

Computer Evidence Training

iTevidence
Criminal - Civil - Arbitration



- ◆ computer forensic evidence
- ◆ mobile phone evidence
- ◆ digital document discovery



Training Topics

Page

❖ Computer evidence – Introduction	4
❖ Computer evidence – Intermediate	6
❖ Computer evidence - Advanced	9
❖ Electronic document discovery	13
❖ Mobile phone forensics	16
❖ Digital evidence for the Judiciary	18
❖ Digital evidence for paralegals	21
❖ Computer incident response	24
❖ Internet – forensic investigation	27
❖ IT law for IT Managers	30



Karl Obayi Esq.
MCSE, CCNA, MCT, CCA, LL.B, BL
Computer forensics Attorney
Principal Legal Consultant

What we do

We act as Specialist Solicitors in matters concerning computer forensics, mobile phone evidence and digital document discovery.

We deliver seminars and organise quality training that covers the broad spectrum of digital evidence discovery, extraction, analysis and presentation in civil, criminal and arbitration proceedings.

The problem

Evidence! Evidence!! Evidence!!! This is the essential ingredient that determines whether or not you win or lose in Court or arbitration; to extend the theme further, not just evidence but the quality of evidence.

A couple of factors come to the fore when the Courts determine what constitutes admissible and relevant evidence and the quality or probative value to attach to a piece of evidence. Lawyers by training are comfortable with these parameters.

Given, that more than 90% of Business documentation, internet communication and 21st century social interaction is conducted via computers and digital devices, It is a matter of regret that professional legal training has not kept pace with the rapid advancement in computer technology. In this digital age, a nodding acquaintance of the application and relevance of computer evidence will not suffice.

Our Solutions

We provide quality training that covers an end to end approach on all matters concerning digital evidence from investigation, extraction, evidence analysis to court room presentation. Our courses are structured in modules to accommodate a paced learning environment. The courses are hands on and delivered by a solicitor who is also a qualified computer forensic expert.

Our unique Advantage

Our Principal Consultant and trainer previously practiced as a Barrister for more than a decade, a former university law lecturer for many years, and presently, a practicing Solicitor in England and Wales. In addition, he is a Certified Computer Systems Engineer and certified computer forensic investigator with more than 20years, combined experience in information technology and legal practice.

Our Clients

We conduct training and seminars for private clients, schools and corporate organisations; Barristers, Solicitors, Banks, legal training institutions, insurance firms, fraud auditors and Judicial officers.

“What you don’t know can hurt you”

Computer evidence – Introduction

Aim

The aim of this course is to provide delegates with an understanding of the role of computer evidence in criminal, civil and arbitration matters. It covers the broad spectrum of digital evidence identification, analysis and presentation in a corporate environment a court of law.



Audience

This course is aimed at first responders, prosecutors, paralegals, lawyers, judicial personnel, systems administrators, Legal professionals, accounting fraud investigators.

Syllabus:

History of computer evidence

- UK
- USA
- Global concerns
- Europe
- UN
- G-8

Unique attributes of computer evidence

- Evidence is in binary format
- Deleted files can be recovered
- Easily tainted and manipulated

Relevance of Computer evidence

- Criminal cases
- Civil cases
- Arbitration

Legal issues

- Admissibility of computer evidence
- Proof of evidence
- Civil procedure directions
- UK - Status
- USA - Status

How computers work - overview

- Parts of a computer
- How computers work - The boot process
- Unique characteristics of computer evidence
- Storage devices - Types
- Network computers
- The internet

Introduction to computer forensics

- What is computer forensics?
- Scope of computer forensics
- The investigative process

Introduction to electronic document discovery

- What is electronic document discovery?
- Scope of electronic document discovery
- The discovery process
- Searching techniques
- Digital document management

Where is computer evidence located?

- Storage devices
- Windows artifacts
- The registry
- logs
- Folders
- System components

What are you looking for?

- Characteristics of digital documents
- Document extensions
- Example of binary notations
- Relevance of Time lines
- Anti forensics
- Practical demonstration

The Court Room Environment

- Evidence presentation and report writing
- Demonstrative evidence
- Key players in the courtroom
- Role, obligations and expectations of the expert witness.

