Ethical Duties and Electronically Stored Information

John R. Mallery

Director, Digital Forensics

JMallery@ArcherHall.com

855.839.9084

ARCHERHALL
AIM HIGH

ARCHERHALL
AIM HIGH

Digital Forensics & eDiscovery experts serving attorneys in all 50 states

- Cellphones
- Computers & Tablets
- External Hard Drives
- Smart Devices
- Emails & SMS
- Social Media Accounts
- Cloud Data
- Electronic Medical Records

Business Litigation

Employment Law

Schools and Higher-Ed

Medical Malpractice

IP Theft

Bankruptcy

John R. Mallery

- 23 years experience in Computer Forensics and eDiscovery.
- Created first private sector computer forensics lab in Kansas City
- Testimony in State and Federal Court, Civil and Criminal Cases.
- Provided P.O.S.T. accredited training to law enforcement.
- Authored 40+ articles on network security and computer forensics.

Identifying ESI

ARCHERHALL
AIM HIGH

Electronically Stored Information (ESI)

- **Any data that resides on electronic or digital media.**
- **Includes data stored on:**
  - Computer Disks
  - Printer or Fax memory
  - Tape storage
  - Databases
  - Network Storage
  - Mobile Devices
  - Cloud Services
  - Social Media
  - ANY Digital media that may be invented

