Privacy solutions