Intended Learning Outcomes

- On successful completion of this course the delegate will be able to:

Knowledge

- Understand the scope and relevance of computer and digital evidence in criminal and civil cases.
- Understand the steps involved in the collection and analysis of computer evidence.
- Understand steps involved in the management of digital evidence
- Understand the evidential rules within which digital evidence is collected
- Recognise and respond to the difficulties inherent in presenting computer evidence.
- Develop effective risk management protocols for storing and maintaining the integrity of computer evidence.

Skills

- Implement protocols to ensure data integrity and admissibility
- Implement measures to reduce the risk of evidence contamination
- Investigate and implement gap analysis in a corporate environment
- Assist investigating officers, legal officers, legal counsel

Computer forensics – Intermediate

Introduction

This course addresses the theoretical and practical application of computer forensics for the first responder and the computer forensic engineer within the corporate and legal environment. This course is compulsory for those who wish to proceed to our professional level course - Computer forensics-Advanced.



Aim

The aim of this module is to provide delegates with a sound knowledge and understanding to enable them to recover admissible evidence from PC based computers and the skills and competencies to prepare such evidence for presentation in a Court of Law.

Syllabus

The course will detail the fundamentals of forensic computing to a degree that will enable delegates understand precisely how commercial forensic tools operate and that will allow them to operate beneath the level of the tool and extract digital evidence directly from binary images.

Introduction

- Brief history
- Why computer forensics – before, now (emergent crimes and corporate demands)
- Is computer forensics a science – fry and daubert test
- Global organisations overseeing
- Associations
- Qualifications

Physical components of the PC and how they fit together and interact.

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

How Computers work

- An explanation of the Power On Self Test (POST)
- Boot sequence.
- CMOS
- MBR
- Operating system
- Applications

Volatile and non volatile data

- Relevance for Computer forensics
- Where is volatile data located?
- Where is non volatile data located?

Disk Geometry

- Types of disk storage and their characteristics
- Hard disk internals
- Disk management processes – fdisk, format
- Data storage mechanism – how data is stored and sorted
- Master boot record

Data storage

- Sector
- Partition
- Volume
- Ambient data – slack space, host protected areas

Operating systems and file systems

- FAT 12
- FAT 16
- FAT 32
- NTFS
- Linux ext2 and ext3.
- File Meta data - MAC attributes

Passwords and encryption

- Explanation of passwords keys and hashes.
- Dealing with password protected and encrypted files.

Steganography

- Data hiding-Forms of data hiding – System Area, slack space, disk size,
- Changing file extension, background page and font colour,
- Concatenation
- Anti forensics

Computer evidence investigation

- Preparations to be made before seizure.
- Actions at the scene. Treatment of exhibits
- Laboratory ethics – chain of custody
- Evidence e storage

Forensic examination tools and practical exercises

- Win hex,
- FTK - Access Data,
- Encase,
- Net analysis

- A series of practical lab exercises designed to demonstrate how to access forensic artefacts within hard disk drives and to develop the student's skills in forensic analysis. Importance of keeping a log. Methods of hiding data on hard and floppy disks, practical recovery of such data using methods to preserve its integrity. Methods of recovering deleted files. Copying and imaging

Introduction to Computer Networks

- OSI reference Model
- Overview of computer networks
- The Internet – topology
- Network devices

Legal issues and consideration

- Seizure of computers. – search warrants, scope and authority of investigator
- Civil investigation of computer evidence –special considerations
- Admissibility of computer evidence
- Initial obstacles
- Relevant Case Law
- Relevant procedural regulations

Report Preparation and giving of evidence.

