

Fios

Electronic Evidence Collection in eDiscovery Process

Karl J. Flusche, CFE

Manager, Evidence Collection Services

Fios, Inc

(469) 387-2426



- eDiscovery Definition
- Terms Used
- Collection Steps
 - Types of Collection
 - Methods of Collection
- Specific Tools for Collection
- Other Techniques
- Summary



Definition of eDiscovery

eDiscovery (Electronic discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

Why important? Zubulake vs. UBS Warburg



Terms Used

- ESI – Electronically Stored Information
- Metadata – data associated with documents not normally visible within content
 - Data describing other data
 - File level - date created, modified, accessed
 - Application (OLE) level – creator, revision #
- Custodian – key person who is a owner or holder of ESI



- **Legally Defensible [manner]** – is comprehensive, maintains content integrity and preserves form, well documented by Chain-of-Custody procedures and can be authenticated.

- **Forensics** – Science used to answer questions of interest to the legal system
 - Roman times meant “before the forum”
 - Modern Times for ESI – application of scientific methods & technology in order to recover data from electronic/digital media



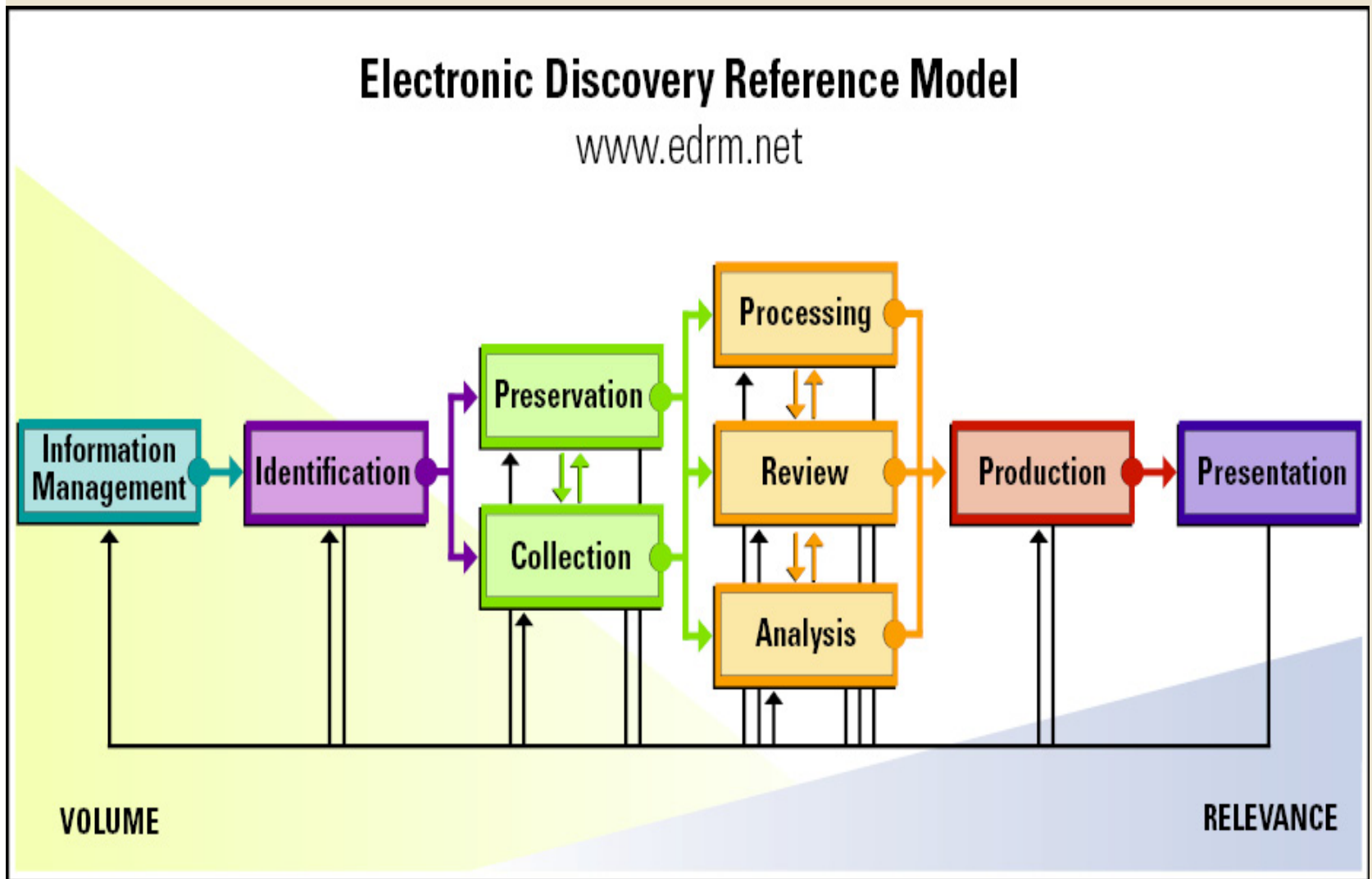
- **Forensic Copy** – legally defensible active file only copy of ESI; can be performed with common utilities
- **Forensic Image** –obtaining an image of a drive to allow for in-depth forensic analysis on the image, or to collect both active files and deleted files and fragments of files from slack space and unallocated space.



