

# The Essential Workshop

## Digital Forensics and E-Discovery

**Seamus E. Byrne**

Australian Lawyer

20 July 2009

For the LexisNexis Hong Kong E-Discovery and Digital Forensics Conference

# Today

- **Introduction**

- Your Presenter
- Your Presentation

- **Introduction to Digital Evidence**

- **Digital Forensics**

- Practice and Procedure
- Best Practice Guidelines and Standards

- **Electronic Discovery (E-Discovery)**

- Practice and Procedure
- Electronic Discovery Reference Model (**EDRM**) Workflow

# Digital Evidence Historical Perspective

- Until recently, civilization has solely relied upon physical information storage
- **Documents are the basic unit of information storage**
  - “*documentum*” = proof
  - Data may constitute information
  - Information may constitute a document
  - Select documents may be considered a record
- ***Evidence Ordinance***, Cap 8
  - Document means “*anything in which information of any description is recorded*”
- 98% of documents in today’s corporation are stored in electronic form only
  - Created as electronic documents
  - Paper documents converted to electronic form

# Digital Evidence Historical Perspective



## Industrial Revolution

- Typewriter
- Carbon paper
- Filing cabinet



## Information Revolution

c. 1960

- Mainframe computer
- Xerox photocopier
- Magnetic storage



## Information Revolution

c.1985

- Personal computer
- Computer networks
- Optical storage



## Information Revolution

c. 1995-

- Portable computing
- The Internet
- Solid-state storage

## Digital Evidence Key Features

- **Metadata** or “*data about the data*”
- **Easily copied** to defy the physical concept of an “*authentic original*”
- **Easily altered**, even without human intervention, to blur “*integrity*”
- **Easily deleted**, and often, recovery may present an onerous task
- **Easily mismanaged**, particularly when the same electronic document is stored in, or synchronized to, many distributed locations
- The **volume** of electronic documents continues to increase

## Digital Evidence Storage and Deletion

- A **file system** is used to store, organize and retrieve data
- A file system is located within a **volume** on a **hard drive**
- Multiple volumes can be stored on one hard drive using **partitions**



# Digital Evidence Storage and Deletion

- **Common File Systems**

- File Allocation Table (**FAT**) - Microsoft Windows (Legacy), Portable Storage
- New Technology File System (**NTFS**) - Microsoft Windows (Modern)
- Hierarchical File System (**HFS**) - Apple Macintosh
- Third Extended File System (**ext3**) - Linux
- Universal Disc Format (**UDF**) - Optical Storage Media (CD, DVD)

# Digital Evidence Storage and Deletion

- File systems manage data files using an **index**
- When a data file is **stored to the file system**
  - The data file is recorded as an **index entry** in the index
  - The index entry contains **file system metadata**
  - The **active data file** is **allocated** to a location on the hard drive

## Digital Evidence Storage and Deletion

- When a data file is **deleted from the file system**
  - The data file **index entry is deleted**
  - The location on the hard drive that the data file was allocated to is marked as “*unallocated*”
  - **The actual data file is generally not deleted**, but may be overwritten, in part or whole, at a future date, if a new data file is stored to the now unallocated location
- Dependent on a number of variables, a deleted data file may be recovered

## Digital Evidence Storage and Deletion

- **Formatting**
  - Creates an “*empty file system*” within a volume on a hard drive;
  - Marks the entire volume unallocated, but does not permanently delete previously stored data files
- **Secure deletion and overwriting**
  - Endeavors to permanently delete both the index entry and the actual data file
  - Makes any data recovery process difficult, if not impossible
  - Popular utilities include Evidence Eliminator, Eraser and CCleaner

# Digital Evidence Storage and Deletion

- **Redundant Array of Inexpensive Disks (RAID)** technology is used to group multiple hard drives for redundancy or performance
  - Commonly found in computer servers and high-end personal computers
  - A volume and its file system may be distributed across multiple hard drives
- **RAID Level 1 - Mirroring**
  - Minimum 2 Hard Drives (1/2 Storage, 1/2 Redundancy)
- **RAID Level 5 - Distributed Parity**
  - Minimum 3 Hard Drives (2/3 Storage, 1/3 Redundancy)