- Witness statements
- briefing case officers and Counsel
- testifying as a witness

Intended Learning Outcomes

On successful completion of this module a delegate will be able to:

Knowledge

- Recognise the component parts of a computer, understand how these parts physically and electronically interact, and apply sound electrical safety procedures in a forensic examination environment.
- 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.
- Recognise the need for digital evidence integrity as it applies to its admissibility in court
- Understand what is required during testimony in court

Skills

- Apply a detailed knowledge of disk geometry to the examination of data storage systems and understand the advantages and disadvantages of imaging and copying for evidential purposes.
- Use data recovery software tools, understand the overall principle of original integrity, and be competently practised in the methods and principles of disk examination and logging, and the preparation of evidence for Court.
- Demonstrate a sound understanding of the law relating to evidence recovered from computers and law relating to the search for and investigation of computer evidence.

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.

Electronic Document Discovery

Aim

The aim of this Course is to help delegates develop an understanding of the nature of electronic data and its relevance in criminal, civil and arbitration matters, understand how to set up relevant protocols to respond to electronic discovery request. Understand and respond to possible legal issues that may arise during the process of negotiating the cost, scope and format of discovery. Delegates will be thought how to collect and manage electronic documents and prepare documents for trial or arbitration. Delegates will work within a life computer network environment reflecting a real life situation.



Audience

This course is aimed at Computer forensic investigators, first responders, Prosecutors, Defense lawyers, and IT security officers and Fraud investigators.

Syllabus

Introduction

- The internet as a global community
- Global compliance regulations - UK, USA, Sox law,
- An overview of the internet technological framework
- Key players in the internet technology infrastructure
- The many benefits of the internet - ecommerce and globalisation
- The many evils of the internet - fraud, ID theft, virus, spamming, phishing, web bug, privacy- cookies, CP, terrorism

What is electronic document discovery?

- E-Document as evidence in law
- Traditional approach
- Modern approach
- Legislations - (USA, UK)
- Court's attitude to e-document

Electronic document discovery – The preliminaries

- Gap analysis
- Corporate environment
- Criminal investigation
- The incident response team
- Data collection, filtering and achieving
- Achieving technologies

First responder procedure

- The incident response team
- The discovery process -
- Securing and evaluating electronic scene
- Types of digital devices
- Data collection, filtering and achieving
- Achieving technologies

Characteristics of electronic documents

- Binary format vs. printed copy
- Types of documents
- File header and extension
- Meta data
- May be volatile
- MAC times

Where is e-document located?

Stand alone PC

- Hard disk, USB, floppy, My documents,
- Mapped drives, offline files

Network

- File servers
- mail servers
- print servers
- shared folders
- backups, NAS storage, RAM

Device logs

- Switches
- Firewalls
- Intrusion detection systems
- Practical – document location

Document Search

- Automated tools V. Manual search
- Document filtering
- Document search methodologies
- Privileged document
- Redaction
- Document repositories and achieving
Practical - data search, filtering and archiving

Strategies for initiating a digital document request

- The case theory
- Letter of preservation
- Working with a forensic consultant
- Scope of request
- General and specific disclosure
- At the pretrial conference meeting
- Document production format
- Practical - Sample Motion to disclose

Strategies for responding to a digital document request

- Litigation hold
- At the pre trial conference
- Resisting discovery
- Reasonable and proportional standards
- Working with a forensic consultant
- Privilege documents
- Document redaction
- Document production format

Best practices

- Relevant team in place
- Authorised and trained person
- Image departing staff hard drive.
- Binary, wipe drives before you dispose at eBay
- Metadata deletion
- Redaction - for privileged portions of documents
- Practical - Court room tools for the presentation of digital evidence

Intended Learning Outcomes

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

Knowledge

- Recognise the need for proactive preparation in the use of electronic documents in criminal, civil and arbitration matters.
- Understand the steps necessary to implement a digital document discovery request and the inherent complications and resolution inherent in the process.
- Recognise the strategies for commencing and resisting a digital document disclosure request.

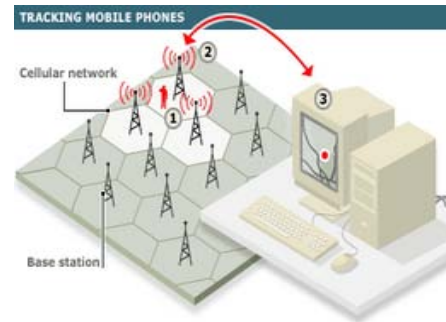
Skills

- Formulate and implement an electronic document discovery protocol.
- Attend pre trial conferences to confer and agree on electronic document disclosure protocols.
- Participate in the extraction, review and redaction of electronic documents
- Present electronic documents in court as custodians.