Device Sources

DESKTOP

LAPTOP

MUSIC PLAYER

NETWORK EQUIPMENT

NOT-SO-SMART PHONE

PRINTERS

SMART PHONE

DIGITAL CAMERA

TABLET

VIDEO CAMERA

VEHICLE CANBUS

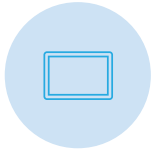
VIDEO GAME SYSTEM

PERSONAL DIGITAL ASSISTANT

ANSWERING MACHINE

GPS

SECURITY SYSTEM



EREADER

IOT DEVICES

Media Sources

CD/DVD

CLOUD STORAGE

FLOPPY DISK

HARD DRIVE

MAGNETIC TAPE

THUMB DRIVE

SD CARD


Life in
Luxury


Poker
Stars


Canon
EOS
5D

Cloud Sources

Data / File Types

DATABASES

DEVICE SETTINGS

DIAGRAMS

DRAWINGS

EMAIL

GEOLOCATION DATA

IMAGES

PDF

SOCIAL MEDIA POSTINGS

SPREADSHEETS

TEXT MESSAGES

VIDEO

AUDIO

WEB PAGES

WORD PROCESSING DOCS

VIRTUAL DISKS

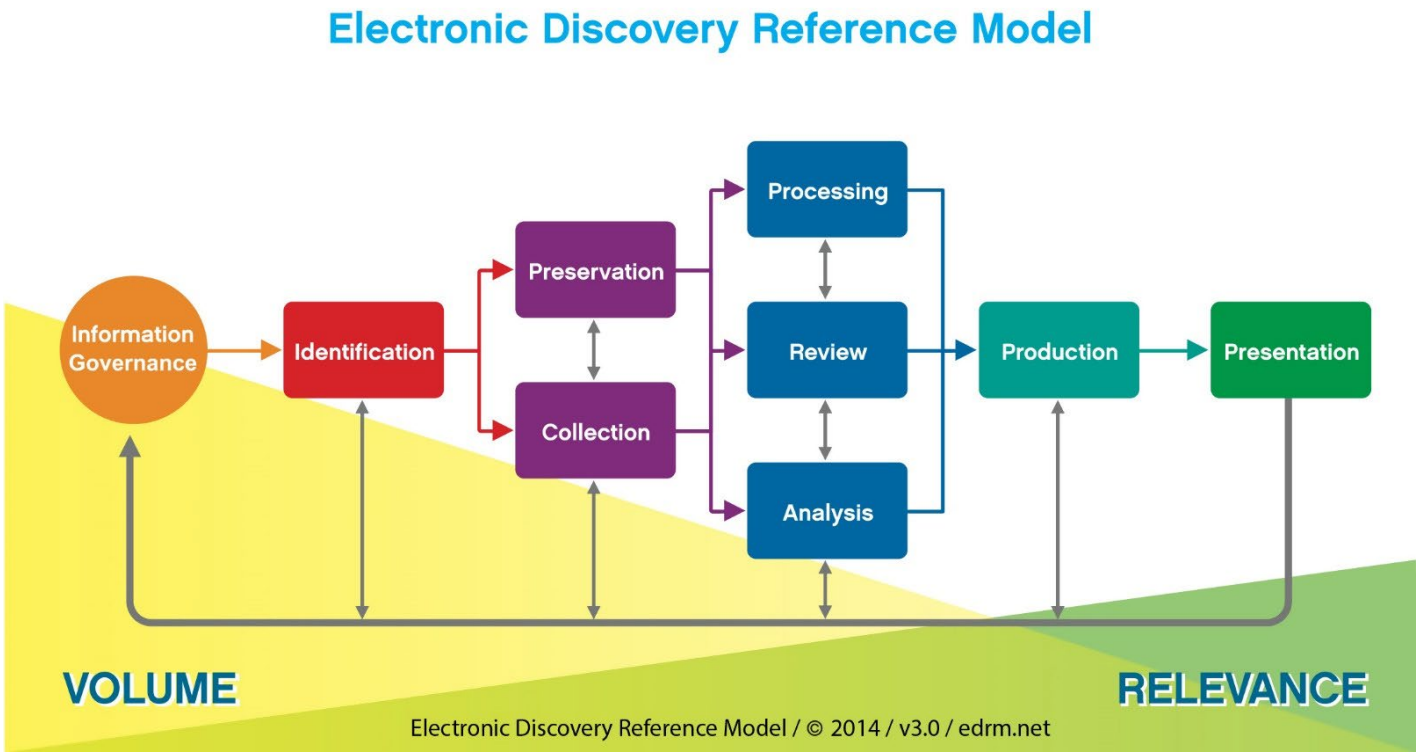
PRESENTATIONS

INTERNET ACTIVITY

NETWORK INFORMATION

Electronic Discovery or eDiscovery

- The process of locating, securing, and searching ESI to use as evidence in a legal proceeding.

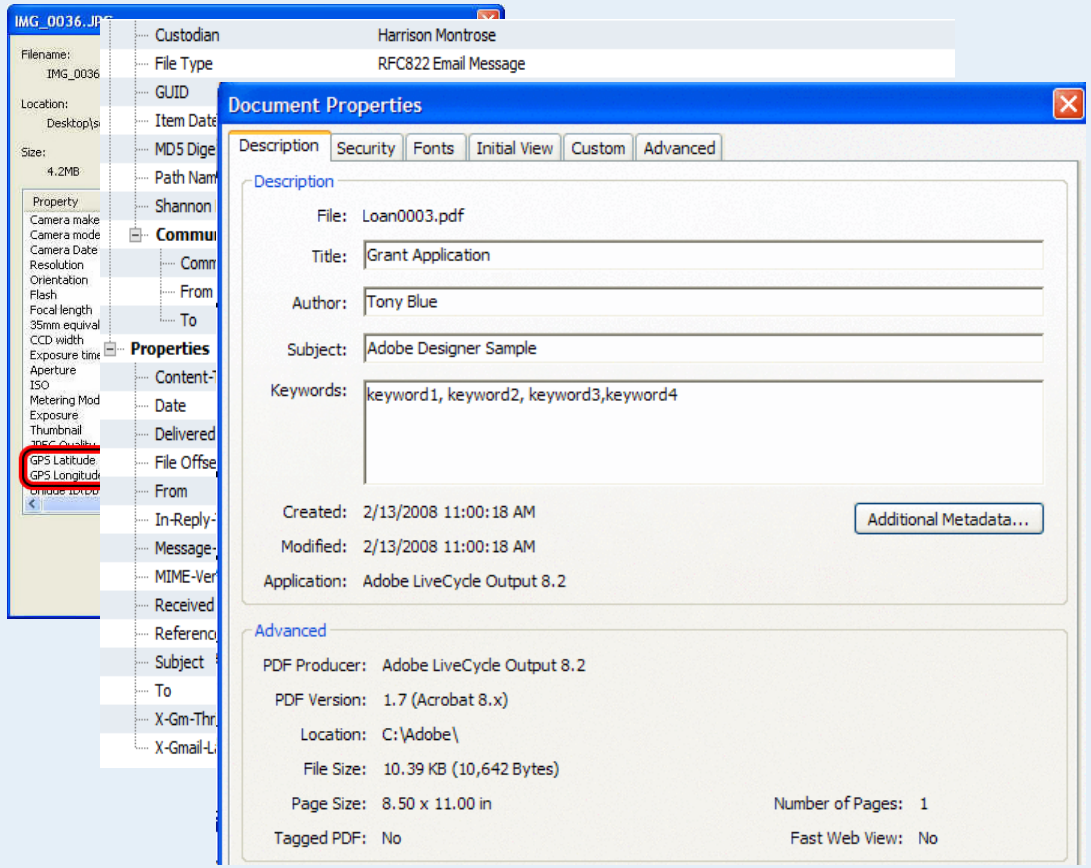


Digital Forensics

- The use of specialized techniques for recovery, authentication and analysis of ESI.

