



# Identification and Collection Methodologies for Electronically Stored Information (ESI)

Seamus E. Byrne (eDiscovery Tools) and Geoffrey Lambert (KordaMentha)

## **Please Read - Disclaimer**

This presentation is made available by [Seamus E. Byrne](#) and Geoffrey Lambert, Australian legal practitioners, for educational purposes only.

Content is not to be used as legal opinion or as a substitute to qualified matter-specific legal advisory within your jurisdiction.

All endeavours have been made to ensure content accuracy as at June 2008.

For the [VSCL](#) Legal Technology Conference 2008 – Litigation Management Stream - Australian English (Duration: 40 minutes, Extended Public Draft)

# Today



- **Preliminary**
  - Your Presentation
  - Your Presenters
- **Definitions**
  - Identification
  - Preservation and Collection
- **Key Events**
- **Key Considerations**
  - Operational
  - Technical
  - Legal
- **Closing Remark**

# Your Presentation



- **Coverage**

- Australia
- Primarily Civil Litigation
- Guiding Principles and Best Practice

- **Primary Audience**

- Australian Litigators
- Litigation Support Personnel
- Computer Forensic Practitioners

# Your Presenters



## ■ **Seamus E. Byrne**

- Chief Operating Officer, **eDiscovery Tools**
- Lawyer and Computer Forensic Expert (CISSP, CCE, EnCE)
- Co-Drafted Federal Court of Australia Practice Note
- eDiscovery advisor and counsellor to a number of **S&P/ASX 200** companies

## ■ **Geoffrey Lambert**

- Director, **KordaMentha**
- Lawyer and Computer Forensic Expert
- Specialist International Legal Panel, **International Journal of Digital Forensics**
- Regulatory electronic evidence management specialist (**ACCC**, **ATO**)



## ■ Identification

- “...Is the time that the **types, source and location** of **all ESI** must be **identified for preservation**” ([Arkfeld on Electronic Discovery and Evidence](#), 2<sup>nd</sup> ed.)

