Digital Evidence Handbook

Introduction

Emergency Investigation Check List

Evidential Basics

Testimonial Evidence
Real Evidence
Documentary Evidence
Business Records
Technical Evidence
Expert Evidence
Derived Evidence
Continuity / Chain of Custody / Provenance
Completeness
Informal Indications that a particular form of Digital Evidence can be safely relied on
Principles of handling Digital Evidence
Multiple Sources / Corroboration
"Exhibits" are not direct evidence, just representations
Role of Expert Witnesses
Standards of Proof
Contents of an Expert Report
Daubert Tests
Prosecutor's Fallacy
Confirmation or Cognitive Bias
Digital Evidence may have a physical existence – and there may be other types of evidence present

Evidence: legal basics

Admissibility: an important bit of legal terminology
Self-authentication
Standards of Proof
Powers to investigate
Powers and Obligations in Civil Litigation
Third-Party Disclosure in Civil Proceedings
Civil Search Orders / Anton Piller Orders
Law enforcement powers

Evidence from Other Jurisdictions: MLATs
Hired Experts and Technicians

Forensic Science: Digital Forensics Research Methodology

What is "forensic science"?
Daubert Rules
Forensic Science and Event Reconstructions
Digital Evidence
Reverse Engineering and "Closed" Systems
Artefact Research
Testing Times
Reconstructing Events in the Digital Domain
Forensic Science Standards, Accreditation, Qualifications
Good Practice Guides

Evidence Acquisition and Preservation: General Principles

Good Practice Advice
Acquisition: Imaging
Preserving Files and Media: Write to CD/DVD
Preserving Files and Media: Digital Fingerprinting

PCs: Acquiring and Preserving Evidence: Forensic Disk Imaging

Audit Trail / Chain of Custody / Continuity
Specific Advice: Seizure and Acquisition
Forensic disk imaging methods
Forensic Disk Formats
Evidence Preservation
Screenshot Evidence

Smart Phones and Tablets: Evidence Acquisition and Preservation

The Basics
Contemporaneous Notes!
Detailed Procedures
Isolation
Extraction
Preservation
Analysis
iPhone Specifics
Android Specifics

Professional Software

Video, CCTV, Personal PVRs, DashCams, VideoDrones

Legalities
Evidential quality
Images into evidence
Types of CCTV and PVR
Permanently installed CCTV
BodyCams, “Action” Cameras, Covert Devices
Remotely Controlled Covert Devices
DashCams
Drones
File formats
Image enhancement
Facial recognition
Other Video Analysis Techniques+

CD, DVD and BD Forensics

Writeable, Re-Writeable, RAM
Physical Formats and Capacities
Logical Formats / File Formats
Finalising
Dates, times
Bootable CD and DVD Disks
ISO files
Where you think there may hidden and deleted material on a CD or DVD
Other forensic opportunities

Evidence from the Cloud and Out-Sourcers

A bit of history
The variety of models
Evidential and Legal Issues
Practicalities
Where one or more cloud-based files are required for litigation
Where there is a remote cloud-based database which is required either in its entirety or some form of extract of records
Where there is an entire virtual machine which must be acquired
Where a device back-up is desired

Network investigations, monitoring and surveillance

Limitations
Legalities

Traceroute
Call Data, Communications Data, Metadata, Lawful Intercept
Technologies and Levels of Intrusiveness
What is “Communications Data”?
International standards
Lawful Intercept - Phones
Lawful Intercept - Internet Data
Software Analysis

Cell Site Analysis

Mobile Phone Call Data Records
Mobile Phone / Mast Registration Data
Cell Site Location Analysis
Cell / Tower Dumps
IMSI catchers
On-phone records:
Spy programs
Other forms of Geolocation

Emails

How email works
Traditional Email's Two Versions
Where is the email evidence to be found?
Emails as Evidence
Acquisition and Preservation: “Traditional” Email
Email Attachments: Evidential Acquisition
Web Mail: Evidential Acquisition
Police Powers
Analysing emails and email archives
Email Threading
Email Headers
More advanced email analyses
Proof of Delivery
Encrypted Email
Web correspondence forms
Fax

SMS – Text Messaging

Legalities
Evidence acquisition and preservation
Screen capture
Data download

Data from Message Service Provider
Cloud Backup
Author Tracing

Social Media Networks: evidence

Legalities
Social Media History
OSINT
Evidence Acquisition: general principles
Evidence Acquisition: Some specific examples
Twitter
Facebook
Social Media Forensics
Author Tracing / Attribution

Evidence from the Web

Capturing web-based evidence: some background
Capturing web-based evidence: objectives and tactics
Capturing a web page
Capturing an entire website
Capturing live web activity
Internet Archive / WayBack machine
Google's Cache
Tracing ownership of a website
Browser cache
Professional Examination Routes: Web Servers

VOIP / Internet Telephony

VoIP Evidence
Skype
FaceTime
Other Services

Identity Theft and Card Frauds

Mutual Obligations
Identity Theft in Overview
Example 1: mass attack on individuals
Example 2: consequences of device theft/loss
Example 3: targeted attack on individuals, SMEs
Example 4: Capture via fake WiFi hotspot
Example 5: Capture and Clone by NFC
Example 6: hardware attack on financial institutions and those who use them

Example 7: attack on businesses
How Identity Theft is detected
How to react to a suspected Identity Theft

Attribution: Tracing on the Internet: IP Addresses and more

IP addresses
The shortfall: IP v4 and IP v6
Overcoming the shortfall
Limitations of NAT and DHCP
Traceroute
UUIDs / GUIDs
Email Tracing
Social Media Tracing
Other means of attribution
Law enforcement investigative methods