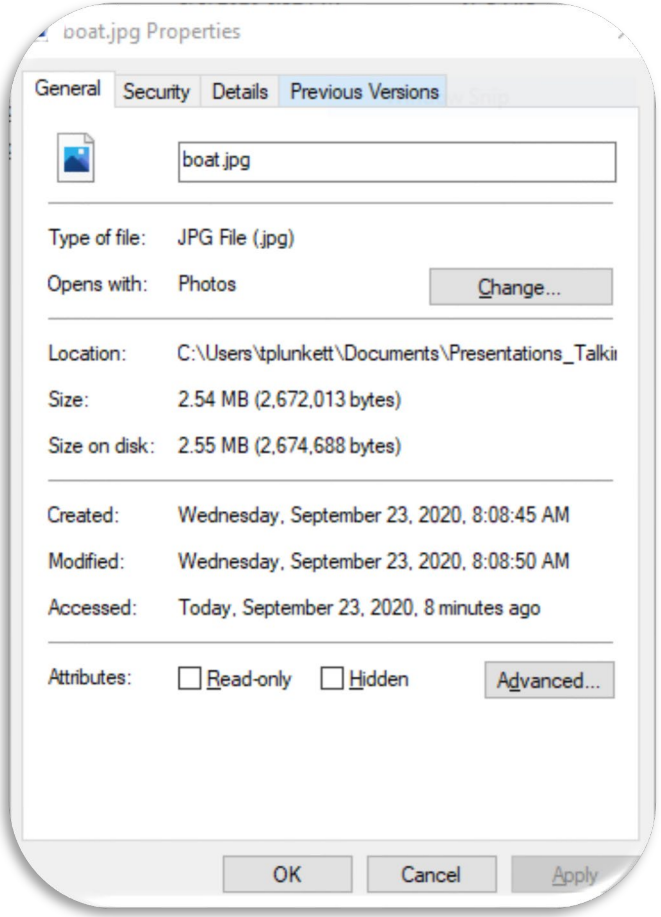
Metadata

- Information about Data
- Internal
  - Stored within the file itself
  - Comprehensive
- External
  - Stored in the file system
  - Summary



Internal vs External

External Metadata



Internal Metadata

```
Lens Make                       : Apple
Lens Model                      : iPhone X back dual camera 6mm f/2.4
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Altitude Ref                : Above Sea Level
GPS Speed Ref                   : km/h
GPS Speed                       : 4.308832651
GPS Img Direction Ref           : Magnetic North
GPS Img Direction               : 305.0164948
GPS Dest Bearing Ref            : Magnetic North
GPS Dest Bearing                : 305.0164948
GPS Horizontal Positioning Error: 8.001208277 m
```

```
Shutter Speed                   : 1/625
Create Date                     : 2020:08:09 18:52:51.554-04:00
Date/Time Original              : 2020:08:09 18:52:51.554-04:00
Modify Date                     : 2020:08:09 18:52:51-04:00
Thumbnail Image                 : (Binary data 8255 bytes, use -b option to extract)
GPS Altitude                    : 234 m Above Sea Level
GPS Latitude                    : 42 deg 45' 3.61" N
GPS Longitude                   : 85 deg 32' 5.00" W
Circle Of Confusion             : 0.003 mm
```

CALIFORNIA ETHICS OPINION 2015-193

ARCHERHALL
AIM HIGH

Guidance From The California State Bar

- **What are an attorney's ethical duties in the handling of discovery of electronically stored information?**
  - Basic understanding of, and facility with, issues related to eDiscovery and ESI
  - Duty of competence may vary case-by-case, requiring a higher level of technical knowledge
  - An attorney lacking the required competence for e-discovery issues has three options:
    - Acquire sufficient learning and skill before performance is required
    - Associate with or consult technical consultants or competent counsel
    - Decline the client representation
  - Lack of competence in eDiscovery issues also may lead to an ethical violation of an attorney's duty of confidentiality