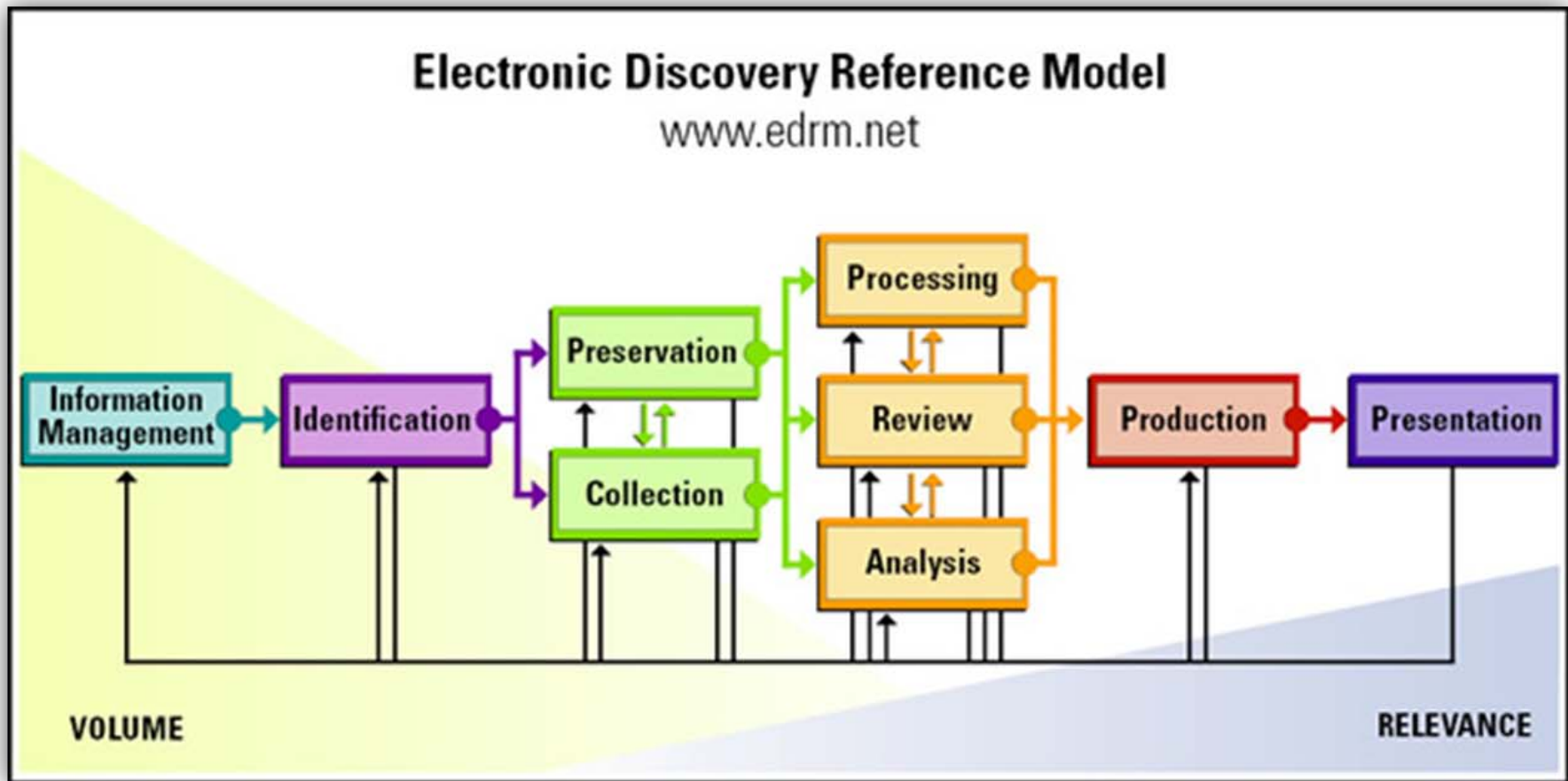
## ■ Preservation and Collection

- **Refined** identification, protective management (and agreement) as to ‘potentially relevant’ ESI
- **Collection** of ‘potentially relevant’ ESI for **processing, analysis and review**

## ■ Methodology

- “a **system of methods** used in a particular field” ([Oxford English Dictionary](#))

# EDRM Workflow



© 2005-2007 Socha Consulting LLC and Gelbmann & Associates. All Rights Reserved.  
See also: [EDRM Evergreen Project](#) (2007-2008).

# Key Events



- **‘Trigger Events’** for Identification and Collection
- **Civil Litigation**
  - **Search Order (Anton Piller)**
    - **Applicant:** Preparation and Upon Attendance
    - **Respondent:** Upon Notice
  - **Discovery**
    - **Yesterday:** Upon Notice of Discovery
    - **Today:** Both Parties for **Pre-Discovery Conference (PDC)** (as Discovery Directions Hearing)
- **Criminal or Regulatory Investigation**
  - **Investigatory Body:** Preparation and Upon Attendance
  - **Target:** Upon Notice
- **Internal (Corporate) Investigation**
  - Dictated by seriousness of ‘trigger event’ and existing internal procedure

# Key Considerations



Consideration	Elements
<b>Operational</b>	<ul style="list-style-type: none"><li>•Commercial Impact</li><li>•Project Management</li><li>•Personnel and Expertise</li></ul>
<b>Technical</b>	<ul style="list-style-type: none"><li>•Environments</li><li>•Advances</li></ul>
<b>Legal</b>	<ul style="list-style-type: none"><li>•Relevant Issues</li><li>•Strategy</li></ul>

All considerations possess an **inherent risk component**, which is to be considered, and appropriately mitigated, at each stage.

# Identification Operational



- Driven by ‘**Trigger Event**’
  - Type
  - Severity
- **Commercial Impact**
  - Ensure clear and concise **first communications**
  - Manage key stakeholder (e.g. employee) **concerns and potential fear**
- **Project Management**
  - Assess Court-imposed **timeframes** (and where possible, anticipate)
  - Be prepared to knowledgeably negotiate for ‘cost containment’
- **Personnel and Expertise**
  - Identify key **internal** and **external technical and legal personnel**
  - Meet with key personnel to discuss identification strategy
- **Documentation**
  - Diligently document all key activities

# Identification Technical – ESI Types



- Includes, **but is not limited to**:
  - E-mails
  - Documents
  - Spreadsheets
  - Databases
  - Presentations
  - Images
  - Logs (e.g. Activity, Transaction, Instant Messaging)
  - Audio (e.g. Voicemail)
  - Video

