MIT(CS)-202

Digital Forensics

BLOCK-I

UNIT I: INTRODUCTION TO DIGITAL FORENSIC

INTRODUCTION, Definition of Computer Forensics, Cyber-crime, Computer based crime, Computer facilitated crime, EVOLUTION OF COMPUTER FORENSICS, STAGES OF COMPUTER FORENSICS PROCESS, BENEFITS OF COMPUTER FORENSICS, USES OF COMPUTER FORENSICS, OBJECTIVES OF COMPUTER FORENSICS, ROLE OF FORENSICS INVESTIGATOR, FORENSICS READINESS, What is Forensics Readiness?, Goals of Forensic Readiness, Benefits of Forensic Readiness, Steps for Forensic Readiness Planning.

UNIT II: COMPUTER FORENSICS INVESTIGATION PROCESS

INTRODUCTION TO COMPUTER CRIME INVESTIGATION, Initial Decision-Making Process, ASSESS THE SITUATION, Notify Decision Makers and Acquire Authorization, Review Policies and Laws, Identify Investigation Team Members, Conduct a Thorough Assessment, Prepare for Evidence Acquisition, ACQUIRE THE DATA, Build Computer Investigation Toolkit, Preparing Your Organization for a Computer Investigation, Collect the Data, Store and Archive, ANALYZE THE DATA, Analyze Network Data, Analyze Host Data, Analyze Storage Media, REPORT THE INVESTIGATION, Gather and Organize Information.

UNIT III: DIGITAL EVIDENCE AND FIRST RESPONDER PROCEDURE

DIGITAL EVIDENCE, Locard’s Principle, Best Evidence Rule, Characteristics of Digital Evidence, Stages in Digital Evidence Investigation Process, FIRST RESPONDER TOOLKIT, Some Common Mistakes First Responder should avoid, ISSUES FACING COMPUTER FORENSICS, Technical issues, Legal issues, Administrative issues, TYPES OF INVESTIGATION, Criminal forensics, Intelligence gathering, Electronic discovery (eDiscovery), Intrusion investigation, TECHNIQUES OF DIGITAL FORENSICS, Cross-drive analysis, Live analysis, Volatile data, Recovery of Deleted files, Stochastic forensics, Steganography.

UNIT IV: UNDERSTANDING STORAGE MEDIA AND FILE SYSTEM

HARD DISK DRIVE, Working, Interface, DETAILS OF INTERNAL STRUCTURE OF HDD, Low-Level Formatting, High-level formatting, Glossary of some important terms, Slack space, Lost Cluster, Bad Sector, Master Boot Record, THE BOOTING PROCESS, Linux Boot Process, Mac OS Boot Sequence, Boot Sequence in Windows 7, FILE SYSTEM, Some Common File systems, FAT, NTFS, ext2, ext3 and ext4, XFS, ZFS, BTRFS, Types of file systems, Disk file systems, Flash file systems, Tape file systems, Database file systems, Transactional file systems, Network file systems, Shared disk file systems, Special file systems, Minimal file system / audio-cassette storage, Flat file systems.

BLOCK-II

UNIT I: WINDOWS FORENSICS

INTRODUCTION, Background and need for Window forensics, Major forensic areas in windows, Volatile information, Non Volatile information, RECOVERING DELETED FILES AND PARTITIONS, Anatomy of a disc drive, Data organization in Windows, Retrieving deleted files, Retrieving cached files, Retrieving files in unallocated space, MORE ABOUT RECOVERING LOST FILES/DATA, Slack space, swap file, deleted files, Slack Space, Swap space, File Carving, Event logs.

UNIT II: LOGS & EVENT ANALYSIS AND PASSWORD CRACKING

INTRODUCTION, WINDOWS REGISTRY, Registry and forensics, System information, WINDOWS EVENT LOG FILE, Windows Event Log File Format, Reading from an Windows event log file, Using Microsoft log parser, Understanding Windows user account management logs, Understanding Windows file and other object Access sets, Auditing policy change, WINDOWS PASSWORD STORAGE, SAM, Removing LM hash, Related attacks, AD, APPLICATION PASSWORDS CRACKERS, Password cracking methods, Brute force attack, Dictionary attack, Syllable attack, Rule Based Attack, Hybrid attack and password guessing, Rainbow Attacks, System passwords, Tools for passwords cracking, CMOSPwd, ERDCommander, Office pwd recovery, Passware kit, PDF Password Crackers.

