powered by people

PRESENTATION FOR

HEARTLAND ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

03/14/17

Olivia Gerroll, Vice President, Sr. Discovery Engineer

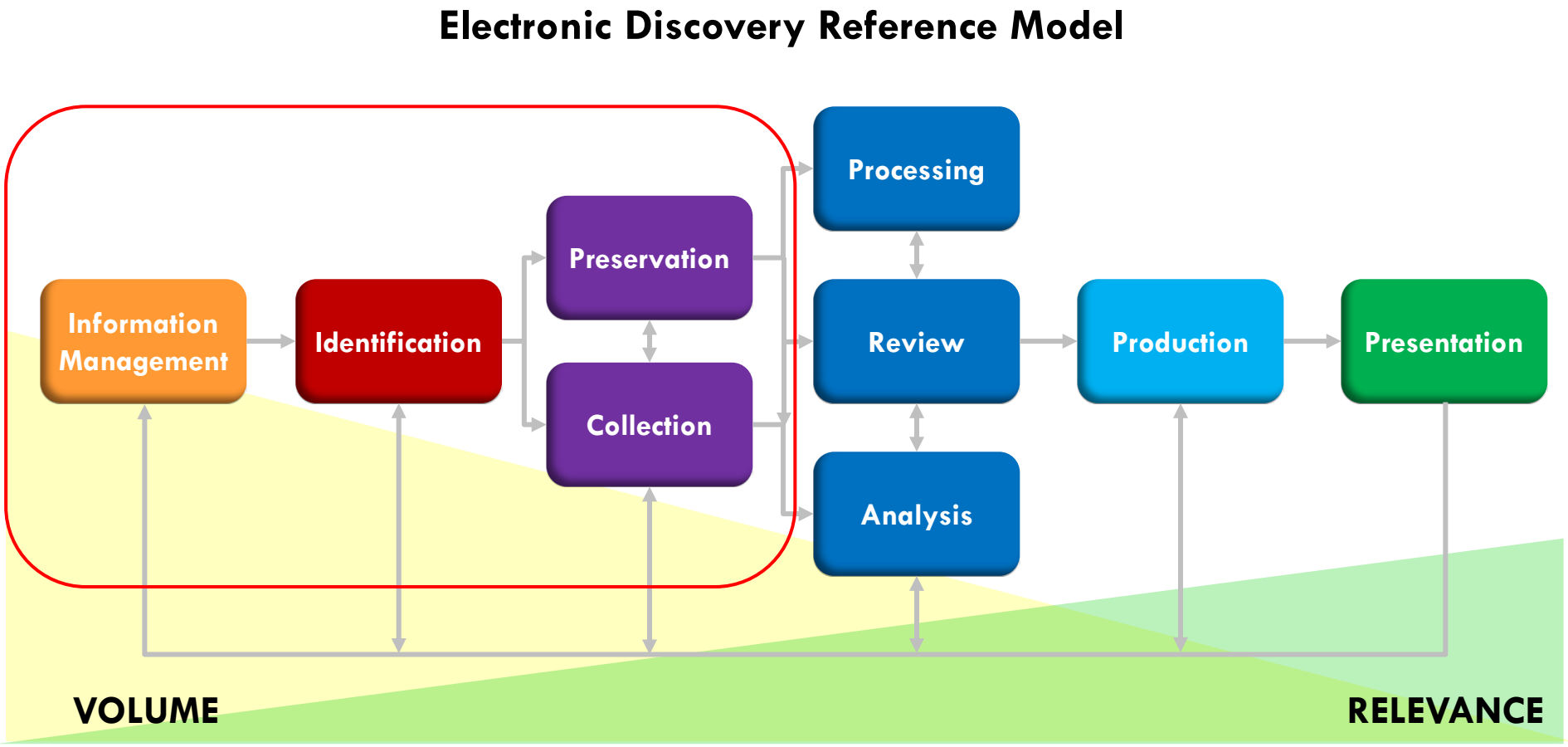
Agenda

- Overview of the litigation lifecycle
  - EDRM model
- Forensic vs Discovery Requirements
  - Description/overview of Forensic Services
  - Description/overview of Discovery Services
  - What to think of to determine what is required
- Collection Demands
  - Forensic v Discovery
  - Pros and Cons for both
  - Expert vs DIY
  - Forensic collection vs Forensic Analysis
- What are "Best Practices"
  - Forensic
  - eDiscovery

eDiscovery

Understanding Forensic Needs vs. Litigation Requirements and Best Practices around both

EDRM Model


Electronic Discovery Reference Model
Information Management
Identification
Preservation
Collection
Processing
Review
Analysis
Production
Presentation
VOLUME
RELEVANCE

Definition

eDiscovery

- Discovery of electronic documents and data including e-mail, Web pages, word processing files, computer databases, and virtually anything that is stored on a computer.
- Usually involves both software and a process that searches and indexes files on hard drives or other electronic media.
- Extracts metadata automatically for use as an index. May include conversion of electronic documents to an image format as if the document had been printed out and then scanned.