Mobile Phone Forensics - Introduction

Aim

The aim of this Course is to help delegates develop an understanding of the nature mobile phone evidence and its relevance in criminal, civil and arbitration matters, understand how the mobile phone communication infrastructure is setup to determine the flow of information data. Delegates will be taught how to locate mobile phone evidence and interpret call records. Emphasis will be drawn to what is legally possible and permissible in the use of mobile phone evidence. Reliance will be placed on existing legislations and a host of decided case law in the United States and the United Kingdom.



Audience

This course is aimed at Computer forensic investigator, first responders, Prosecutors, Defense lawyers, IT security officers and Fraud investigators.

Introduction

- What is mobile phone forensics
- Relevance of mobile phone and handheld forensics
- Types of mobile phones
- The evolution of the mobile phone - 3G
- How do mobile phones work

The mobile phone communication infrastructure

The mobile station

- SIM
- ME

The base station subsystem

- BTS
- BSC

The Network Subsystem

- HLR
- VLR
- MSC
- EIR
- AUC

The essential components of a mobile phone

- The SIM card
- The ROM
- The operating system
- Data storage – Volatility

Mobile phones as evidence

- The legal importance of mobile phone evidence
- What are the many functions of mobile phones?
- Where is the evidence located
- The phone - Hardware, Software and the Network
- Example of Case laws showing relevance of mobile phone evidence
- Practical class in Mobile phone triangulation P
- Practical class in cell site analysis

Extracting mobile phone evidence

- Preliminaries and expectations
- Evidence integrity and reliability
- Sequence of necessary steps
- Analysing mobile phone evidence
- The Call data records (CDR)
- Spatial mapping of phone records
- Automating mobile phone evidence
- Practical – extracting mobile phone evidence

Testifying as a witness in court

- Do
- Don'ts

Intended Learning Outcomes

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

Knowledge

- Understand the rudiments of mobile phone communication
- Understand the need for mobile phone evidence integrity and reliability
- Recognise the legal relevance and use all species of mobile phone evidence
- Understand the full life circle of digital evidence as it affects the use of mobile phone
- Recognise the risk involved in sloppy investigations

Skills

- Identify and determine the relevance of mobile phone evidence in a legal matter
- Secure potential crime scene involving a mobile phone
- Liaise with in-house counsel , external consultants and the police with coherent report
- Produce protocol for incident response involving the use of mobile phone

Digital evidence for the Judiciary

Aim

The aim of this course is to provide Judges, Court officials and lawyers with the necessary tools to understand and resolve issues concerning digital evidence in criminal, civil and arbitration matters. More importantly, to enable delegates acquire the relevant skills to deal with issues concerning the admissibility or otherwise of digital evidence. It covers the broad spectrum of digital evidence identification, analysis and presentation before a court of law or tribunal.



Audience

This course is aimed at Judges, Judicial officers, Arbitrators and lawyers.

Introduction

- The paradigm shift
- The influencing role of computer technology
- The need for a new learning and a new approach
- What is digital evidence – computer, mobile phone and digital document discovery
- Examples of digital devices
- Scope of digital evidence
- Junk science argument
- Lessons for the Judge and the court

Global Concerns

- EU
- UN
- US
- UK
- Canada
- Conflict of laws
- Cross boarder issues – evidence across international borders
- Lack of local legislations
- Lessons for the Judge and the court

Digital devices

- Types of digital devices
- Essential parts of a computer
- Brief introduction - How computers work
- Where is the evidence stored
- Real and deleted data
- How reliable is digital evidence?
- How to determine the Authenticity or otherwise of digital evidence
- Lessons for the Judge and the court

Relevance of digital evidence in Civil and Criminal matters

- Criminal Jurisprudence
- The mens rea
- The actus reus
- Strict liability
- Comparative analysis of criminal legislations
- Digital evidence in civil jurisprudence
- Lessons for the Judge and the court