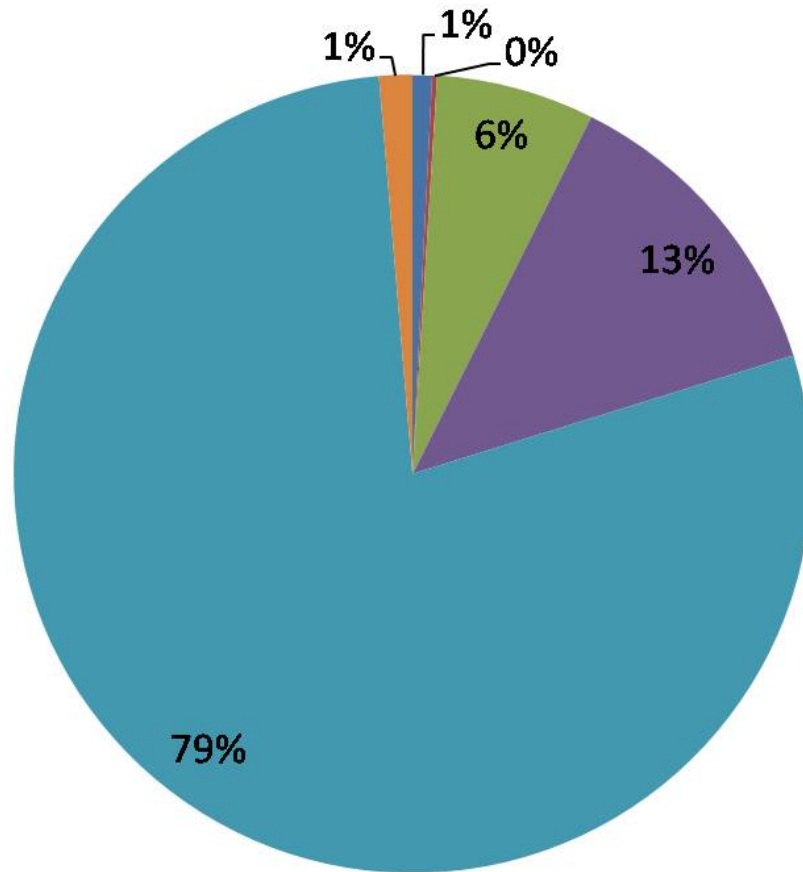
- **Deleted Files** – files that have been marked as deleted from the file system but not yet overwritten and still have intact data and structure (Recycle Bin is NOT).
- **Slack Space** – space between logical end of file (disk) and physical end of file (disk)
- **Unallocated Space** – space on a disk not allocated to a current file where fragments and leftover pieces of files could reside.



Fios Industry Model



eDiscovery Costs



- Identification
- Preservation
- Collection
- Processing
- Review
- Production



Collection Steps

- Define Sources of Data
- Define/ID Custodians
- Determine Method/Type Collection
- Prepare and Publish Collection Plan
- Schedule Collection Activity
- Assemble Resources and Execute
- Document and Report



Define Sources of Data

- Basic scoping of environment
 - Policy effect on infrastructure (or not)
 - Email system, retention policy
 - DMS or email archiving
 - Security or technical restrictions
- Server hosting, vendor, physical location
- Systems, OS, encryption/restrictions
- Work close with client IT Department to identify custodian access, potential areas of data storage



Define/ID Custodians

- Legal/Management interview custodians/key personnel
- Determine if personal (non-standard) sources of data exists
- Avoid custodian self-collection or self-determination of relevance
- Identify key custodians with different collection requirements



Determine Method/Type Collection

- Mainly Legal/Executive Management Decision
- Review pros/cons of each
- Availability of resources and risk acceptance
- Resolve issues before beginning collection
- Ensure complete, legally defensible collection with minimum business impact



