

## Digital Forensics Investigation

**Prerequisite(Ethical Hacking)**

**Duration(60 Days)**

**Module:1 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 Crime Reports
- 6.0 DEFT,CAINE OS.

**Module:2 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

**Module:3 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

**Module:4 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

# IT Certification Guru PVT.LTD



## Module:5 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

## Module:6 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

## Module:7 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

## Module:8 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

## Module:9 Database Forensics

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

## Module:10 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.

## Module:11 Malware forensic

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



# IT Certification Guru PVT.LTD



## **Module:12 Investigating Email Crimes**

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

## **Module:13 Mobile forensic**

- 1.0 Mobile Device**
- 2.0 Cellular Network**
- 3.0 Crimes using Mobile Phones**
- 4.0 Mobile Forensic**
- 5.0 Mobile Forensic Process**

## **Module:14 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**

## **Module:15 What is Next.**

- 1.0 What is Malware Analyst**
- 2.0 What is Exploit Development**

IT Certifications  
guru