Computer forensic evidence

- Brief introduction
- Scope of the discovery
- What needs to be discovered
- Evidence integrity
- Issues of admissibility
- Lessons for the Judge and the court

Mobile Phone evidence

- Brief introduction
- Scope of discovery
- What needs to be discovered
- Issues of admissibility
- Lessons for the Judge and the court

Digital document discovery

- What is digital document discovery?
- When is it relevant?
- Issues associated with digital document discovery
- Lessons for the Judge and the court

Admissibility of digital evidence

- The discovery and recovery of digital evidence
- The legal expectations in the discovery and recovery process
- Lessons for the Judge and the court

Anti Forensics

- Data hiding
- Encryption
- Steganography
- Cryptography
- Black Hat
- Lessons for the Judge and the court

The role of the forensic expert witness

- An analysis of the forensic experts methodologies
- Managing the expert evidence process

The Judges Domain

- Before the trial
- Relevant court orders
- Managing the scope of evidence
- Managing litigant antics
- Managing issues of cross border evidence
- Court sanctions

Practical

Case scenario with relevant elements examined and analysed by delegates.

Intended Learning Outcomes

On successful completion of this course the delegate will be able to:

Knowledge

- Understand the scope and relevance of computer and digital evidence in criminal and civil cases.
- Understand the steps involved in the collection and analysis of computer evidence.
- Understand steps involved in the management of digital evidence
- Understand the evidential rules within which digital evidence is collected
- Recognise and respond to the difficulties inherent in presenting computer evidence.
- Develop effective risk management protocols for storing and maintaining the integrity of computer evidence.

Skills

- Implement protocols to ensure data integrity and admissibility
- Implement measures to reduce the risk of evidential contamination
- Investigate and implement gap analysis in a corporate environment
- Assist investigating officers, legal officers, legal counsel

Digital evidence for Paralegals

Aim

The mountain of documents that needs to be dealt with in a criminal or civil case has increased over the years. But the real news is that the location of documents has moved from file cabinets to computers and other digital devices like mobile phones and personal digital assistants. The aim of this Course is to help delegates develop an understanding of the nature of electronic data and its relevance in criminal, civil and arbitration matters, understand how to set up relevant protocols to respond to electronic discovery request. Assist lawyers and fee earners in the electronic document discovery process. Delegates will be thought how to collect, manage, preserve and filter electronic documents, deal with external consultants, and potential litigation issues. Delegates will work within a computer network environment reflecting a real life situation.



Audience

This course is aimed at Paralegals, fee earners, corporate lawyers, Defense lawyers, IT security officers and Fraud investigators.

Syllabus

Introduction

- The history of digital documents
- Global compliance regulations
- An overview of the internet technology framework
- Key players in the internet technology infrastructure
- The many benefits of the internet
- The many evils of the internet - fraud, ID theft, virus, spamming, phishing, web bug, cookies, terrorism.

What is electronic document discovery?

- E-Document as evidence in law
- Traditional approach
- Modern approach
- Legislations - (USA, UK)
- Court's attitude to e-document
- When will e-document be required

Electronic document discovery – The preliminaries

- Gap analysis
- Corporate environment
- Criminal investigation
- The incident response team
- Data collection, filtering and achieving
- Achieving technologies

First responder procedure

- Litigation hold request or crime scene
- Securing and evaluating electronic evidence
- Types of digital devices
- Data collection, filtering and achieving
- Some useful Achieving technologies
- Local or online
- Document custodians

Characteristics of electronic documents

- Binary format vs. printed copy
- Types of documents
- File header and extension
- Meta data
- Volatile data
- MAC times

Where is e-document located?

