Certificate Course in Digital Forensics

Detailed Curriculum

Name of Unit of Qualification	**:**	Cyber Crime and Introduction to Computer Forensic
Duration	**:**	15 Hours
Topics	**:**	Cyber Crime and Introduction to Computer Forensic

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
1. Familiarization with Cyber Crime	Categorization of cybercrimes, Security policy violations, Online financial frauds, Elaboration of cybercrimes with techniques used by the cyber criminals • Phishing, Cyber-stalking, Cyber Harassment Cyber Frauds, • Tampering with computer source documents, Hacking with computer system, Publishing of obscene information in Electronic form	6
2. Introduction to FileSystem	Architecture ,Importance of File systems, Windows file structure FAT, NTFS, Unix File Systemext2, ext3	4
3. Introduction to Computer Forensics	Introduction, Need of computer forensic investigation of the cybercrimes, Forensic investigation process	3
4. First Responder	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 cybercrime.	2

Name of Unit of Qualification	**:**	Seizure & Imaging of Digital Evidence
Duration	**:**	15 Hours
Topics	**:**	Seizure & Imaging of Digital Evidence

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
1. 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,	4

	chain of custody forms	
2. 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	5
3. Seizing & Imaging of Non-volatile Data	Disk imaging software tools & hardware equipment, • 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	4
4. 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	2

Name of Unit of Qualification	**:**	Windows and Linux Forensic
Duration	**:**	15 Hours
Topics	**:**	Windows and Linux Forensic

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
1. 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	8
2. 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	7

Note: After completion of course there is a final qualifying exam will be there which is not included in the course duration, for that an extra 1 or 2 days will be given to do the final assessment.