# Digital Evidence Metadata

- Metadata comes in two flavors
  - **File system metadata** is stored independently by the file system and managed by the computer's operating system
  - **Document metadata** is typically embedded as part of the electronic document and managed by a specific software application
- Metadata is the **primary difference** between an electronic document in its native, electronic form and the same electronic document printed to paper

# Digital Evidence Metadata

File System		
<ul style="list-style-type: none"> <li>• <b>Electronic Document</b></li> <li>• <b>Metadata</b> <ul style="list-style-type: none"> <li>• File Name</li> <li>• Last Modified Date and Time (<b>M</b>)</li> <li>• Last Accessed Date and Time (<b>A</b>)</li> <li>• Creation Date and Time (<b>C</b>)</li> </ul> </li> </ul>		
Word Document	E-mail Message	JPEG Image
<ul style="list-style-type: none"> <li>• <b>Formatting</b></li> <li>• <b>Text</b></li> <li>• <b>Metadata</b> <ul style="list-style-type: none"> <li>• Author(s)</li> <li>• Creation Date and Time</li> <li>• Last Saved Date and Time</li> <li>• Last Printed Date and Time</li> <li>• Comments and Revision History (Track Changes)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Formatting</b></li> <li>• <b>Text</b></li> <li>• <b>Metadata (Header)</b> <ul style="list-style-type: none"> <li>• Sender</li> <li>• Recipients (To, CC, BCC)</li> <li>• Subject</li> <li>• Sent Date and Time</li> <li>• Routing Information</li> <li>• Attachment Information</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Image</b></li> <li>• <b>Metadata (EXIF)</b> <ul style="list-style-type: none"> <li>• Date Taken</li> <li>• Camera Make and Model</li> <li>• Geolocation (GPS)</li> </ul> </li> </ul>

# Digital Evidence Evidentiary Considerations

- Evidence **must be relevant** to a “*matter in question*”
- Evidence **must have a probative value** sufficient to satisfy the applicable burden of proof (civil or criminal)
  - **Authenticity** - Is this electronic document what it purports to be?
  - **Integrity** - Is the computer and technology infrastructure considered reliable?
  - **Authorship** - Was this electronic document actually authored by the computer or human referenced?
- Evidence **must be tendered** in accordance with relevant procedures (e.g. certification) and any other applicable laws (e.g. *Personal Data (Privacy) Ordinance*, Cap 486)

## Digital Evidence Evidentiary Considerations

- **Documentation** - Maintain detailed notes for all observations and tasks undertaken, including any errors encountered and mistakes made
- **Chain of Custody** - Maintain detailed custody logs, documenting all custody transfers, from collection to Court to destruction
- **Evidence Copies** - Remember Locard's exchange principle - Collect and analyze without (or with minimal) alteration
- **Overriding Consideration** - The digital evidence management practices used should be appropriate to the matter

## Digital Evidence Expert Opinion and Testimony

- How contentious is this matter?
- Do I require specialist expertise not readily possessed by the "everyday" information technology practitioner?
- Do I need to mitigate the risk of being unable to clearly explain the potential significance of digital evidence?

# Digital Evidence

## The Expert

- Should possess **multi-disciplinary background**
- May possess **tertiary qualifications**
- May possess **industry certifications**
  - Information Technology - CompTIA, Microsoft, Cisco
  - Information Security - Security+, CISSP
  - Digital Evidence (Neutral) - CCE, CFCE
  - Digital Evidence (Vendor Specific) - EnCE, ACE
- Must possess **demonstrated experience**

# Digital Forensics

## Definition

- Defined by McKemmish for the Australian Institute of Criminology (1999) as *“the process of **identifying, preserving, analyzing and presenting digital evidence** in a manner that is legally acceptable in any judicial or administrative hearing”*
- Also commonly referred to as computer forensics, forensic computing or forensic technology
- **Applied to resolve uncertainty in relation to a “digital event”**
  - Investigation (corporate or regulatory)
  - Litigation (civil or criminal)
- Can also play a key supporting role in contentious e-discovery matters