UNIT III: NETWORK FORENSICS

INTRODUCTION, NETWORK COMPONENTS AND THEIR FORENSICS IMPORTANCE, Host, Node, Router, Switch, Hub, Network interface card (NIC), OSI, OSI model, TCP/IP Layers, FORENSICS INFORMATION FROM NETWORK, Intrusion detection/ prevention system, Wireless Access Points, LOG ANALYSIS, Analyzing time stamps, Analyzing data, FORENSICS TOOLS, Network tools used for forensics, Software tools used for network forensics.

UNIT IV: WIRELESS ATTACKS

INTRODUCTION, WIRELESS FIDELTY (WI-FI)(802.11), Capturing 802.11 frames, WIRELESS SECURITY, Attacks, WIRELESS ATTACKS DETECTION TECHNIQUES, Wireless Access Point Monitoring, Wireless Client/Node Monitoring, General Wireless Traffic Monitoring, WIRELESS INTRUSION DETECTION SYSTEMS, Snort-wireless, WIDZ, Bro

BLOCK III

UNIT I: INVESTIGATING WEB ATTACKS

INTRODUCTION, Cyber-attack, Cyber Warfare and cyber terrorism, TYPES OF WEB ATTACKS, Spoofing, Email spoofing, Website spoofing, Repudiation, Privacy attack, Denial of Service, Privilege escalation, SQL Injection Attacks, WEB ATTACK FORENSICS, Web services forensics, Web Application Forensics, Preliminary Analysis, Application Forensics Readiness, Methodology, Website traffic analysis, WEB APPLICATION FORENSICS TOOLS, Logparser, EventLog Analyzer, Web log analyzer, Open Web Analytics8, Webalizer.

UNIT II: INVESTIGATING EMAIL ATTACKS

INTRODUCTION, Email Structure, Types of email services, Web-based email, POP3 email services, The Internet Message Access Protocol (IMAP), MAPI email servers, Simple Mail Transfer Protocol, EMAIL ATTACKS AND CRIMES, Flaming, Email spoofing, Email bombing, Email hacking, Spams, Phishing, Email fraud, Phishing emails, PRIVACY IN EMAILS, Email privacy, Email tracking, EMAIL FORENSICS, Forensically important email parts, Email forensics investigation, Analyzing an email, Instant Messages, EMAIL FORENSIC TOOLS, eMailTrackerPro, Online EMailTracer.

UNIT III: MOBILE DEVICE FORENSICS

INTRODUCTION CHALLENGES IN MOBILE FORENSICS, MOBILE COMMUNICATION, 802.11 or WiFi, Bluetooth, Infrared (IrDA), EVIDENCES IN A MOBILE DEVICE, Service provider logs, Subscriber identification module, Mobile Logs, Phone books/contact lists, Text messages, Application files, MOBILE FORENSIC PROCESS, Seizure, Acquisition, Examination and Analysis, FORENSIC ACQUISITION TOOLS, Hardware acquisition tools, Software acquisition tools.

UNIT IV: INVESTIGATIVE REPORTS, EXPERT WITNESS AND CYBER REGULATIONS

INTRODUCTION, REPORT PREPARATION, Gathering the data, Analyzing the results, Outlining and organizing the report, Writing and Revising a Rough Draft, Expert Witness, Finding an expert, Testifying v. Consulting, What Can (and Can’t) an Expert Do?, Why Use an Expert, LEGAL ASPECTS OF COMPUTING, Jurisdiction, Net neutrality, Open Internet, Indian Information Technology Act(IT Act) 20006, Against Individual, Individual Property, Against Organisation, Against Society at Large, Amendments– Indian IT Act (2008).