CDFS

CBIT Digital Forensics Services

Digital Forensics & Data Analysis 101

(4-day instructor-led course)

Course Summary

Gain an understanding of Electronic Discovery, starting with an introduction to discovery in Australian civil litigation and the Electronic Discovery Reference Model (EDRM). You will learn about the complexities of electronic data, including data storage media and metadata, and practice identifying digital storage media and working with metadata.

This class will also cover the critical role of processing in electronic discovery, including encoding, steganography, and data mapping. You will learn about opportunities and obstacles related to electronic discovery from mobile devices, preserving social media content as evidence, and using search protocols to hone your search skills.

By the end of the class, you will have knowledge on how to handle sensitive data with care, maintain the integrity of digital evidence, and comply with electronic discovery rules and protocols.

COURSE OUTCOMES

- Digital Forensic Triage
- Digital Forensic Acquisition
- Reviewing Digital Evidence
- Communicate and work efficiently with Digital Forensic and Cyber Teams

TARGET AUDIENCE

- Government and Law Enforcement Investigators
- Cyber Crime Investigators
- Digital Forensic Investigators
- IT Security Managers
- Incidence Response Members

THEORY AND PRACTICAL

Multiple practical exercises are provided to enforce key concepts learned.

MODULE 1: FORENSICS AND DIGITAL FORENSICS

- What is Forensic Science
- The role of Forensic Science in the Legal System
- Why is it important to understand forensic evidence
- Identifying Forensic Traces

MODULE 2: DIGITAL FORENSIC PRINCIPLES

- Introduction and Discussion

MODULE 3: SOURCES OF DIGITAL EVIDENCE

- Desktops, laptops
- Smart Devices (Mobiles, Tablets)
- Internet of Things (IOT)

MODULE 4: STORAGE MEDIA PRINCIPLES

- Different types of Digital Storage Devices and Media
- Introduction to data organisation (file systems and data structures)
- Remote / Network / Cloud Storage

MODULE 5: OPERATING SYSTEMS

- What is an Operating System?
- Different types of Operating Systems
- Common OS forensic artefacts

MODULE 6: DATA PRESERVATION PRINCIPLES

- Different types of Hardware Write Blocking and Imaging Devices
- Software Write Blocking Applications
- The importance of testing and verification of DF tools
- Boot Process
- Forensic Boot

MODULE 7: DIGITAL EVIDENCE AT THE CRIME SCENE

- What is a Digital Forensic Crime Scene
- Prepare before attending the Crime Scene
- Search Warrant Conditions, the role of the DF team member, and the warrant holder
- Assisting with interviewing suspects in relation to digital evidence
- Processing a crime scene involving digital evidence and perform preliminary survey
- Protect and manage digital evidence at the crime scene
- Document digital evidence at the crime scene
- Introduction to Digital Forensic Triage order
- Develop a plan for successful triage of digital evidence order

MODULE 8: THE ACQUISITION PROCESS

- Digital evidence collection
- How to prepare/sterile Target Media
- What is Forensic image and what is a Clone
- Data collection
    1. Perform basic imaging
    2. Data collection
    3. Prepare target media
    4. Test and verify DF tools
    5. Imaging
    6. Cloning
    7. Data Containers
    8. Targeted Collections
    9. Authentication

MODULE 9: DIGITAL FORENSIC TRIAGE

- The theory of DFT (Digital Forensic Triage)
- Using different tools to perform DFT (Digital Forensic Triage)
- Triaging of storage devices
- Prioritising devices for live examination and collection (Volatility Risk Assessment)
- Triaging of computer systems and smart devices
    1. Windows
    2. Apple
    3. Android
- How to Identify “Hot Zones” for effective DFT on powered-on systems
- Live DFT Workflow
- DFT and RAM
- Identify Encrypted structures (Volumes, Folders…)
    1. Bit Locker
    2. Specialties of APPLE devices

MODULE 10: OHS AND OFFICER SAFETY

- How to identify and manage individual and environmental threats to an officer's safety
- How to deploy proper procedures and tactics to ensure personal safety as well as the safety of others at the electronic crime scene

MODULE 11: DIGITAL EVIDENCE IN COURT

- Introduction
- Bevan v The State of Western Australia

PRICE

$6,000
per person ex GST

OR

4 CDFS Training Vouchers
per person ex GST

* Vouchers can only be used for courses delivered by CDFS at our training facility or via Virtual Instructor-Led Training.