- **Stand alone PC**
Hard disk, USB, floppy, My documents,
Mapped drives, offline files
- **Networked environment**
File servers, mail servers, print servers,
shared folders, backups, NAS storage, RAM
- **Device logs**
Switches, Firewalls, Intrusion detection systems
Practical exercise– Document location and mapping

Document Preparation

- Document identification
- The Scanning process
- The OCR process
- Document repositories
- Document output format
tiff, bmp, gif, jpeg, pdf, video, sound
- Production media format

Document Search

- Automated tools V. Manual search
- Document Mapping
- Metadata
- Search terms
- Search techniques
- Document filtering
- Document search methodologies
- Privileged document
- Redaction
- Document repositories and achieving
Practical exercise - data search, filtering
and archiving

Best practices

- Relevant team in place
- Authorised and trained person
- Image departing staff hard drive.
- Binary, wipe drives before you dispose at eBay
- Metadata deletion
- Redaction - for privileged portions of documents
- Stick to your lawyers instructions
- **Practical** - Court room tools for the presentation of digital evidence

Intended Learning Outcomes

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

Knowledge

- Recognise the need for proactive preparation in the use of electronic documents in criminal, civil and arbitration matters.
- Understand the steps necessary to implement a digital document discovery request and the inherent complications and resolution inherent in the process.
- Understand the difference between document formats and output
- Understand the document filtration process

Skills

- Manage and oversee the electronic document search and filter process
- Formulate and implement an electronic document discovery protocol.
- Attend pre trial conferences to confer and agree on electronic document disclosure protocols.
- Participate in the extraction, review and redaction of electronic documents
- Appear in court as document custodians.

Computer Incident Response

Introduction

This course addresses the relevant components in any computer incident environment as it applies to criminal or civil matters. It is an essential course for the first responder and the computer forensic engineer who conducts or processes digital investigations within the corporate and legal environment.

Aim

The aim of this module is to provide delegates with a sound knowledge and understanding to enable them to investigate secure and recover admissible evidence from computers and digital devices. Acquire the skills and competencies to prepare such evidence for presentation in a Court of Law. This course will assist the delegate who wishes to proceed to the other courses on computer forensic evidence investigation.



Preliminaries

- Computer security
- Computer incident
- Incident response

What is a Computer

- Varied definitions
- Scope of definitions
- Summary of definitions
- Computer devices
- Parts of a computer
- Computer storage technologies

Computer evidence

- Characteristics of computer evidence
- Volatile and non volatile data
- Computer storage technologies

Architecture of a Computer Network

- Standalone Computer
- Computer Network
- Computer operating Systems
- Computer peripherals

Computer incident – Classification

- What constitutes a Computer incident?
- Misuse – Security breach – operational mishaps

Misuse – Corporate environment

- Email abuse
- Resource access
- Privilege hijack – shoulder surfing
- Internet surfing

Security breach

- What constitutes a security breach
- Classification of breach – (Internal / External)
- Objects of the breach
- Targets of the breach – Files, Repositories, Web sites
- Workstation, Servers, Routers, Switches, Hubs, PDA & Mobile phones

Incident Response

- Summary of above
- What Constitutes response to an incident
- Traditional forms of response
- The Bigger picture with response – Corporate security
- Possible civil litigation and criminal prosecution

How to conduct an incident response

- Securing the scene
- Victim interview process
- Preliminary concerns ~ Data protection
- Human rights - Privacy
- The need for a response Team – Proactive placement
- Membership of the Team
- Legal preliminaries – Formulation of User policy
- Log on scripts, templates, employment conditions
- Documenting delegated authority

Manual v. Automated investigation / response

- Preliminaries – Note taking, securing evidence, evidence integrity
- Incident scene – Locards principle usb, Pasted Notes, Cd, Floppy, DVD, digital cameras, cctv cameras, laptop switch, hub, external drives.
- Fire brigade approach / Documented approach
- Do's and Don'ts ~ Log files , MAC modification, Bios modification
- Tipping off, Power off or plug off, Screen image.
- Volatile and Non volatile resources need to secure volatile data.
- Manual – incident response, available personnel dictates approach/ Complexity of response. Check device logs, event viewer, registry processes, resource access, open files.
- Automated – incident response ~ level of personnel skill, available software, standalone or remote subject, time factor, cost.