Types of Collection

→ Client Self-Collected

- Drain on client IT resources, time, business
- Least expensive, max control

→ On-Site by Third-Party/Vendor

- Planning required, more expensive
- Small impact on business
- Costs can be shared with opposing

→ Empowered (Client performed with Vendor management)

- Excellent hybrid, balance in costs/impact
- “Remote-Empowered” good for isolated custodians

→ Remote (Third party tools)

- Expensive software to buy, install, support
- Good for on-going, not good for reactive



Methods of Collection

- User Discretion/Drag & Drop/ "email me"
- Forensic Copy (Active File Copy)
- Forensic Imaging (Deleted files/slack space)
- Restore from Tape/Archive/Old Media
- Content Export (DMS or email Archiving System)
- Data Base Report/Replication



Methods of Collection

	Pros	Cons	Remarks
User Discretion	Simple, Little skill, Fast, Easy, In-House, cheap	Spoil metadata, reliance on surface review	Common, not legally defensible
Forensic Copy	Ready to Process/load, broad capture	No deleted or slack space	Not good for Investigations, OK for servers
Forensic Image	Deleted & slack space, completeness	Specialized Skill, expensive, double time	Preferred for Investigations, not for servers
Tapes, Archives	Historical, cover "gap" periods	Tape life-cycle; restoration process	Older tapes often corrupted, disorganized



→ On-Site Culling?

- NIST filtering possible, can take time
- Date Cull good, supported by most utilities
 - Date accessed or created, last modified
 - Good for refresh collections
- By File type/extension impractical
 - Extensions can be changed, temp
- Location – “My Documents” only not valid
 - May be OK if legal review/risk acceptance
 - Consider custodian interviews
- Key word search time consuming
 - What if new keyword later?

“Collect Broadly, Filter Discretely”



→ Which is Most Legally Defensible?

- Forensic Copy?
- Forensic Image?
- Tape?

→ Answer – If properly executed, all can be legally defensible. Some methods more accepted/easier to prove.

→ Legal defensibility - is comprehensive, unaltered, documented and authenticated



Prepare and Publish Collection Plan

- Critical to Success – publish, and all sides/parties agree to their responsibilities
- Include custodian roadmap << KEY!
- Still be flexible to changing conditions
- Part of documentation process required to prove legal defensibility



Schedule Collection Activity

- Critical to minimize impact on business and custodians
- Best if custodian collection performed in multi-processing method vs. linear
- Prepare to overcome objections
 - “You’re not copying MY laptop!”
 - I’m too busy/important...
- Be creative – Conferences, after hours, ship out laptops via overnight



Assemble Resources/Execute

→ **Drives are cheap!**

- Use only NIB drives; Combine external bays with removable drives

→ **Take care of details:**

- ID/Meet POCs: Client, IT, Legal, Management
- Confirm address, location of servers, PCs, etc
- Hotels, FedEx locations, etc near client site

→ **Follow custodian road-map, adjust**

→ **Accommodate, reduce impact on custodians, business**



Assemble Resources/Execute (cont)

- Refer individual objections to legal/management team
- Secure data for transport/shipment to processing
 - FedEx Priority Overnight acceptable
 - Client may want additional protection from loss
 - Consider hardware/software encryption (planning)
 - Option to hand carry data
- Chain-of-Custody continues throughout processing and review



Document and Report

- Critical part of validation process
 - Chain-of-custody
 - Custodian road-map
 - Exceptions to Collection Plan
- Data amount collected to client ASAP
 - Processing costs usually based on sizing
 - Alert if too far over estimate
- Alert to any exceptions/re-collections
- Maintain accurate records until case closed/adjudicated



Specific Tools for Collection

- Robocopy for active collections on PCs
- CP for Apple, UNIX (preserve, recursive)
- DD, EnCase or FTK for images
 - Not good for servers due to business interruption
 - Can combine with robocopy or CP as needed
- Paraben Tools for cell phones/PDAs
- ExMerge for Outlook, Notes in clear
 - Groupwise best by tape backup!
- Involve providers for web-based email
 - With custodian permission, log in direct and acquire



Other Techniques for Preservation (not collection)

→ Keep key custodian's hard drives

- Drives are cheap!
- Preservation vs. Collection
- Keep secured/Evidence Locker/Single Point Access