# Digital Forensics Identification

- Identifying the
  - **Types** of digital evidence required for preservation and analysis
  - **Sources** of digital evidence containing the types required
  - **Locations** of the potential sources of digital evidence
- Identification is a balancing exercise between
  - Identifying **sufficient digital evidence** to corroborate purported events
  - Identifying a **volume of data that will not jeopardize** the digital forensic process or exceed the capacity of allocated resources
  - **Legal constraints** (e.g. Search Warrant, Search (Anton Piller) Order)

# Digital Forensics Identification - Types

- **Business Records**
  - Documents, spreadsheets, presentations, databases and transaction logs
- **Communications**
  - Web browsing activity, messaging activity (E-mail/IM/SMS/VM), calendar entries, call logs
- **Multimedia**
  - Images, audio and video
- **Artifacts**
  - Recently logged-on users - Event Logs
  - Recently accessed data files and folders - Registry, Shortcut (Link) Files
  - Recently connected portable storage media - Registry, Event Logs
  - Recently deleted data files - Recycle Bin, INFO2 File

# Digital Forensics Identification - Sources



## Personal Computers

- Desktop and Notebook
- Portable Storage (Floppy, CD/DVD, USB)

## Computer Servers

- File
- Internet (Web, E-mail)
- Database
- Remote Access
- Storage (NAS, SAN, Tape)

## Communication

- Mobile Phone
- Smartphone and PDA
- GPS Navigation System
- Multifunction Printer

## Multimedia

- Media Player (iPod)
- Digital Still/Video Camera
- Digital Voice Recorder
- Digital Video Recorder
- Gaming (PS3, Xbox)

# Digital Forensics Identification - Locations

- Location is both electronic and physical
  - **Synchronization** means the same data may be located in multiple locations and you must efficiently prioritize
  - **Virtualization** technology is used to allow multiple computers to transparently operate from one physical computer
  - **Physical location** may mean a source is difficult or unlawful to access
- You may be unable to consult the client's technology personnel to assist

# Digital Forensics Preservation and Collection

- Once sources of digital evidence have been identified, steps should be taken to ensure that it is preserved for collection and analysis
- Preservation also includes understanding that some data may not be preserved
  - **Volatile data** - Data that is no longer available after a short time or once computer loses power (e.g. temporary system data, RAM memory)
  - **Non-volatile data** - Data that remains available even when computer loses power (e.g. user-created data stored on a hard drive)

# Digital Forensics Preservation and Collection

- Collection is the actual process used to make a verifiable copy of potential digital evidence, from its source to a destination for analysis
- **Collection Types**
  - Physical Forensic Imaging
  - Logical Forensic Imaging
  - File Copy
- **Collection Methods**
  - Dead
  - Live
- Understand the options available, their respective merits and resource requirements

# Digital Forensics Collection - Types

	Physical Forensic Imaging	Logical Forensic Imaging	File Copy
Purpose	<ul style="list-style-type: none"> <li>• Exact copy of all data on a hard drive</li> <li>• Includes all active and deleted data</li> <li>• Includes all privileged and confidential data</li> </ul>	<ul style="list-style-type: none"> <li>• Exact copy of specific active data (e.g. all Microsoft Word documents on a hard drive returning search hits for the keyword "wages")</li> </ul>	<ul style="list-style-type: none"> <li>• Copy of specific active data (e.g. all Microsoft Word documents within a folder)</li> </ul>
Integrity	<ul style="list-style-type: none"> <li>• Stored within an "image"</li> <li>• Able to be verified using cryptographic hash (e.g. MD5, SHA-1, SHA-256)</li> </ul>	<ul style="list-style-type: none"> <li>• Stored within an "image"</li> <li>• Able to be verified using cryptographic hash</li> </ul>	<ul style="list-style-type: none"> <li>• Unless a proven copy method is used, data is subject to alteration</li> </ul>
Notes	<ul style="list-style-type: none"> <li>• Relatively slow but provides flexibility for detailed analysis</li> <li>• Creation of forensic image for an average hard drive takes 60-180 minutes (40GB-250GB)</li> </ul>	<ul style="list-style-type: none"> <li>• Relatively fast but analysis is limited to active data collected</li> <li>• Increasingly accepted as the default e-discovery collection type</li> </ul>	<ul style="list-style-type: none"> <li>• Fast but analysis is limited to active data collected</li> </ul>

