CERTIFICATE COURSE IN CYBER FORENSICS

Detailed Curriculum

Name of Unit of Qualification : **CYBER CRIME, INDIAN IT AMENDMENT) ACT 2008 AND INTRODUCTION TO COMPUTER FORENSICS**

Duration : **120 Hours**

Topics : **CYBER CRIME, INDIAN IT (AMENDMENT) ACT 2008 AND INTRODUCTION TO COMPUTER FORENSICS**

Performance Criteria(OUTCOME) No.	Contents	Hrs.
Familiarization with Cyber Crime	• Categorization of cybercrimes,Security policy violations,Online financial frauds,Elaboration of cyber crimes with techniques used by the cyber criminals • Phishing, Cyber-stalking, Cyber HarassmentCyber Frauds, • Tampering with computer source documents,Hacking with computer system,Publishing of obscene information in Electronic form • Hands on Lab	20
Indian Cyber Laws	• Indian IT (Amendment) Act 2008,Objective, Applicability, and Jurisdiction;Various Cyber crimes under Sections 43 (a) to (j), 43A, 65, 66, 66A to 66F, 67, 67A, 67B, 70, 70A, 70B, 80, etc . along with respective penalties,Punishment and fines;Protected System,Penalty for misrepresentation,Breach of Confidentiality and privacy Penalty for publishing false Digital certificate, Publications for fraudulent purpose, Offences or contravention committed outside India • Hands on Lab	30
Introduction to FileSystem	• Architecture ,Importance of File systems, Windows file structure FAT, NTFS, Unix File Systemext2, ext3 • Hands on Lab	15
Awareness with Data Storage devices	• Optical, magnetic, semiconductor, etc. and their interfaces with a computer system, IDE, SATA, SCSI; CD/DVD, • Physical characteristics of Hard Disks sectors, clusters,	20

	cylinders, heads,formatting of Hard Disks, RAID Storage • Hands on Lab	
Different Data Hiding techniques	• Swap Files,Slack space ,Unallocated and allocated space, • Alternative data streams (ADS) • Hands on Lab	10
Introduction to Computer Forensics	• Introduction, Need of computer forensic investigation of the cyber crimes,Forensic investigation process, • Identification, seizing, imaging and analysis of digital evidence, • Report preparation • Hands on Lab	10
FirstResponder	• Role of a First Responder, • First Responder's Toolkit, • Use of digital camera with date &time imprint • First Responder's logbook, Common Mistakes by a First • Responder, • Do's and don'ts for the First Responder at the site of • cyber crime • Hands on Lab	10

Name of Unit of Qualification : Seizure & Imaging of Digital Evidence

Duration : 120 Hours

Topics : Seizure & Imaging of Digital Evidence

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
Digital Evidence	• Handling of digital evidence at the site of the crime, • Basic rules of digital evidence; • Safe & secure packing and transportation of digital evidence to a computer forensic laboratory, • Antistatic PVC covers, air bubble PVC covers, chain of custody forms • Hands on Lab	30
Volatile & non volatile digital evidence	• Volatile data, order of volatility, • Importance of volatile data, • Collecting Volatile Data, • Acquisition of RAM data and the tools to capture, • Steps to image the volatile data (RAM) and other volatile data from a live system, tools - dd, windd, FTK Imager • Hands on Lab	30
Seizing & Imaging of Non-volatile Data	• Disk imaging software tools & hardware equipments, • Imaging vs copying of digital evidence, • legal reasons for using an "image" and not a "copy" of the digital evidence for analysis; • Steps to image the non-volatile data; • Forensic boot CD/DVD, various methodologies to image the non-volatile data in different circumstances, • Dead & Live Acquisition of digital evidence, imaging of virtual systems • Hands on Lab	40
Integrity verification Methods	• Wiping of data in storage devices, • Data/disk wiping tools, • Write blockers, their need, • Software and hardware based write blockers, • Integrity verification of digital evidence using hashing algorithms md5 and shal, tools for generating md5 &shal checksums / hash values • Hands on Lab	20

Name of Unit of Qualification : Analysis of Digital Evidence
Duration : 120 Hours
Topics : Analysis of Digital Evidence