Digital Forensics

- The use of specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.
- Requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.
- Involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.

In Other Words…

eDiscovery

- Content-based
- "What" of a scenario
- Filtering/culling data to review set based on specific criteria such as search terms, date range, custodians, etc.
- Results in potentially relevant files for attorney review for production purposes
- Unit = document

Forensics

- Context-based
- "How" and "when" of a scenario
- Investigative tool
- Results in report and relevant files
- Testimony of expert to back-up report and findings
- Requires licensing and credentials
- Unit = data elements (log files, registry entries, link files, etc.)

Shared Goal

- Seek evidence to support investigations or fact discovery
- Example:
  - eDiscovery would find a key email.
  - Forensics would show how it arrived, how often it was opened, if it was sent to another location, if it was deleted, if it was copied to an external device, etc.

PC vs Mobile Devices



PC

- Pull hard drive, make an image, use forensic tools to analyze, report
- Techniques and tools are well-developed

Mobile Devices

- Mobile Device Industry is "young" with a multitude of O/S, protocols and data storage methods
- Encryption challenges – Apple – new technology which has not been broken
- No established, standard approach

Myth Busting

- "Forensic Copy" and "Forensically Sound" are NOT synonymous
  - Forensic Discovery = Forensic Copy
  - eDiscovery = Forensically Sound
- Courts do NOT "require" forensic copies for most cases
  - Reasonable approach is the "name of the game"
- Courts have NOT "validated" some tools
  - Just because a product is named in a court opinion does NOT render the product "court validated"

Decision Time

- Do I need Forensic Discovery?
  - ✓ Did someone backdate an electronic document?
  - ✓ Did an employee e-mail company trade secret documents to his personal e-mail address or copy it to an external drive?
  - ✓ Did a security camera capture footage of an accident?
  - ✓ Did an employer send harassing text messages to an employee?
  - ✓ Did a company spoliate electronic evidence?
  - ✓ Was an e-mail manufactured after the fact?
  - ✓ Was a computer intentionally used to download illegal content?
  - ✓ Did an employee delete data?

FAQ

- What can be found in a computer forensics exam?
  - Information about files that currently reside or used to reside on the device being examined.
  - Files deleted recently or in some cases long ago.
  - Deleted email messages, pictures, audio files, or any other type of file such as business documents and databases.
  - Fragments of files from long ago may also be uncovered.
  - Details about certain user activity.
- Is it OK to have our IT staff look for things on a computer first prior to requesting a forensic examination?
  - NO.
  - Any access can potentially change the data, corrupt or even overwrite data on the computer.
- We're thinking about requesting a forensic examination of a computer. Are there any precautions we should take while we are deciding?
  - Stop all access to the device.
  - Shut it down and do not turn it back on.

Comparison Sheet*

Factors	eDiscovery	Computer Forensics
Origins	Civil Litigation	Law Enforcement
Focus	General	Specific
Collection Process	Bit image only	Bit by bit
Data Types Collected	Accessible	Accessible and inaccessible
Active Data	Yes	Yes
Metadata	Yes	Yes
Automatically Stored Data	Maybe	Yes
Deleted Files	No	Yes
"Ghost" or residual data	No	Yes
System data	No	Yes
Evidence of wiping software	No	Yes
Testimony	Fact	Expert

http://www.forensicstrategic.com/wp-content/uploads/2012/09/Dunn-on-Damages-Fall-2012-Computer-Forensics-v.-E-Discovery-What-Every-Expert-Should-Know.pdf

Forensic Investigation

- Concerned with four principles:*
  - Minimization of data loss
  - Recording of detailed notes
  - Analysis of collected data
  - Reporting findings
- Phases of an investigation (can be similar to the eDiscovery processes)
  - Verification
  - Identify
  - Preserve
  - Collect
  - Analyze
  - Present

*Lee, R. (2008, December). *Forensic and Investigative Essentials*

Verification

- Confirm that “something” has occurred
- The “triggering” event in civil litigation
- Does the event “warrant” the initiation of a forensic investigation
  - Ask the questions?