# Digital Forensics Collection - Methods

	Dead	Live
Purpose	<ul style="list-style-type: none"> <li>• Data is collected after the computer is disconnected from standard operation</li> </ul>	<ul style="list-style-type: none"> <li>• Data is collected with minimal disruption to the computer's standard operation</li> </ul>
Method	<ul style="list-style-type: none"> <li>• Computer is disconnected by "pulling the plug" or "graceful shutdown"</li> <li>• Hard drive is connected via a write blocker to a forensic computer</li> <li>• Alternatively, use forensic boot disk may be used</li> <li>• Computer date and time is verified via BIOS</li> </ul>	<ul style="list-style-type: none"> <li>• Connection is made to computer whilst in operation, directly or via network</li> <li>• Computer date and time is verified via operating system analysis</li> </ul>
Notes	<ul style="list-style-type: none"> <li>• Traditionally accepted</li> <li>• Does not allow for most encrypted and volatile data</li> </ul>	<ul style="list-style-type: none"> <li>• Efficient for matters involving a large number of computers and limited forensic resources</li> <li>• Reduces traditional liability issues with shutting down "mission critical" computers</li> <li>• Allows for collection of most encrypted and volatile data</li> <li>• Increasingly accepted as the default e-discovery collection method</li> </ul>

# Digital Forensics Preservation and Collection



## Forensic Equipment

- Forensic Computers
- Forensic Write Blockers
- Adapters, Cables, etc.
- Boot Disks and Dongles
- Wiped Storage



## Technical Equipment

- Notebook, Pens, Pencils
- Computer Toolkit
- Digital Camera
- Handheld GPS (Time)
- Gloves, Torch, Batteries



## Transport

- Evidence Bags
- Containers and Labels
- Portable UPS
- Select Spare Parts
- Legal Documents



## Safe Custody

- Secure Storage
- Chain of Custody Logs

# Digital Forensics Analysis

- Analysis generally involves the reconstruction of past “*digital events*”
  - **What** is the event?
  - **Who** caused the event?
  - **When** did the event occur?
  - **How** did the event occur?

# Digital Forensics Analysis

- **Searching** for electronic documents responsive to specific a search query, date range or file type
- Analyzing **user activity** and reconstructing **timelines** of computer, network, web browsing and e-mail events, including the creation, access to, and copying of electronic documents
- Analyzing **authenticity** of an electronic document or e-mail
- Performing **data recovery** - deleted, password-protected, encrypted, compressed

# Digital Forensics Analysis - Casey's Certainty Scale

Certainty Level	Evidence Description	Qualification
<b>C0</b>	● Contradicts known facts	<b>Incorrect</b>
<b>C1</b>	● Highly questionable	<b>Highly uncertain</b>
<b>C2</b>	● One source of evidence that is <b>not protected against tampering</b>	<b>Somewhat uncertain</b>
<b>C3</b>	● One or more sources that are <b>more difficult to tamper with</b> ● Insufficient evidence to support a firm conclusion	<b>Possible</b>
<b>C4</b>	● One or more sources that are <b>protected against tampering</b> ● Verified by independent sources	<b>Probable</b>
<b>C5</b>	● One or more sources that are <b>protected against tampering</b> ● Verified by independent sources that are <b>also protected against tampering</b>	<b>Almost certain</b>
<b>C6</b>	● <b>Tamper proof</b> and unquestionable	<b>Certain*</b>

## Digital Forensics Analysis - Case Study

- John recently purchased Michael's business
- John has identified an anomaly between reports generated by the business' computerized accounting system software and an invoice dated 1 January 2008 provided prior to purchase by Michael, as a paper printout
- John can find no record of the invoice in the accounting system
- The invoice also looks slightly different to invoices typically produced by the accounting system
- John believes that Michael may have forged the invoice