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
Recovery of data	• Deleted files, • Recovery of data from the hard disk, • Damaged FAT, • Using of file carving tools • Hands on Lab	20
Evidence	• Methodology of analysis, • Preparation & updation of the list of relevant keywords, • Their search, timeline of files usage, • Analysis of RAM data to find user-ids, passwords, etc., • Analysis of CD/DVD and other memory cards, • Tool LiveView, • Booting the system using the forensic image of a system using Liveview • Hands on Lab	10
Analysis of media files	• Analysis of media files headers, • Manual analysis of graphics, audio,Video files; • Steganography in media files, • Process of hiding of data / data files in media files, • Steganalysis tools, • Steganographic detection • Hands on Lab	10
Log analysis	• Role of logs in forensic analysis, • Access logs from various sources, • Log analysis tools, • Analysis of logs using log analysis tools and manually • Hands on Lab	10
Analysis of secured documents	• Tools for finding/ cracking/ bypassing of passwords, • encryption keys for recovery of data from the password protected / encrypted documents; • tools & techniques to find/reset passwords, brute force, rainbow tables • Hands on Lab	10
Computer forensic tools and toolkit	• Well known commercial and freeware toolkits, • Their features, • WinHex, advantages over other CLI/GUI tools, • Cyber Check Suite, Access Data FTK, EnCase Forensics, Helix, The Sleuth Kit, Toolset BackTrack	30

	• Hands on Lab	
Report preparation	• Computer Forensic Analysis Reports, • Executive Summary, • Goals/Objective of the Analysis, • Case questionnaires with relevant findings,referring to annexing of supporting documents, screenshots, photographs; tools used, forensic analysts involved, Report writing Guidelines, organizing the Reports, Documenting Investigative Steps with sections & subsections, Conclusion, Expert witness, testimony by a forensic analyst and role of an expert witness in judicial courts • Hands on Lab	30

Name of Unit of Qualification **:COMPUTER FORENSICSFOR WINDOWS & LINUXSYSTEMS AND ANTI-FORENSICS**

Duration **: 120 Hours**

Topics **: COMPUTER FORENSIC SFOR WINDOWS & LINUX SYSTEMS AND ANTI-FORENSICS**

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
Familirization Windows Forensics	• Examination of recycle bin INFO / INF02, • Windows shortcut files, • Swap file pagefile.sys, • Hibernation file, print spool files, • Windows registry analysis, registry analysis tools, registry hives, • Knowing about USB devices used, typed URLs, • Files extracted using winzip, • Recently opened/ downloaded/ saved files, • Date of installation & version of software applications, time zone, last shutdown time, IP & MAC Address, autorun programs • Hands on Lab	30
Linux Forensics	• Use of built-in command line tools for computer forensic investigation • dd, dcfldd, fdisk, mkfs, mount, umount, md5sum, shalsum, dmesg; • Mounting of the hard disk having forensic image, • Data recovery tools • Use of search tool 'find' with various options to find specific files, Linux boot sequence, • Timeline analysis of files using find • Hands on Lab	30
Internet usage analysis	• Websites in favourites, history, • Cookies, temporary internet files, • Data in cache, saved passwords, • Auto-complete feature, • Internet usage analysis tools • Hands on Lab	20
Tracing the source of the e-mails	• Identification of mailbox in client system, • Recovery of deleted e-mails, • E-mail headers, viewing & analysing the e-mail headers in popular e-mail software applications, • Message-id, ESMTP-id, IP address of e-mail server & client system associated in sending emails, • whois, etc. tools for finding location of an IP address; e-mail server access logs, spam/spoofed e-mails, phishing e-	30

	mails, use of tools and forensic toolkits in tracing e-mails • Hands on Lab	
Anti-Computer Forensics	• Challenges or bottlenecks in computer forensic investigation for a computer forensic analyst; • Encrypted, compressed, password protected documents • Hands on Lab	10

Name of Unit of Qualification : Enhancing Communication & Soft Skill

Duration : 20 Hours
Topics : Enhancing Communication & Soft Skill

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
Acquiring Communication Skill	• Communication , verbal and non-verbal communication	6
Managing career, staff and professional relationships	• Building professional relationship, Relationship at work , Making the most of personal and professional relationships, Competency Description, Managing Difficult Business Relationships	6
Preparing for interview	• Interview Techniques: Planning For The Interview, Preparing for an Interview, Interview Formats, Stages Of The Interview, Types Of Interview Questions • Best Bet for Interview Preparation: Mock Interviews, The Benefits of Mock Interviews Experience & Skills, • Curriculum Vitae: Overview, types of CV, Covering letter, Writing a Resume, Acceptance Letter, Thank You Letter	8