Best Practice

- Need for proactive measures – Team, existing protocol,
- Criminal incident – to report or not to report?
- Cost of non compliance with protocol – Case law examples and legislation examples
- Corporate Governance and Compliance WorldCom, Arthur Anderson, Sox, Card industry, HIPPA, Companies Act as amended
- Need for IT Audit and Gap analysis
- ACPO and Sedona Principles

Course Review / Questions

Intended Learning Outcomes

On successful completion of this module a delegate will be able to:

Knowledge

- Recognise the different components that are required for setting up an incident response team.
- Design and implement a protocol for computer incident response within a corporate environment.
- Secure the incident scene and assist in the investigation of a digital incident environment
- Understand what is required during testimony in court

Internet - Forensic investigation

Aim

The aim of this module is to enable delegates develop the necessary skills and knowledge to investigate and recover admissible evidence from computers which have been used to exchange information across the Internet.

Audience

This course is suitable for the first responder, Fraud investigator, Paralegal, Barrister, Solicitor and constitutes a good foundation for the computer Forensic investigator advanced course.



Syllabus

Introduction

- History of the internet
- Architecture and topology of the internet
- The role of the ISP
- Benefits of the internet
- Current developments – from Web1 to Web2

How information is transferred on the internet

- Basic introduction to computer networking
- The OSI networking model with emphasis on
- The Network layer
- The transport layer
- The session layer
- The application layer

The problem with the internet

- Legal issues
- Hackers
- Viruses, Malware, Trojans, backdoors

Hacking methodology

- The hacking community
- Why hack
- How hacking is effected
- Some control measures

Internet platforms

- Domain structures
- Web sites – Purpose, scope and types
- Services provided on the internet
- Online Commerce
- Collaboration Portals – share point

- Emails, FTP sites
- Research - Google
- Blogging
- Forums

Common Applications used on the internet

- Internet explorer, Google
- Web sites
- Emails
- FTP
- Peer- to-Peer
- wiki's

Where is internet evidence located?

- Web cache
- Temporary files
- Internet history file
- Cookies
- Windows Registry
- Firewalls
- Routers
- IDS

Investigating internet use and abuse (Part 1)

- The legal frame work
- Do's and Don'ts
- Automated vs. Manual
- Tools for automated investigation
- Practical class – examining internet history file (index. dat)

Investigating internet use and abuse (Part 2)

- Hacking tools
- Spoofing
- Phishing
- Trojan
- Malware
- Cookies
- Rootkit

Practical

- examination of internet history files
- examination of email header
- interpreting a who is trace
- Using Dig from the command line

Preparing the investigative report

- Documentation
- Reporting requirements
- Essentials of the report
- Testifying in court

Intended Learning Outcomes

On successful completion of this module the student will be able to:

Knowledge

- Demonstrate an understanding of the law as it affects internet transactions
- Demonstrate an understanding of internet technologies and the associated cast of characters.
- Demonstrate an understanding of the scope of activities that take place on the internet – Social, Business, public and private
- Identify the core areas containing evidence or information about Internet transactions on a Computer Hard disk and apply this knowledge to recovery of relevant data.
- Interpret and decode relevant system files connected with the use of the internet
- Demonstrate an understanding of the file download process
- Demonstrate knowledge and understanding of the procedures which have taken place electronically in the transmission and reception of E-mail and attachments
- Demonstrate knowledge and understanding of the procedures which have taken place electronically in the posting, circulation and downloading of Usenet Newsgroup items.
- Demonstrate knowledge and understanding of the effects of Malware, viruses and backdoors.

Skills

- Identify and assess the data structures of a number of leading Internet related applications and consequently adopt the correct data recovery strategy.
- Quickly create a template for the examination of a computer that has been used to access the Internet by identifying relevant areas for examination.
- Preparing acceptable reports for use in trial or arbitration
- Participate as a technical witness in court.

IT Law for IT Managers

Aim

The aim of this Course is to help delegates develop an understanding of the nature of electronic data as it relates to the management and litigation readiness of a computer network.

Audience

The target audience for this course is anyone whose job function it is to manage and prepare any business concern for litigation readiness.