## Digital Forensics Analysis - Case Study

- You perform a keyword search for the term "*invoice*" and manually review the results to identify a folder on the hard drive named "*Unsorted Invoices*"
- The folder contains one (1) deleted Microsoft Excel spreadsheet
- You recover the deleted spreadsheet and identify that the spreadsheet is password-protected
- Using a password cracking utility, you identify the spreadsheet's password as "*secret123*"
- You access the spreadsheet contents and it appears to match the printed invoice previously provided

## Digital Forensics Analysis - Case Study

- The spreadsheet's file system and document metadata reflects that the spreadsheet containing the invoice was created on 1 November 2008, 11 months after it was purported issued
- Document metadata reflects that the spreadsheet was created by the computer user "*Michael*" and was last printed on 1 November 2008
- You analyze the Print Spool folder and recover deleted artifacts which support the contention that a copy of the spreadsheet was printed from the computer on 1 November 2008
- You perform a timeline analysis of activity on the hard drive and analyze other available artifacts to verify operational reliability of the computer, including the computer clock's date and time

## Digital Forensics Presentation

- **Report preparation**
  - Prepare in accordance with Court requirements
  - No standard layout
  - Understand the audience
  - Avoid technical terminology overload
  - Use an appendix wisely
- **Court attendance**
  - Potentially months or years later

# Digital Forensics Presentation

- HIS HONOUR: Mr Couper?
- MR COUPER: I'll call Mr Byrne, if your Honour pleases.
- HIS HONOUR: Yes.
- MR COUPER: We'll see if all this technology is what it's cracked up to be.
- HIS HONOUR: Is that what you're going to ask Mr Byrne?
- MR COUPER: More or less, your Honour.

# Digital Forensics Further Reading

- **Reference Materials**

- DOJ, [Search and Seizure Manual](#) (USA)
- NIJ, [Electronic Crime Scene Investigation: A Guide for First Responders](#) (USA)
- ACPO, [Good Practice Guide for Computer-Based Electronic Evidence](#) (UK)
- BS 10008, Evidential Weight and Legal Admissibility of Electronic Information
- AS HB 171-2003, Guidelines for the Management of IT Evidence
- NIST, [Computer Forensic Tool Testing Project](#) (USA)

- **Websites**

- [The Electronic Evidence Information Center](#)
- [Forensic Focus](#)

# E-Discovery Definition

- **Traditional E-Discovery**

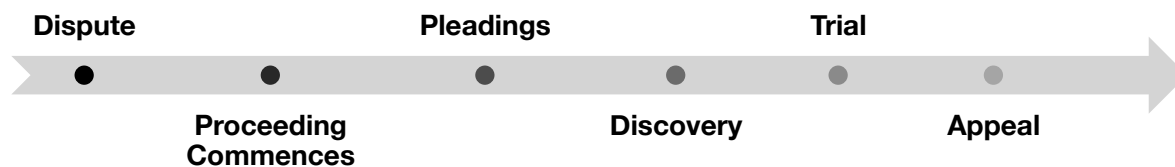
- Management of discoverable paper documents by conversion to electronic form

- **Modern E-Discovery**

- Management of discoverable electronic documents in electronic form

- **Today = Transitional Phase**

# E-Discovery Litigation Workflow



- Dispute arises between two or more parties based on fact and/or law
- Proceeding commences by the plaintiff preparing, filing and serving a claim
- Upon service, the defendant acknowledges their intention to contest the claim
- Pleadings endeavor to settle undisputed matters by refining the plaintiff's claim and the defendant's defense (often over the course of multiple replies)
- **Pleadings should focus the dispute, and consequently, should limit discovery**
- Discovery includes "*the disclosure, and subject to privilege, inspection of an opponent's documents*" (Cairns, 2007)