# Identification

## Technical – ESI Sources



### Common ESI Sources

#### ■ Personal Computers

- Desktop
- Notebook

#### ■ Computer Servers

- File Servers (e.g. [NAS](#))
- E-mail Servers
- Fax Servers
- Remote Access Servers

#### ■ Tape Backups

### Potential ESI Sources

#### ■ Communication Devices

- Mobile Phones and [BlackBerry](#)
- Personal Digital Assistants (PDAs)
- Modern Photocopiers

#### ■ Consumer Devices

- [iPod/MP3](#) Players
- Digital Cameras
- Digital Voice Recorders

#### ■ Portable Storage

- Optical Media (CD, DVD, [Blu-ray](#))
- Memory Cards
- Flash Storage (e.g. [USB](#))
- External Hard Drives

#### ■ Internet-Based Repositories

# Identification

## Technical – ESI Locations



- **Location is:**
  - Electronic; and
  - Physical (Geographical)
- Understand common **environmental synchronisations** of ESI sources (i.e. *multiple locations where the same ESI subsists*) in anticipation of having to **advise upon** and/or **prioritise locations for collection**
- Examples
  - Microsoft Outlook (Client) and Microsoft Exchange (Server)
  - Apple iPhone (Mobile Phone) and
    - Microsoft Exchange (Server)
    - MobileMe (Internet-Based Repository, Cloud Computing)



## ■ **Ideal World**

- Client has taken steps towards '**litigation readiness**'
  - Policy and Procedure
  - Training
  - Technology Implementation (e.g. EDRMS)
  - Regular Review

## ■ **Real World**

- ?

# Identification

## Legal - Document



- **Unlike the US FRCP, Australia defines ESI within the umbrella definition of a ‘document’**
  - *Acts Interpretation Act 1901 (Cth) s 25;*
  - *Evidence Act 1995 (Cth) Dictionary*
- **Includes ‘metadata’**
  - *"It is clear that embedded electronic information in relation to relevant documents, including the information embodied in electronic metadata, is discoverable"*
    - *Jarra Creek Central Packing Shed v Amcor Limited* [\[2006\] FCA 1802](#) (per Tamberlin J).

# Identification

## Legal – Federal Court



- **Pre-Discovery Conference (PDC)**
  - Parties must ‘meet and confer’ **prior to PDC**
  - Pre-Discovery Conference Checklist (**PDCC**)
    - **Relevance**
    - **Reasonable Search** (and **Reasonably Inaccessible**)
    - **Electronic Document Strategies**
    - **Preservation**
    - Discovery Scope
    - Time Schedule
    - Privilege
    - Engagement of Service Providers
    - Document Management Protocol (**Default or Advanced**)
    - **Areas of Dispute**

# Identification

## Legal – Federal Court



- **Order 15, rule 2(5)** provides the matter-specific variables a party may consider in 'making a reasonable search':
  - *(a) the nature and complexity of the proceedings; and*
  - *(b) the number of documents involved; and*
  - *(c) the ease and cost of retrieving a document; and*
  - *(d) the significance of any document likely to be found; and*
  - *(e) any other relevant matter.*
  
- **Order 15, rule 2(6)**
  - *If the party **does not search** for a category or class of document, the party must include in the list of documents a statement of the category or class of document not searched for **and the reason why**.*



- **Commercial Impact**
  - Technology Downtime?
- **Project Management**
  - Reliant upon flow-on strategy devised at Identification stage
- **Personnel and Expertise**
  - Increasingly, tools are available to facilitate a range of people (i.e. **non-forensic practitioners**) to collect 'potentially relevant' ESI in a **forensically acceptable and justifiable manner**



## ■ Copy Type

- Physical Forensic Imaging
- Logical Forensic Imaging
- File Copy

## ■ Copy Method

- Dead (Traditional)
- Live (Emerging)



## ■ Physical Forensic Imaging

- An exact copy (bitstream) of **all data** from a physically imaged ESI source
  - Active and Deleted
  - Relevant and Non-Relevant
  - Privileged and Confidential
- Relatively slow but provides flexibility for in-depth analysis
- Creation of a '**forensic image**' for an average hard drive generally takes 60 – 180 minutes (40GB – 250GB)



