Certified Digital Forensic Professional - CDFP

MODULE 1: Legal Aspects Of Digital Forensics & Global Approach

- **Digital Forensics Overview**
- **Brief introduction tForensic science**
- **Major legal systems**
- **Taxonomy of cyber-crimes**
- **Global Initiatives against cyber-crimes**
- **Commonwealth Cybercrime Initiative (CCI)**
- **Interpol**
- **Federal Bureau of Investigation**
- **OECD**
- **Council of Europe – Convention on Cybercrimes**
- **Global Cyber Security Index (GCI)**
- **Understanding threats tInformation Assets**
- **Challenges in investigating cyber-crimes**

MODULE 2: Computer Hardware

- **Computer Hardware Components**
- **The Boot Process**
- **Hard Disk Partitioning**
- **File System Overview**
- **How is a file stored (Media Creation, Modified, Accessed)**
- **The effects of deleting and un-deleting files**

MODULE 3: File Systems

- **Concept of computer file systems**
- **FAT (File Allocation Table) Basics**
- **Physical Layout of FAT**
- **Viewing FAT Entries**
- **The Function of FAT**
- **NTFS (New Technology File System)**
- **Clusters and Sectors**
- **Alternate Data Streams**
- **Linux Files Systems**
- **Slack Space**
- **Resilient File Systems (RfS)**

MODULE 4: Disks And Storage Media

- **ISO9660**
- **UDF – Universal Disk Format**
- **Media Devices:**

- **HDD**
- **Magnetic Tapes**
- **Floppy Disk**
- **Compact Discs, DVD and Blue Ray**
- **Ipods, Flash Memory Cards, etc.**

MODULE 5: Digital Evidence - Foundations

- **What is Digital Evidence?**
- **Computer "Incidents"**
- **Evidence Types**
- **Search & Seizure**
- **Voluntary Surrender**
- **Subpoena**
- **Search Warrant**
- **Planning for and gathering digital evidence**
- **The Physical Location**
- **Personnel**
- **Computer Systems**
- **What Equipment ttake**
- **Search Authority**
- **Handling Evidence at the scene**
- **Securing the Scene**
- **Taking Photographs**
- **Seizing Electronic Evidence**
- **Bagging and Tagging**

MODULE 6: Managing Digital Evidence

- **Chain of Custody**
- **Definition**
- **Controls**
- **Documentation**
- **Evidence Admissibility in a Court**
- **Relevance and Admissibility**
- **Best Practices for Admissibility**
- **Hearsay Rule, Exculpatory and Inculpatory Evidence**

MODULE 7: Boot Process: Windows, Linux And Macintosh

- **The Boot Process**
- **System Startup**
- **The relevance of Boot process for digital forensic investigator**
- **Loading MS-DOS**
- **Loading Windows OS**
- **Loading Windows 2003 Server**
- **Loading Linux**

- **Loading Linux Server**
- **Loading Macintosh**
- **When to Pull the Plug or Shutdown?**

MODULE 8: Mobile Devices Forensics

- **Mobile device forensics**
- **Mobile Operating Systems**
- **Data acquisition on mobile / hand held devices**
- **Investigative options available to crack password-protected file**

MODULE 9: Acquiring, Processing And Presentation Of Digital Evidence

- **Using Live Forensics Boot CD's**
- **Boot Disks**
- **Viewing the Invisible HPA and DCdata**
- **Drive-to-Drive DOS acquisition**
- **Forensics Image Files**
- **Data Compression**
- **Image File Forensics Tools**
- **Copy Right Issues – Graphic Files**
- **Network Evidence acquisition**
- **Why Network acquisition?**
- **Network Cables**
- **FastBloc**
- **LinEn**
- **Mounting a File System as Read Only**

MODULE 10: Forensic Investigation Theory

- **Locard's Exchange Principle**
- **Reconstructing the crime scene**
- **Classification**
- **Comparison**
- **Individualization**
- **Behavioral Evidence Analysis**
- **Equivocal Forensic Analysis**
- **Basics of Criminology**
- **Basics of Victimology**
- **Incident Scene Characteristics**

MODULE 11: Processing Evidence

- **Windows Registry**
- **System identifiers**
- **Sources of unique identification within OS**
- **Aspects of OS data files, tinclude Index.dat and other system files**
- **"Recycle" folder and deleted files.**

- **Image metadata**

MODULE 12: Presenting Evidence

- **Documenting and Reporting Digital Evidence**
- **Review and analyze the methods used tdocument and report the results of a computer forensic examination.**

MODULE 13: Forensic Models, Appliances And Protocols

- **Four Cardinal Rules**
- **Alpha 5**
- **Best Practices**
- **Software Licensing Types**
- **Free Software**
- **Industry Accepted Software**
- **Forensics Hardware Devices:**
- **Disk Duplicators**
- **Write Blockers**

MODULE 14: Cryptography, Password Cracking And Steganography

- **Basics of cryptology and cryptography**
- **Cryptography and cryptanalysis Processes**
- **Hash Types**
- **Pre-Computed Hash Tables**
- **Types of encryption concepts**
- **Investigative options available tcrack password-protected files**

MODULE 15: Lab Protocols

- **Quality Assurance**
- **Standard Operating Procedures**
- **Peer Review**
- **Administrator Review**
- **Annual Review**
- **Deviations from the SOP**
- **Lab Intake and what you must receive**
- **Tracking Digital Evidence in the Lab**
- **Storage Requirements**
- **Proficiency Tests**
- **Code of Ethics**