Introduction

- Who is the IT Manager - Job function not necessarily Job title
- The unique role of the IT Manager
- The myth about restrictive role to technical issues on the Network
- The ideal - prominent member of the board in the design and implementation of corporate policy
- Traditional Role of the IT Manager debunked

Tangential laws affecting liability in the running of a Computer Network

- Rule of law
- Human Rights protection for the User
- Privacy laws
- Freedom of information Act
- Data protection Act
- Safe harbour principle
- Criminal law
- Espionage
- Hacking - No hack back
- Compliance regulations e.g Sox

Resolution

Use of log on Banners
Employment contracts properly drafted- liaise with HR
Regular IT audit

Why it is important to understand the role of law in a computer network environment?

- Paradigm shift from paper documents to digital documents - statistics
- Emails
- Internet
- File sharing
- Security and corporate espionage
- Human resource
- Health and safety
- Document custodians
- IT Budgets
- Tendering for business - 3rd party requirements about the network

Criminal Law Provisions – UK

- Computer misuse Act
- Terrorism Act
- Telecommunications Act
- Data protection Act
- RIPA
- WEEE
- PACE

Criminal law Provisions – USA

- CFMA
- ECPA
- Other Title 18 offences

Civil law provisions

- Human Rights Act
- Copy rights design and Patents
- Distant selling directives
- Contract and Commercial law

Electronic document discovery

- Electronic document recovery
- Statutory compliance – emails see Sox
- Document archiving
- Online repository

Examine the OSI model – Potential problems at each layer

Layer	Responsibility
7	This layer represents the end user application - http, ftp, smtp or telnet - what can possibly go wrong -
6	Handles formatting, compression, encryption and presentation of data to the application e.g. SSL and TLS
5	Deals with management and setup of sessions between computer applications
4	Deals with data transport and error control
3	Routing packets between networks - routers
2	Data layer from one host to another
1	Physical link, cabling and binary transmission of data.

Reporting a Computer crime

- Why report
- Before you report
- Impedements
- Police agent
- Board concerns

Working with law enforcement

- Preliminaries - Questions to ask
- What reports to provide to the police
- What you cannot do

Investigating computer misuse

- Working with the victims
- Legal pitfalls
- Technical pitfalls
- Best practice

Auditing Network Devices

- Switches
- Routers
- firewalls
- IDS

Auditing Stand alone computers

- What are you looking for?
- Where to look
- Know your limitations

Auditing relevant servers

- Domain controller
- File server
- Print server
- Database server
- AV server
- Honey pot or sandbox
- Know your limitations

The incident response Team

- What is an incident response team
- Role of the incident response team
- Setting up an incident response team
- Responding to an incident
- Designing an incident response protocol
- Implementing an incident response protocol

The Litigation ready Network

- What does this mean?
- Proactive protocol for litigation readiness
- Who is a document custodian?
- Expectations of a document custodian
- What document to protect and in what format
- What is a litigation hold
- What is spoliation
- Conducting a document search
- Producing responsive data
- Privileged documents
- Redaction

Expert relationships

- Assisting the corporate board
- Working with external consultants
- Working with in house counsel
- Assisting the police

Life circle of computer evidence- overview

- Evidence identification
- Evidence collection
- The digital evidence scene – Locards principle
- Evidence analysis / filtering
- Evidence preservation – chain of custody
- Evidence presentation.

Testifying as a witness in court

- Do's
- Don'ts

Intended Learning Outcomes

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

Knowledge

- Recognise the need to design and implement a digital evidence protocol within and IT environment
- Understand the need to design and implement an incidence response team
- Recognise the legal implications of conducting a computer investigation
- Understand the full life circle of digital evidence within a computer network
- Recognise the risk involved in hasty investigations

Skills

- Conduct a gap analysis of corporate requirements in digital data security
- Design and implement an incidence response protocol with appropriate team members.
- Liaise with in-house counsel , external consultants and the police
- Testify as an expert witness or document custodian in court.

Computer forensics evidence Training



Computer evidence
Mobile phone evidence
Digital document discovery

iTevidence
Office 12, The Generator
95, Miles Road, Mitcham
Surrey. CR4 3FH
London

www.itevidence.co.uk

Tel: 020 8408 1616

Fax: 020 8408 1617

info@itevidence.co.uk