MTCF – 201 Digital Forensics

Unit-1 Digital forensic

Computer forensics and investigations as a profession, Understanding computer forensics, computer forensics versus other related disciplines, A brief History of computer Forensics, Understanding case laws, Developing computer forensics resources, Preparing for computer investigations, Understanding law enforcement agency investigations, Following the legal process, Understanding corporate investigations, Establishing company policies, Displaying warning Banners.

UNIT – II Windows Systems and artifacts

Windows Systems and Artifacts:Introduction, Windows File Systems, File Allocation Table, New Technology File System, File System Summary, Registry, Event Logs, Prefetch Files, Shortcut Files, Windows Executables.

UNIT – III Linux Systems and artifacts

Linux Systems and Artifacts:Introduction, Linux File Systems, File System Layer, File Name Layer , Metadata Layer, Data Unit Layer, Journal Tools, Deleted Data, Linux Logical Volume Manager, Linux Boot Process and Services, System V , BSD, Linux System Organization and Artifacts, Partitioning, File system Hierarchy, Ownership and Permissions, File Attributes, Hidden Files, User Accounts , Home Directories, Shell History GNOME Windows Manager Artifacts, Logs, User Activity Logs, Syslog, Command Line Log Processing, Scheduling Tasks.

UNIT – IV Current Computer Forensics Tools

Evaluating Computer Forensics Tool Needs, Types of Computer Forensics Tools, Tasks Performed by Computer Forensics Tools, Tool Comparisons, Other Considerations for Tools, Computer Forensics Software Tools, Command-Line Forensics Tools, UNIX/Linux Forensics Tools, Other GUI Forensics Tools, Computer Forensics Hardware Tools, Forensic Workstations, Using a Write-Blocker.

Unit-V Identification of data

Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats ,Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime ,Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks ,Router Forensics. Cyber forensics tools and case studies.

References:

1. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress imprint of Elsevier.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Fourth Edition, Course Technology.
3. Angus M.Marshall, “Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008.

w.e.f. July-2013

MTCF – 202 Computer Forensics Analysis and Investigations

Unit-I Computer forensics analysis

Determining what data to collect and analyze. Addressing data hiding techniques, Hiding partitions, Marking bad cluster, Bit –shifting, using steganography to hide data, Examining encrypted files, Recovering Passwords, Performing Remote Acquisitions, Remote Acquisitions with Runtime Software.

Unit-II Recovering graphics files

Understanding vector Graphics, Understanding graphics file formats .Lossless and lossy compression. Identifying graphics file fragments, Repairing Damaged Headers, Searching for and carving data from unallocated space. Understanding steganography in graphics files. Using steganalusis tools. Understanding copyright issues with graphics.

Unit-III Virtual Machines, Network forensics, and Live Acquit ions

Performing live acquit ions, Performing a live acquit ion in windows, Developing standard procedures for network forensics, Reviewing network logs. Using network tools, using Unix/Linux tools. Using packet sniffers, examining the honey net projects.

Unit-IV E-Mail Investigation

Exploring the role of email investigation, Exploring the role of client and server in email, Investigating E-mail crimes and violations, Examining E-mail Messages, Viewing E-mail headers, Examing E-mail headers, Examining additional E-mail files. Tracing an e-mail message, Using network E-mail logs, Understanding E-mail servers, Examining Unix e-mail server logs, Examining Microsoft email server logs.

Unit-V Cell phone and mobile device forensics

Understanding mobile device forensics, Mobile phone basics, inside mobile devices, inside PDAs, Understanding acquisition procedures for cell phones and mobile devices, Mobile forensics equipment.

Consultant books:

1. Bill Nelson,Amelia Phillips,Christopher Steuart,"Guide to Computer Forensics and Investigations", Fourth Edition,Course Technology.
2. Angus M.Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.

MTCF – 203 File System Forensic Analysis

Unit 1

Digital investigation foundation - Digital investigations and evidence, Digital crime scene investigation process, Data analysis, overview of toolkits, Computer foundations - Data organizations, booting process, Hard disk technology, Hard disk data acquisition.