Nine Skills of Competency

1. Initially assess eDiscovery needs and issues, if any
2. Implement or cause to implement appropriate ESI preservation procedures
3. Analyze and understand a client's ESI systems and storage
4. Advise the client on available options for collection and preservation of ESI
5. Identify custodians of potentially relevant ESI
6. Engage in competent and meaningful meet and confer with opposing counsel concerning an eDiscovery plan
7. Perform data searches
8. Collect responsive ESI in a manner that preserves the integrity of that ESI
9. Produce responsive non-privileged ESI in a recognized and appropriate manner

Guidance From The State Bar

1. Initially assess eDiscovery needs and issues, if any.

- What information could I possibly be looking for?
  - New data formats – cloud hosted – client may not be aware
- Where could that information be located?
  - My client's possession
  - Opposing client's possession
  - 3rd party possession

Interviews and Investigation

- **Talk to your client**
  - What devices do they use?
  - What accounts do they have?
  - Walk through a typical day to identify potential sources of information
- **Identify others to interview**
  - IT staff? Admin staff?
  - Witnesses/3rd Parties
  - Ask them about data, accounts, devices, etc.

Guidance From The State Bar

2. **Implement/cause to implement appropriate ESI preservation procedures.**
   - Time Sensitive
     - What information could be deleted or wiped?
       - Phone company and Internet Service Provider (ISP) records
       - Backups
       - Emails

Preservation

In-Place

Usually corporate environment

Allows continued use of data without modification

No immediate collection

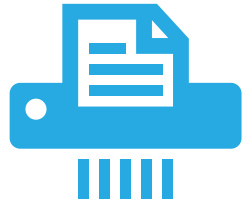
Metadata is preserved

Forensic

Physical – Bit-for bit copy of a device

Logical – Mirror copy of the ESI

Preserves all available metadata



Non-Forensic

Copy and Paste

Email forwarding

Zip files

Metadata may be lost

Guidance From The State Bar

3. Analyze and understand a client's ESI systems and storage.

- Computer, Server, Backups, External Drives
- Smartphone / Cell Phone
- Cloud Storage/Backup (Google Drive, DropBox, OneDrive, CrashPlan)
- Cameras / Video Surveillance
- New Types of ESI

Guidance From The State Bar

4. **Advise the client on available options for collection and preservation of ESI.**

- Digital Forensics / eDiscovery Expert
  - Forensic Collection / Preservation to meet court requirements
  - Organizational integrity
- Attorney retains evidence
- Vendor or another attorney supervise collection
- Having IT staff perform collection is usually insufficient

Guidance From The State Bar

5. **Identify custodians of potentially relevant ESI.**
   - Your client / opposing party
   - Other employees at the firm
   - IT Employees
   - Telephone / Cell Phone Companies
   - Internet Service Providers
   - Hosted Application Providers (Salesforce, Online Time Card, Facebook, DropBox, etc)
   - Email / Text Message CC Recipients

Guidance From The State Bar

6. **Engage in competent and meaningful meet and confer with opposing counsel concerning an eDiscovery plan.**
   - Work with your client to determine clear search terms.
   - Consult with e-discovery or forensics expert regarding potential search terms and also potential overbroad search terms.
   - Review data obtained from your clients before it is released to opposing counsel.
     - Do not rely on claw back

Guidance From The State Bar

7. Perform data searches

- Search both searchable and non-searchable data
  - Some files may require OCR or manual review
- Alternate spellings / misspellings
- Avoid terms such as single or short words
- Use Boolean Logic (AND, OR, NOT) to be as precise as possible
  - (“peanut butter” AND jelly) w/1 (sandwich OR sammich)
- Indexed searches vs. Plain Text or Raw search