## ■ Logical Forensic Imaging

- An **exact copy of specific data** (e.g. all Microsoft Word documents on a Server computer returning search hits to 'wages') in a **virtual container**
- Uses a **proven copying method** (e.g. with [MD5](#) or [SHA-256](#) verification) to ensure data integrity
- Awaiting widespread adoption by forensic practitioners

## ■ File Copy

- A logical copy of one or more **specific active** (*cf* deleted) data files (e.g. all Microsoft Word documents within a folder)
- **Unless** data is copied using a proven copying method, data will be altered
- Relatively fast but only allows the data files specifically copied to be analysed
- Further Reading: [Pinpoint Labs Whitepaper](#)



## ■ **Dead (Traditional) Copy Method**

- Computer is powered down and **offline** during copying process

## ■ **Live (Emerging) Copy Method**

- Creating a forensic image or copying data when a **computer is on**
- Typically reduces liability issues associated with shutting down mission-critical computers (e.g. Servers)
- Allows capture of **most** encrypted ESI



## ■ Write Blocker

- Similar to opening the write-protect tab on a floppy diskette, a write blocker is generally used to **ensure the preservation of ESI, and associated metadata, during collection - by making the ESI source 'read-only'**
- For example, a **hardware write blocker** (e.g. **Tableau T8**) is recommended to preserve ESI during collection from **USB storage devices** (e.g. USB external hard drive)