Unit 2

Volume Analysis - introduction, background, analysis basics, PC based partitions- DOS partitions, Analysis considerations, Apple partitions, removable media, Server based partitions- BSD partitions, Sun Solaris slices, GPT partitions, Multiple disk volumes- RAID, Disk Spanning.

Unit 3

File system analysis- What is a file system, File system category, Content category, Metadata category, File name category, Application category, Application-level search techniques, Specific file systems, FAT concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. FAT data structure- Boot sector, FAT 32 FS info, FAT, Directory entries, Long file name directory entries.

Unit 4

NTFS concepts- Introduction, Everything is a file, MFT concepts, MFT entry attribute concepts, Other attribute concepts, Indexes, Analysis tools, NTFS Analysis- File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures, File system metadata files.

Unit 5

Ext2 and Ext3 concepts- File system category, Content category, Metadata category, File name category, Application Category. Ext2 and Ext3 data structures-Super block, group descriptor tables, Block bitmap, Inodes, Extended attributes, Directory Entry, Symbolic Link, Hash trees, Journal data structures, UFS1 and UFS2 concepts and analysis - Introduction, File system category, Content category, Metadata category, File name category, UFS1 and UFS2 data structures- UFS1 superblock, UFS2 superblock.

Textbooks:

1. File System Forensic Analysis – Brian Carrier, Addison Wesley, 2005
2. Digital Evidence and Computer Crime- Casey, Eoghan , edition 2, Academic Press, 2004.
3. Computer Forensics- Kruse, Warren and Jay Heiser, Addison Wesley, 2002.

MTCF – 204 Cyber Crime & Information Warfare

UNIT-I

Introduction of Cyber Crime, Categorizing Cybercrime, Cybercrime Theory, Criminology perception of cyber criminals: hackers, computer intrusions and Attacks, Privacy, surveillance and protection, hiding crimes in cyberspace, cryptography, hacking vs cracking, privacy and security at risk in the global information society.

UNIT-II

Introduction to IT Law and Cyber Crime, Social Engineering, Legal system of information technology, Cyber Security, Information Warfare- concept, information as an intelligence weapon, attacks and retaliation, attack and defense.

UNIT-III

An I-War risk analysis model, implication of I-WAR for information managers, Perceptual Intelligence and I-WAR, cyber pornography, Software piracy, Intellectual property right

UNIT-IV

Handling Cyber Terrorism and information warfare. Crime against person.

UNIT-V

Web defacements and semantic attacks, DNS attacks cyber Law Industrial espionage and cyber terrorism.

Books Recommended:

1) William Hutchinson Mathew Warren;Information Warfare: *"Corporate attack and defense in digital world"*; Elsevier

2) Kaufman, Pearlman and Speciner; *"Network Security"*; Pearson Education. 1995

MTCF – 205 Mobile Device Security and Forensics

Unit-I

Overview of wireless technologies and security: Basic cellular network fundamentals, Components of a cellular system, GSM, CDMA, Common Wi-Fi security recommendations, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.

Unit-II

Guidelines on cell phone forensics: Cellular network characteristics, Mobile phone characteristics, Memory configuration in mobile device, Identity module characteristics, Forensic tools, Procedures and principles, Preservation, Acquisition, Examination and analysis

Unit-III

Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues

Unit-IV

Mobile phone forensics: crime and mobile phones, evidences, 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, Android forensic techniques

Unit-V

Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination- Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

References

1. Gregory Kipper, "*Wireless Crime and Forensic Investigation*", Auerbach Publications, 2007
2. Iosif I. Androulidakis, *"Mobile phone security and forensics: A practical approach"*, Springer publications, 2012
3. Andrew Hoog, "*Android Forensics: Investigation, Analysis and Mobile Security for Google Android*", Elsevier publications, 2011
4. Angus M.Marshall, *"Digital forensics: Digital evidence in criminal investigation"*, John – Wiley and Sons, 2008
5. Rick Ayers, Sam Brothers, Wayne Jansen "Guidelines on Mobile Phone Forensics", NIST