Decision Time – Reminder

- Do I need Forensic Discovery?
  - ✓ Did someone backdate an electronic document?
  - ✓ Did an employee e-mail company trade secret documents to his personal e-mail address or copy it to an external drive?
  - ✓ Did a security camera capture footage of an accident?
  - ✓ Did an employer send harassing text messages to an employee?
  - ✓ Did a company spoliate electronic evidence?
  - ✓ Was an e-mail manufactured after the fact?
  - ✓ Was a computer intentionally used to download illegal content?
  - ✓ Did an employee delete data?

Identify

- Identification of the potential sources of evidence
  - Computer hard drives
  - Mobile Devices
  - Tablets
  - GPS Devices
  - Social Media Websites
  - Internet Messaging
  - ANY device that has memory – digital cameras, iPods, flash drives, SIM cards
- Forensic expert selection

Preservation



- Preserve the evidence
- Ensure chain of custody
- Plan to ensure that nothing will change from acquisition to analysis to final reporting

Collection/Acquisition

- Vital phase
  - Define the needs and collect appropriately
- Options
  - Targeted - eDiscovery
    - Specific files, custodians, locations
    - Apply forensic methodologies
  - Full Capture – eDiscovery and/or Forensic
    - Copy of entire “media” (hard drives, mobile devices, etc.)
    - Capture without modification
    - Seal evidence to prevent tampering
    - More comprehensive

Collection/Acquisition



- Four main principles:

1. No action should change data held on a computer or storage media which may be subsequently relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved.
   - An independent third-party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Analysis - Who Did This?



- Last time specific users logged on
  - When the system was unlocked
  - A user logged onto the computer/network
  - A user logged off the computer/network
- Last failed logon of that user
  - Unknown user
  - Disabled account/expired account
  - User not allowed to logon to that computer/network
  - Password had expired
- Last password change of that user
- RDP usage
- Authentication of accounts
- What groups is this user part of
- What rogue local accounts exist

Analysis – Where Did the Action Take Place?



- What time zone was used on the computer?
- What networks did this computer connect to?
- What wireless networks did this computer connect to?
  - When did it last connect? First connect?
- Browser cookies
  - Google Maps
  - Location aware browsing

Analysis - How/What/When Were the Actions?

- USB drives/external devices
  - Unique identifier for each device connected
  - First/last times used
  - What user(s) used the devices?
  - What volume name was the item given?
  - What drive letter was the item given?
  - What files were opened and viewed on the drive?
- Browser usage
  - What websites were visited on what date/time?
  - What pages were viewed by the user? (Cache)?
  - When certain web pages were viewed? When session ended?
  - What referring web page opening the web page?
  - Super & Flash cookies show sites visited by which account, first visit, last visit
  - Suggested sites history
  - In private browsing

Analysis – How/What/When Were the Actions?

- File Download
  - Which documents were opened and using which application?
  - Which email attachments were opened?
  - Which files were downloaded via Skype?
  - How many times were files downloaded via browser accessed?
  - Which sites were visited, and what files downloaded from that site?
- User communications
  - Email (Outlook, Lotus Notes)
  - Web based email
  - Calendar events
  - Chat
  - Instant Messaging

Analysis – How/What/When Were the Actions?

- File Knowledge and deletion
  - Search assistant stores searches
  - Searches conducted in start menu (Win7/Vista)
  - Track programs used and last file opened with program
  - Recycle bin shows files that were placed into it
  - Index.dat file shows a step by step of every program used and file opened
  - Thumbs.db tracks every photo on machine even if deleted
- Program Execution
  - What programs have been run, opened which files
  - What has been run from the Start-Run
  - What programs exist in the task bar
  - What programs are used frequently by the user

Analysis – How/What/When Were the Actions?

- File Opening and Creation
  - Track any files saved on the system
  - Track any specific program used and what files that program opened
  - Recent Files list shows all recently opened files
  - MS Office Recent Files shows all recently opened Office files
  - Show which folder the user recently opened and viewed

Present

- Report and presentation of findings “ROF”
  - Clearly written – no “geek speak”
- Detail of the equipment and/or software used to perform the analysis, the examiners credentials and the findings.
- The examiner’s “findings” should include specific details, occurrences and supporting exhibits
- Probable need for deposition and/or court testimony based on findings

Things to think about…

- Authentication
  - Proper chain of custody documentation
  - Create hash value of each “copy”
- Federal Rules
  - FRE 702 – Testimony by Expert Witnesses
  - Meet & Confer – Rule 26(F) Amendments
    - Lawyers should take forensic and/or eDiscovery experts to the conference.
- Privacy Concerns
  - Domestic
  - International issues
  - Company policies
- Cost Shifting
  - Possible options to shift costs to requesting party