→ Backup to tape/image HD

- Discovery risk, can also be effective contingency method

→ CD/DVD for email or already zipped or compressed files

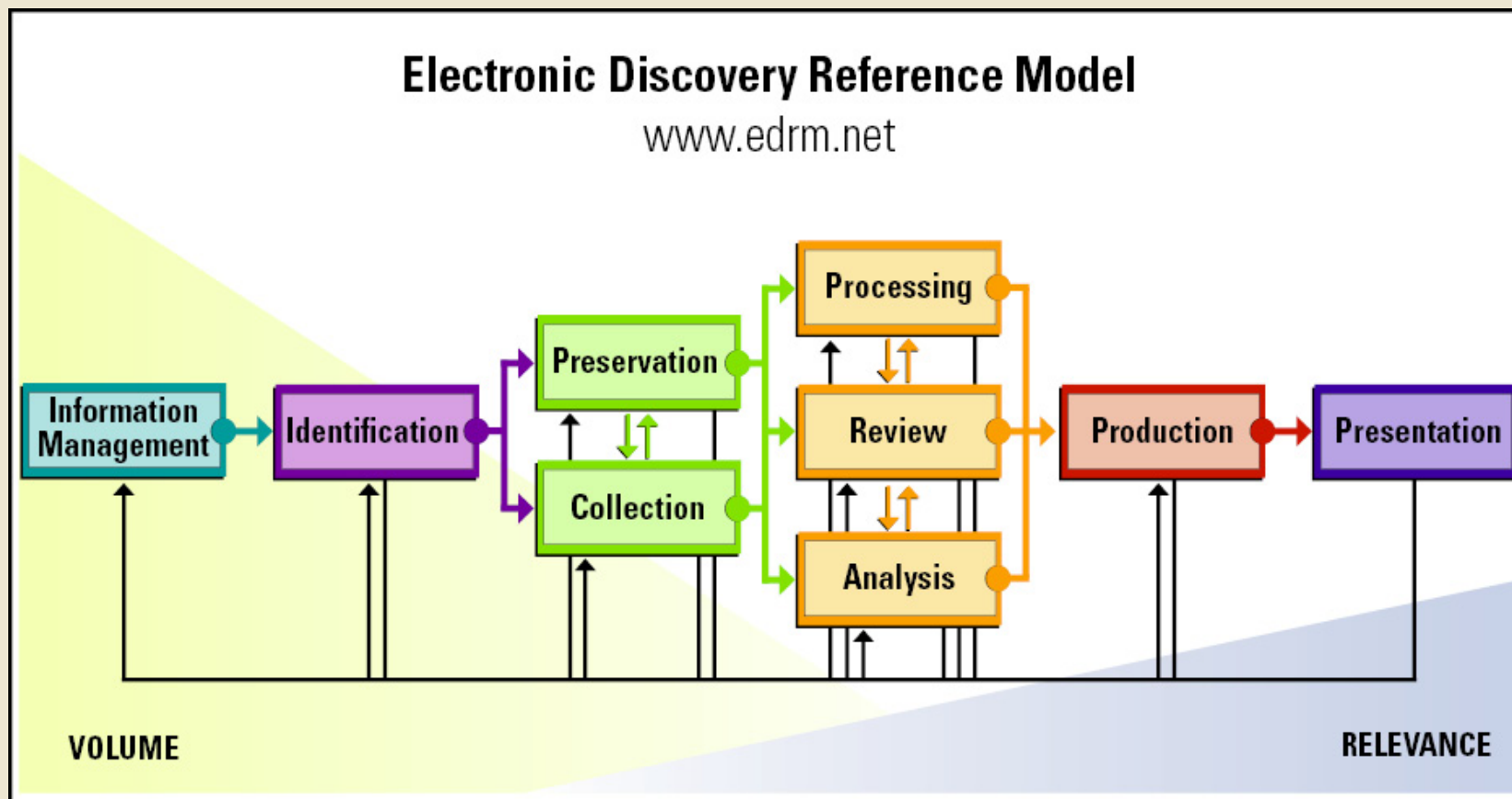
- Where file level meta-data is not critical



Summary

- eDiscovery is a process of many steps, but ID and Collection of data is key
- Client/Legal must make informed decisions on method and type, available resources, and risk tolerance
- Effective and well defined plan required
- Collection must be legally defensible or review and production invalid





Fios Additional Resources



DiscoveryResources.org

Fios Inc. sponsors this useful, informative site, providing articles, news and Web links related to electronic discovery. It links to case law, rules and regulations, CLE Webcasts, news articles and more.

Law Technology News; December 20, 2004

ComplianceResources.org

An independent corporate compliance resource for information regarding government regulations. Provides information that reduces risk and guides you to regulatory compliance through the most effective means, with a special view to legal compliance readiness.



Fios

Thank you!

Questions?