Authenticating Files and Documents; MetaData and Digital Signatures;

Content Authentication
Situations and Motivations
Where has the questioned file come from?
Backups and alternate versions
How has the file been acquired and preserved?
Are the technical details consistent?
Date/Time Stamps
MetaData
On Device Indicators
Linguistic Forensics
Photo files
Cryptography and Digitally Signed documents
File Hashing
Digital signatures
Safeguarding files from illegal copying

Biometric Evidence

Biometric Systems in General
Contexts
Efficacy Tests
An example: fingerprints
Voice biometrics
Facial recognition
Keystroke Biometrics

BIOS: Accessing

On Older PCs with “traditional” BIOS
On UEFI PCs
Boot Options

Computer Intrusion as an Investigatory Route

Confidentiality, Professional Privilege and Redaction

Redacted documents
Redacted Disk Images
Redacted email archives

Data Hiding and Covert Communications

Hidden Files, Folders
Steganography
Within Word
Hidden webpages and hidden data within webpages
Hidden web sites and Internet traffic
Hidden Internet traffic
TOR Network
Secure Hidden Email
End-to-End Encrypted Messaging
Unsaved Webmail
Data Hiding in Social Media

Data Recovery Methods, Data Carving, “Unallocated Space” etc.

Simple Data Hard Disk Data Recovery
Recovery of Fragments
Recovery of Deleted Folders
Keyword Searching for File Fragments
Dates when deletion occurred
Volume Shadow Copies
Data Recovery from RAID arrays
Recovery of Deleted Data in Tablets and Mobile Phones
Recovery from Memory Cards
Data Wiping Programs
Data remanence

Date and Time Stamps

Time Sources
Log Files

Epoch Time
Chronologies and event reconstruction; date/time stamps

File Hashing

File Sharing, Peer-to-Peer, P2P

Newsgroup P2P
P2P Forensics

Geolocation Evidence

GPS
Mobile phone geolocation data
Wi-Fi hotspots
ANPR
Getting hold of GPS data as evidence
Law Enforcement Powers / Criminal Proceedings
Civil Proceedings: Devices you own and control
Civil proceedings: Information held by third parties to which you have automatic access
Civil proceedings: Information about you held by third parties to which you do not have automatic access
Civil Proceedings: Information about others held by third parties

Hacking: evaluating the evidence

Priorities
Top Level Questions

Internet Browser Histories

Cookies
Private Browsing

IoT Forensics

What is IoT?
Where might IoT forensics be useful ?
Value for Money

Jailbreaking and Rooting

Key loggers
Hardware keyloggers
Software keyloggers
Keystrokes as biometric identifiers

Malware

Responsibility for Consequences of Infection
Identification
Identification Practicalities
Explanation
Means of Arrival
Damage Assessment and Causation
Types of malware: terminology

Memory Cards, USB sticks

Memory cards in general
USB storage
Data Preservation and Acquisition
High Street Data Recovery Products
Should you keep the original?
Has a USB device been connected to a PC?

Near Field Communications - NFC, RFID tags

Security Issues

PCs: Examining and Analysing

“Passive” and “Live” Modes of Examination.
What to use for your examination
Hard Disks and Partitions
Disk File Systems
Checking Date and Time
Key Locations
Questions about usage of the computer
Essential Locations in Windows 7 and 8.1 and 10
Who uses the computer?
What programs are being run?
MacOS
Specific Areas for Investigation
Web activity
Emails
Fax
Skype and VOIP
Social Media
File Sharing – P2P
Hidden Areas and Features on PC Disks
Swap and Hibernation Files
Registry

Log and configuration files: system
Log and configuration files: applications etc
Restore Points
Deleted Material
Search Techniques
Full Text Retrieval facilities
Whole Disk Forensic Search
Email-specific tools
Disk Viewing

Photos, Digital Cameras, Video Analysis and EXIF Data

Forensic handling of photo evidence
Identification
Acquisition
Analysis
EXIF MetaData
Detecting photo manipulation
Device identification

Printer forensics

Laser printers
Inkjet printers
Font Forensics

Preservation: Screen Captures

Specific methods: PCs
Windows
MacOS/
Specific methods: smartphones and tablets

Secure Data Destruction

Servers and Network Storage Devices

NAS
Servers
Virtual Servers

SIM cards

SMS – Text Messaging

Legalities
Evidence acquisition and preservation
Screen capture
Data download
Data from Message Service Provider
Cloud Backup
Author Tracing

Usage Monitoring Programs

Law, Ethics
Principles
PC Monitoring Programs
Smart phones and tablets
Internet and LAN Traffic
Evidence Collection
Bug technology

Video Piracy

Sources of Pirated Material
Streaming video
Distribution
Live Reception
Other Copying methods
Evidence
DVD sellers
File-Sharing Systems: Investigatory Methods
Where computers have been seized
Seized STBs

Virtual Machines

VMs in Forensic Examination
Acquiring and Preserving VMs

Instructing Experts

Formulating the Requirement
Identifying expertise
Costs
Staged Instructions
Expert Advisors and Expert Witnesses

Advice for Lawyers

Calculating Losses

Types of Loss: the basics
Fraud Losses
Compromise of 3rd party Personal Data
Malware attack
DDoS attack
Loss of Trade Secrets
Piracy
Definitions of “cybercrime”
Losses to whom?

E-Disclosure and E-Discovery

Civil Procedure
Handling large quantities of data
Third-Party Disclosure in Civil Proceedings
Criminal Procedure

Problems of Legal Professional Privilege and Confidentiality

Common defences and how they are rebutted

How this book came to be written

Glossary