

Computer forensics - Investigator

Introduction

This course covers the full requirements for delegates to become digital forensic investigators, working as field investigators or laboratory technicians. Day 1 will lay the foundation for a solid understanding of the computer forensic universe. Day 2 will cover extensively the technical and legal nuances that are called for, in this emergent science. Day 3 will involve hands on investigation followed by a practical court session where course delegates will experience and participate first hand as expert forensic witnesses and will be cross examined in a mock case by a lawyer.



Aim

The aim of this course is to provide delegates with a sound knowledge and practical understanding of computer forensic evidence. The depth of the course is advanced. It seeks to prepare delegates to become professional computer forensic experts with competent investigative, analytical and presentation skills.

Syllabus

DAY 1

Introduction

- Brief history
- Why computer forensics – past, present (emergent crimes and corporate demands)
- Is computer forensics a science – Fry and Daubert test
- Global organisations overseeing
- Associations
- Qualifications

Physical components of the PC

- Qualifications
- Basic electrical safety.
- Motherboards and the design of the PC.
- Practical - Exercise in dismantling and re-building PCs.

How Computers work

- Self Test (POST). BIOS and CMOS.
- Architecture of real mode. Interrupts. Start of boot sequence. Power On
- An explanation of the Power on Self Test and boot sequence.

Computer Topology

- Stand alone computers
- Network computing
- The world wide web as a network (IP addressing, DNS, MX records, Web servers, ISP)

Data Storage

- Volatile and non volatile data – implications for Computer forensics
- How to convert from Binary to hexadecimal
- How to convert from hexadecimal to binary
- Hex view in forensic software

Disk geometry

- Development of the hard disk. Physical construction.
- CHS and LBA addressing.
- Boot sector
- Master boot record
- Partition table, slack space and free space.
- Disk mapping.

DAY2

How computers store data

- Concept of file deletion and recovery
- Review of MSDOS, Operating systems.
- Practical analysis and examination of FAT 12, FAT 16, FAT 32 and NTFS file
- Introduction to linux file systems Linux ext2 and ext3.
- Meta data –
- File time line
- File formats and extensions

Steganography and cryptography

- Passwords & password cracking
- Disk lock and encryption technologies
- Data hiding
- Different ways of concealing data

Practical exercise

Ways of concealing data

Where is the evidence located?

- Artifacts
- Logs
- Devices

The windows registry – the Hives

- What can you find
- Where can you find evidence

Laboratory protocol

- Evidence seizure preliminaries
- Actions at the scene
- Treatment of exhibits
- Laboratory ethics
- Chain of custody
- Documentation.

Forensic examination tools

- Win hex,
- FTK - Access data,
- Encase,
- Net analysis
- Image mount

Practical

- Disk imaging
- Investigate an image from a hard drive
- USB drive to locate required evidence
- A series of practical lab exercises designed to demonstrate how to access forensic artifacts within hard disk drives and usb thumb drive
- Identify slack space, unallocated sectors, deleted files, file headers, Ram
- Conducting a search of an imaged disk or folder
- File carving
- The forensic Report

Introduction to computer Networks in a forensic environment.

- Overview of computer networks and the Internet – topology and devices
- Problems associated with evidence extraction – live , remote & laboratory

Practical Class

Investigating a computer crime - Mock scenario.

Each delegate will prepare a forensic report they will present in a Court scene on Day 3 as expert witness to be cross examined.

DAY 3

Legal issues and Presentation of report

- Admissibility of computer evidence
- Junk science arguments
- State of the Law - Daubert, CPR directions, FCPR

Seizure of computers - issues

Legal protection for the user - Human rights Act, Data protection, property rights etc warrants, scope and authority of investigator. Scope of seizure

Preparation and giving of evidence.

- The expert witness - Qualifications
- Duties of an expert witness
- Scene of crime notes
- Crime scene exhibits
- Effective communication with court & jury
- Examination in chief
- Cross examination
- Re examination

Practical moot court session

Barrister Karl Obayi - Appearing for the defence
Delegates will appear as expert witness for the prosecution.

Intended Learning Outcomes

On successful completion of this course a delegate should be able to:

Knowledge

- Recognise the component parts of a computer, understand how these parts physically and electronically interact, and observe sound standard operating procedures in maintaining the integrity of computer evidence from investigation, extraction, analysis and presentation in court.
- Understand the start-up procedures of operating systems, particularly in DOS and Windows environments, how they interact with the hard disk and the significance of the paging of memory to disk in a forensic environment.

Skills

- Demonstrate a sound understanding of the law and technique relating to evidence recovered from computers.
- Understand computer evidence as it applies to proof in relation to common offences in the UK and USA.
- Understand the investigation process within the framework of a computer network
- Understand and be able to apply the relevant principles in acting as an expert witness whilst communicating effectively in court.
- Identify available resources (software and Hardware) that will aid the investigation process.