COMPUTER FORENSICS

SevenMentor PVT.LTD

www.sevenmentor.com

1.0 Computer Forensics In Today's World

1.0 Intro To Computer Forensics
2.0 Need For Computer Forensics
3.0 What is Cyber Crime
4.0 Forensics Investigation Process
5.0 Cyber Law

2.0 Computer Forensics Investigation Process

1.0 Forensic Workstation Building SIFT
2.0 Chain of Custody
3.0 Data Imaging(FTK Imager)
4.0 Data Integrity(sha256sum)
5.0 Data Carving(Physical Level)
6.0 Data Analysis(FTK Toolkit)
7.0 Expert witness
8.0 PCI-DSS,DMCA,FISMA ACT

3.0 Understanding Hard Disks and File systems

1.0 Disk Drive Overview
2.0 Booting Process
3.0 Windows File Systems
4.0 Linux File Systems
5.0 Mac File Systems
6.0 The Sleuth Kit(TSK) And Autopsy

4.0 Data Acquisition and Duplication

1.0 Static and Live Acquisition
2.0 Volatile Information from linux and windows
3.0 Acquiring Data on windows
4.0 Acquiring Data on Linux
5.0 FTK Imager and ddclfd(Bit-Stream copy)
6.0 Netcat for Forensic

SevenMentor
PVT.LTD

5.0 Defeating Anti-Forensics Techniques

1.0 Cryptography,PKI,PKC,VPN
2.0 Steganography And Steganalysis
3.0 Password Cracking System and Application
4.0 Cracking BIOS Password
6.0 Alternate Data Stream
7.0 Encrypted file System

6.0 Operating System Forensics

1.0 Network and Process Information
2.0 Cache , Cookie and History Analysis
3.0 Registry Analysis
4.0 Linux Configuration Analysis
5.0 Windows Event Viewer

7.0 Network forensics

1.0 Network Forensic
2.0 Intrusion Detection System(IDS)
3.0 Firewall, IPS and Reverse-Proxy.
4.0 Honeypot And Tracing.
5.0 Traffic Capturing and Analysis

8.0 Investigating Web Attacks

1.0 Web Application Architecture
2.0 Web Attacks
3.0 Apache Web Server Logs Investigation
4.0 Web Attack Detection
5.0 Tracing IP Address

9.0 Database Forensics

1.0 Logon event in windows and Linux
2.0 Syslog Identification
3.0 Log Capturing and Analysis

10.0 Cloud forensic

1.0 What is cloud.
2.0 What is Reverse-Proxy
3.0 Squid Configuration
4.0 Log Analysis using Grep,awk,date,etc.

11.0 Malware Forensic

1.0 Unstructured Memory Analysis
2.0 Bulk EXtractor
3.0 cridex malware identification
4.0 Network Activity to a Process

12.0 Investigating Email Crimes

1.0 Email System Architecture
2.0 Email Crimes
3.0 Email Header Analysis.
4.0 Tracing Emails

13.0 Mobile forensic

1.0 Mobile Device
2.0 Cellular Network
3.0 Knowledge of Mobile forensics tools.
4.0 Mobile Forensic Process.
5.0 Mobile Forensic Reports (Real time)

14.0 Forensics report writing and presentation

1.0 Forensics Report
2.0 Report Writing And Documentation.
3.0 Sample Report Writing
4.0 Writing Reports using FTK
5.0 Writing Reports using Autopsy

15.0 Case Studies.

SevenMentor
PVT.LTD