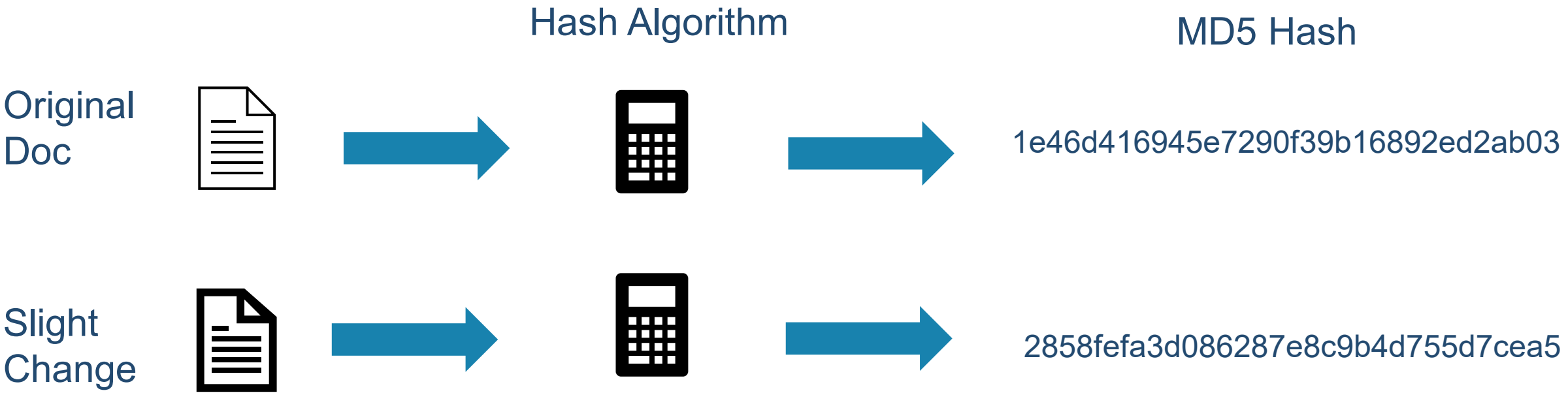
Guidance From The State Bar

8. Collect responsive ESI in a manner that preserves the integrity of that ESI

- Preserving the Integrity
  - Chain of Custody
  - Limiting Access to Data
    - Write Blocking / Working Copies
- Proving Preservation of Integrity
  - Hash value – output of cryptographic algorithm. Digital Fingerprint
  - Digital Forensic Containers

Hash Values

- "A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures." – Microsoft



Guidance From The State Bar

9. **Produce responsive non-privileged ESI in a recognized and appropriate manner.**

- Formal Opinion refers to attorney's ethical obligations relating to his own client's ESI, and does not address the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI.
- Native Formats
- PDF Formats
- Common Metadata
  - Created/Modified/Accessed Dates, Location, Custodian, Checksum

THINGS TO CONSIDER

ARCHERHALL
AIM HIGH

Stored Communications Act

- **Stored Communications Act – 18 USC 121, Sections 2701-2712**
- **Part of the 1986 Electronic Communications Privacy Act**
- **Prohibits a subpoena alone to obtain data**

- **Allows for disclosure when:**
  - To the intended recipients or agent of intended recipient
  - With lawful consent of the communications originator, addressee, or intended recipient (Signed authorization from account holder)
  - Third party's employer or authorized to forward the communication to its destination
  - Disclosure to law enforcement/Court Order (Warrant)

Ethical Duties & ESI

Things to Consider

- **Request for Preservation**
  - The standard of competence changes with technology.
    - New forms of ESI emerge frequently
  - E-discovery expertise helps protect client confidentiality and privilege.
    - Reduce chance of overproduction and privilege breach
  - Opposing counsel may not know what they should be preserving – best to describe locations where data may be kept.
  - Opposing counsel may not know that they may need an eDiscovery or Digital Forensics expert to properly preserve their evidence.

Ethical Duties & ESI

Things to Consider

- **Discovery Process**
  - What can I expect to receive in terms of ESI?
    - You get what you ask for - maybe
  - How should I ask for the ESI?
    - Native Documents – with Metadata! – Maybe a load file
  - How should the data integrity be preserved?
    - Forensic containers with all metadata

Ethical Duties & ESI

Things to Consider

- **Discovery Process**
  - How is data stored?
    - some data may require an expert to retrieve it
  - How do I ask for information that may require an ESI expert to retrieve?
    - Describe the sources and data types
    - Request Forensically Sound productions
  - How do I effectively limit or cull through information captured or received?
    - Information Governance / Retention Policy
    - Date Range
    - Good keywords

We’d love to hear from you!

John R. Mallery
Director, Digital Forensics

jmallery@archerhall.com
855.839.9084

ARCHERHALL
AIM HIGH