Notable Cases

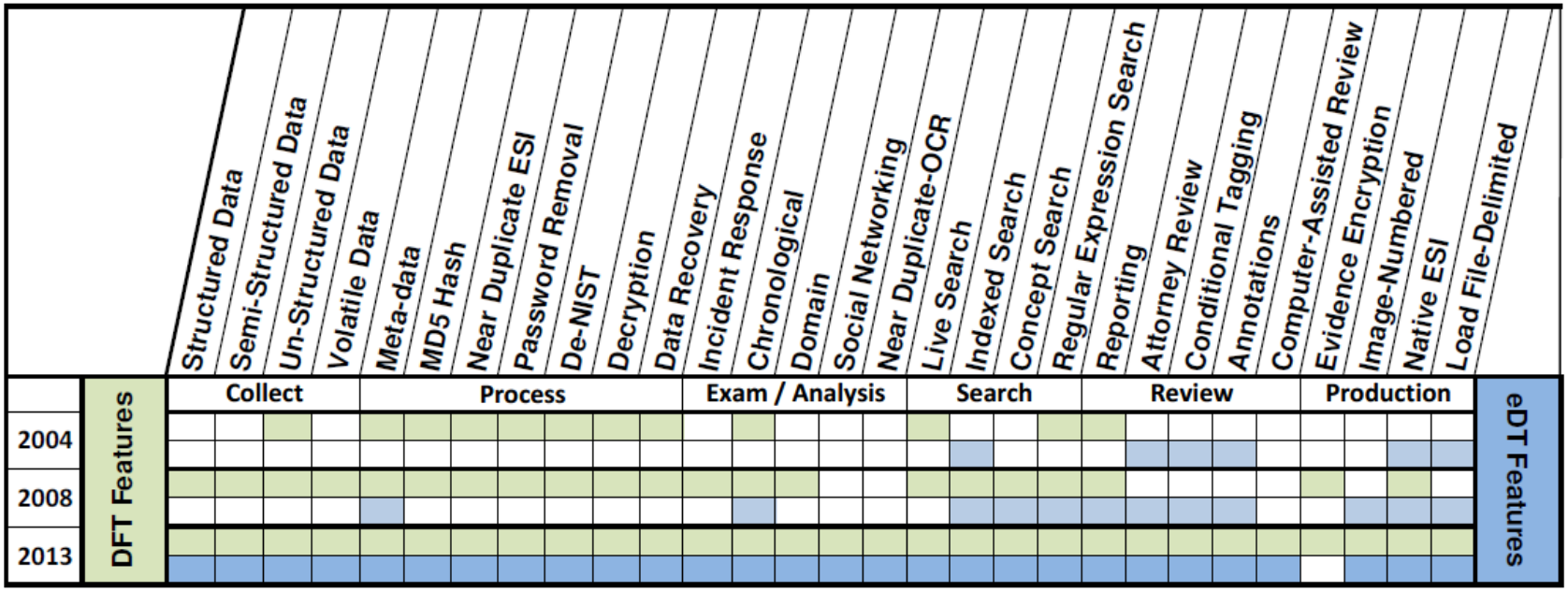
- BTK Killer
  - BTK killer sent a floppy disk to taunt police as he had done before on paper. Forensic experts recovered a deleted file which revealed the file creator.
- Bimbo Bakeries v Botticella
  - VP of Operations copied confidential company files before leaving to work for a competitor
- Leon v IDX Systems
  - Plaintiff was given hold order for his company laptop. Following legal hold order over 2200 files were deleted.
- Taylor v State (Texas)
  - Criminal conviction overturned because investigator did not follow proper procedure - doubt about authenticity of data.

Tools



- Tools should provide for:
  - Acquisition/collection/preservation
  - Search/analysis
  - Reporting/audit log
- Mainstream tools:
  - **FTK – AccessData**
  - **EnCase – Guidance Software**
  - ParabenP2 Commander
  - X-Ways Forensics
  - Many others available
- Tool resource website – National Institute of Standards and Technology - http://www.cftt.nist.gov/

Features – eDiscovery vs. Forensic



http://www.capsicumgroup.com/digital-forensics-and-e-discovery-where-one-stops-the-other-begins-2/

Resources

- *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*
  https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- National Institute of Standards and Technology -
  http://www.cftt.nist.gov/
- Association of Certified Fraud Examiners
  http://nf.acfe.com
- American Society of Digital Forensics & eDiscovery
  http://www.asdfed.com
- The SANS Institute – Specializes in information security and cybersecurity training
  http://www.sans.org
- The Sedona Conference
- www.edrm.net
- International Association for Computer Information Systems
  www.iacis.org

Thank You

Questions?