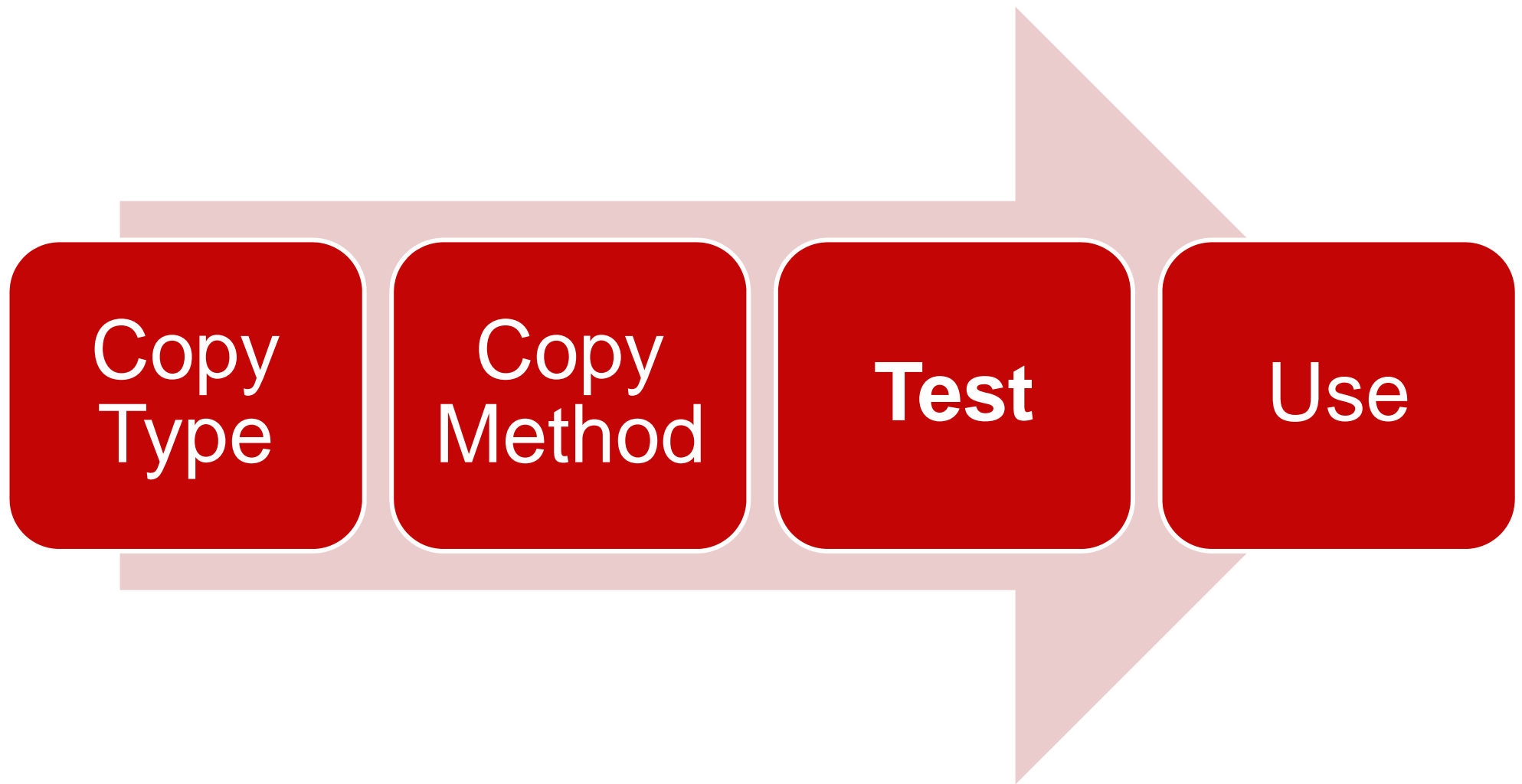


## ■ F-Response

- Uses Internet SCSI ([iSCSI](#)) to connect to a remote computer (over a computer network – i.e. LAN/WAN/Internet) which is then mounted as a **read-only physical storage device** on the local computer
- **Identification**
  - In conjunction with an ESI reporting software tool (e.g. [ShowSize](#) or [alternative](#)), F-Response facilitates an **efficient, yet low-cost ESI preview solution** for one (1) or more remote computers
- **Preservation and Collection**
  - **Reduces travel time** to physically attend a remote computer
  - Acts as a **conduit** to reduce the need for implementation of an enterprise-grade forensic collection software tool in specific circumstances
  - In conjunction with a file copy software tool (e.g. [Pinpoint Safecopy 2](#)), F-Response facilitates a **robust and justifiable ESI collection solution** for active data files stored on one (1) or more remote computers



Copy Type	Software Tools (Alphabetical)
Physical Forensic Imaging	<ul style="list-style-type: none"><li>• <a href="#"><u>AccessData FTK Imager</u></a></li><li>• <a href="#"><u>dd</u></a> (Unix/Linux)</li><li>• <a href="#"><u>EnCase Forensic</u></a></li><li>• <a href="#"><u>X-Ways Forensics</u></a></li></ul>
Logical Forensic Imaging	<ul style="list-style-type: none"><li>• AccessData FTK Imager</li><li>• EnCase Forensic</li></ul>
File Copy	<ul style="list-style-type: none"><li>• <a href="#"><u>Microsoft Robocopy</u></a></li><li>• <a href="#"><u>Pinpoint SafeCopy</u></a></li></ul>
Enterprise-Grade Forensic	<ul style="list-style-type: none"><li>• <a href="#"><u>AccessData eDiscovery</u></a></li><li>• <a href="#"><u>EnCase Enterprise</u></a></li><li>• <a href="#"><u>ProDiscover Investigator</u></a></li></ul>





## ■ Chain of Custody and Evidence Copies

- Managing electronic evidence in a documented manner without (or with minimal) alteration
- Appropriate evidence management procedures, including physical security

## ■ Best Practice

- *Guidelines for the Management of IT Evidence* (HB171-2003), Standards Australia

## ■ Privilege Management

- Attaches to confidential communications **as information**, and not documents as such



- ***Metso Minerals (Australia) v Kalra*** [\[2007\] FCA 2108](#)
  - Search Order
  - Underestimating the time to collect 'potentially relevant' ESI?
- ***Aristocrat Technologies v Global Gaming Supplies*** [\[2006\] FCA 1707](#)
  - Search Order
  - Highlighted the flow-on consequences of voluminous collection
- ***GT Corporation v Amare Safety*** [\[2007\] VSC 123](#)
  - *"I have no doubt that the manner in which [the applicant's] electronic discovery was provided, together with the complete lack of any index, has contributed significantly to the problems which have subsequently arisen"*

# Closing Remark



- The **identification and collection of evidence**, including ESI, is a small part of a much larger litigation process
- However, when mismanaged, the consequences can be devastating!
- For litigation support personnel, diligence of **all key considerations is mandatory**
- For litigators, source **proven expertise** and take **proactive steps** to plan and develop strategy for potential ‘trigger events’ - before your client encounters one!

# Thank You



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

**Seamus E. Byrne**

[sbyrne@ediscoverytools.com](mailto:sbyrne@ediscoverytools.com)

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

**Geoffrey Lambert**

[glambert@kordamentha.com](mailto:glambert@kordamentha.com)