# E-Discovery EDRM Workflow

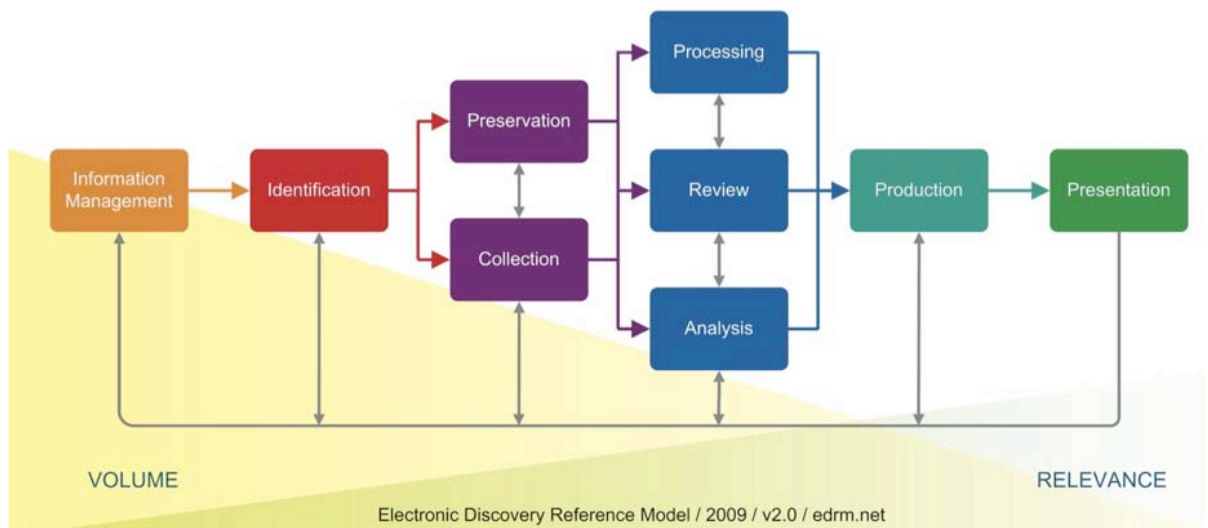


Image Copyright 2005-2009 Socha Consulting LLC and Gelbmann & Associates.

# E-Discovery Civil Justice Reforms

- **Order 24, *The Rules of the High Court*, Cap 4A**
  - Emphasizes greater case management
  - Retains *Peruvian Guano* principles
  - Court has express powers to limit the “scope” of discovery (O 24, r 15A)
- **Practice Direction 5.2**
  - “The parties should proceed with discovery without the need to wait for an order of the Court; and
  - try to agree on the directions for modifying discovery obligations (e.g. limiting discovery to specified issues); or
  - on the manner of their implementation (e.g. exchanging copy documents without the need to prepare lists of documents) with a view to achieving economies in respect of discovery.”

# E-Discovery Information Management

- Consider your organization's **litigation risk profile**
- If your "*electronic house*" is not in order, then the ability to efficiently manage litigation is significantly reduced
- **Proactive information management practices** serve as a measure of good corporate governance and risk mitigation
- Proactive does **NOT** mean keeping all of your electronic documents, including e-mail, forever

# E-Discovery Information Management



## First Steps

- Key Stakeholder Support
- Concise and Relevant Document Retention Policy (**DRP**)



## Use of Technology

- Appropriate Infrastructure
- Clear Documentation



## On-Going Compliance

- Employee Training
- Regular Review



## Emerging Trends

- Internal Checklists
- E-Discovery Champions
- Information Packets
- Preferred Suppliers Panel

## E-Discovery Information Management

- What potentially discoverable documents are in your possession, custody or control?
- What documents do you considered to be “**reasonably accessible**”?
- What resources would be required in order to give discovery of “**reasonably inaccessible**” documents?
- What documents are **no longer** in your possession, custody or control?
- Has document destruction been performed in accordance with your organization’s DRP?
- How do you **promote and enforce** your DRP?

## E-Discovery Identification

- Identify the documents (or document categories) which constitute the ordered or agreed “*scope*” of potentially discoverable documents in your possession, custody or power
- Refer to the digital forensic identification strategy
  - Types
  - Sources
  - Locations
- In contrast to digital forensics, e-discovery generally only involves active technology to facilitate searchable text for non-searchable documents, and does not extend to deleted documents at first instance
- **Early Case Assessment (ECA)** technology allows lawyers to develop informed early case strategy before significant resources are allocated to litigation, including e-discovery

## E-Discovery Preservation and Collection

- Determine the most efficient method of preserving and collecting potentially discoverable documents
- Refer to digital forensic preservation and collection options
- **Legal Hold** technology prevents destruction of electronic documents by
  - Applying security controls to a set of selected documents once litigation is anticipated or has commenced
  - Sending frequent reminders to key custodians as to which documents must be preserved and their individual role in assisting the organization to comply with their discovery obligations

## E-Discovery Processing

- Processing potentially discoverable documents into a **readable and usable** form for analysis and review
  - Electronic Documents
  - Paper Documents
- Understand limitations of your processing tools
- May be undertaken in-house using e-discovery technology or by an external service provider

## E-Discovery Processing - Electronic

- Automated extraction of document and e-mail metadata
- Extract compressed data (e.g. documents in ZIP archives, backup tapes)
- Extract password-protected or encrypted data
- Use **optical character recognition (OCR)** technology to facilitate searchable text for non-searchable documents
- Conversion of audio files to transcript
- Management of complex and proprietary document types (e.g. databases)
- Management of non-English text (Unicode, traditional code pages)

## E-Discovery Processing - Paper

- Scan paper documents to an electronic image format (e.g. TIFF, PDF)
- Manual extraction of document metadata (e.g. Title, Author, Date)
- OCR technology to facilitate searchable text

# E-Discovery Analysis

- Analysis of processed potentially discoverable documents prior to review
- Analysis and review is often treated as an **iterative cycle**
- If the appropriate technology is in place, the majority of analysis tasks can be performed at the Identification stage
- Understand limitations of your analysis tool
- May be undertaken in-house using e-discovery technology or by an external service provider

# E-Discovery Analysis

- **Key Custodians or Storage Locations**
  - Date Ranges
  - File Types
- **Search Queries**
  - Keywords
  - Concept searching
- **De-Duplication**
  - Exact de-duplication
  - Near de-duplication
  - E-mail threading

## E-Discovery Analysis - Considerations

- “Sampling” to validate keyword search queries and other analysis methods
- Agreement to analysis procedure (e.g. keyword search query terms) with opposing party
- Searching non-English text (e.g. tokenization)

## E-Discovery Review

- Lawyers review the filtered set of documents
- At this time, you may also redact (i.e. mask) part-privileged and/or part-confidential documents
- **Most time and cost intensive stage of discovery if not done properly!**
- Documents may be hosted in-house using a document review platform or via an external service provider

# E-Discovery Review - Platforms

- **Tasks**

- Search
- Review
- Classify

- **Considerations**

- Ease of use
- Functionality
- Cost
- Scalability
- Support
- What are the other parties using?

# E-Discovery Production

- Perform final validation and quality assurance
- Prepare **List of Documents** (Form 26) and verification **Affidavit** (Form 27)
- Produce discoverable documents as ordered or agreed
  - Convert electronic documents to an electronic image format (e.g. TIFF, PDF)
  - Assign Bates Number or Document ID to each (page of a) document
  - Create load file for opposing party to import into document review platform

## E-Discovery Presentation

- If the proceeding continues to trial, consider use of the Court's technology resources, including electronic court book facilities, to efficiently manage and display documents within the Court

## Closing Remarks

- Digital forensics is a complex and fast-moving discipline, but one that can support all types of investigations and litigations involving digital evidence
- Unfortunately, the discovery process is not yet as easy, fast, or cost effective as it should or could be!
- Any efficiency (and conversely, delay) to be derived from fulfilling your discovery obligations is largely dependent upon your information management practices
- The EDRM provides a stage-based approach for e-discovery and reduces the likelihood of technology overtaking the real legal issues
- Consult specialist expertise **at the earliest opportunity** to mitigate digital forensic and e-discovery pitfalls
- Be prepared, be informed - Instant knowledge is power!

# Thank You

If you have any questions or feedback regarding this presentation please contact

**Seamus E. Byrne**

+61 (0)416 214 388

[seamus@seamusbyrne.com](mailto:seamus@seamusbyrne.com)

<http://www.seamusbyrne.com>