

Digital Evidence

Week 3 – Introduction to Digital Evidence

Shawn Davis
ITMS X83 – Spring 2026

Slides contain original content from Davis, S. and
E-discovery: An Introduction to Digital Evidence

Week 1 - Review

- Kahoot Week 1 Review – 21 questions
 - 30 seconds for multiple choice
 - 20 seconds for true and false

Overview

1. An Overview of E-Discovery
2. What is Digital Evidence?
3. Factors Affecting Evidence Acquisition
4. Federal Rules in U.S. Courts
5. Rules and Policies Governing Digital Evidence

Objectives

- Define e-discovery and digital forensics
- Describe types of digital evidence
- Explain factors affecting digital evidence collection
- Summarize U.S. federal rules on digital evidence
- Describe other laws related to digital evidence and ESI discovery

Part I

An Overview of E-Discovery

An Overview of E-discovery

- **E-discovery:** process of applying traditional legal discovery process to electronic evidence
- Electronic evidence encompasses any **electronically stored information (ESI)**.
- What are some examples of ESI?
 - Documents, e-mails, text messages, instant messages, pictures, log files, web pages, source code, databases, etc.

Breakout Groups

- I am going to split you into 4 groups
- You'll have 15 minutes
- When we come back, the group will tell the class what they came up with

Breakout Groups – Sources of ESI

- Where (devices, software, etc.) might you find the following for a company?
 - Group 1: Email evidence?
 - Group 2: Electronic Documents (PDFs, MS Office files, etc.)?
 - Group 3: Source code? (Such as in a trade secret theft case)
 - Group 4: Log files? (Such as in a data breach case)

1: Email Evidence Sources

- Desktop/Laptop Clients (Outlook, Apple Mail)
- Mobile Clients
- On-Prem Servers (Exchange)
- Cloud Providers (Gmail, iCloud, O365, Yahoo)
 - Evidence on client systems
 - Evidence on cloud provider (depending on retention)
- Backups (local, network, cloud)
- Ediscovery Email Archiving Software

2: Electronic Documents

- Email attachments
- Laptops/Desktops
- Mobile devices
- External drives
- Backup media
- File servers/SANS
- Optical Media
- Cloud Providers
- Websites
- Printer memory
- Etc.

3: Source Code

- Desktops/Laptops
- Servers
- On-Prem Repos (Git, Mercurial, etc.)
- Cloud Repos (GitHub, Bitbucket, GitLab, Source Forge, AWS CodeCommit, etc.)
- Backup media
- Optical media
- External drives
- 3rd parties

4: Log Files

- Desktop/Laptops/Servers (Events, Host AV or IDS, etc.)
- Mobile Devices:
 - Android – dumphsys, logcat
 - iOS – iTunes Backup, Xcode, Apple Configurator 2, iTools, etc.
- Network Devices (Switches, Routers, Firewalls, Proxies, IDS/IPS, DLP, VPNs Concentrators, SIEMs, WIDS/WIPS, UTM Appliances, Web Filters, A/V Management, etc.)
- Remember that 3rd parties may be contracted for the company and have logs as well

Other Sources of ESI??

- Instant messaging
- Websites
- Databases
- Social Media
- Voice Mail
- Alarm Systems
- Security Camera Systems
- Text Messages
- Third Parties/Cloud
- Cars (logs)
- IoT Devices (Fridges, Smart Locks, Medical Devices, etc.)
- ISPs
- Cell Carriers

Preservation Order

- Example:
 - <https://www.crowell.com/PDF/Sample-Preservation-Memo-Hold-Order.pdf>
- Show example of questionnaire

An Overview of E-discovery

- E-discovery is a form of data mining
 - Data mining is a method companies use to gather information about customers or vendors

Overview of Digital Forensics

- Digital forensics: a scientific method for extracting data or evidence from a digital device or an active network
 - Following this process ensures information will stand up to scrutiny in court

Overview of Digital Forensics

- What does the examiner need to be able to verify before they start their analysis?
 - That the evidence hasn't been tampered with
 - Who the evidence came from
 - Correct time zone
- How?
 - Hashing
 - Chain of custody or declarations
 - Artifacts:
 - TimeZoneInformation registry key
 - File timestamps, system logs, network timestamps, etc.

Overview of Digital Forensics

- Field of digital forensics is divided into two specialties:
 - Device forensics: existing files, deleted files, hidden files, encrypted data, and more are retrieved
 - Network forensics/incident response: deals with network intrusion and hackers

Forensics: Three Main Parts

- Evidence Acquisition
 - Determining systems involved
 - Collecting volatile and non-volatile evidence through forensic imaging
- Evidence Analysis
 - Investigation to determine what happened
 - File and artifact extraction
 - **Forming of timeline of events**
- Reporting
 - Creation of report detailing findings

Digital Forensics Timelines

- Type of evidence examined is OS information
 - MAC times: “modified, accessed, and created” dates and times

Created:	Monday, September 14, 2020, 5:18:12 PM
Modified:	Monday, September 14, 2020, 5:42:17 PM
Accessed:	Today, September 14, 2020, 10 minutes ago

- File access times and network logins are also examples

Overview of Digital Forensics

- What are three common types of investigations for digital forensics investigators?
 - Criminal
 - Civil
 - Corporate
- Common cases with forensics for each??

Overview of Digital Forensics

- In digital forensics, investigations typically involve:
 - Incriminating or exculpatory evidence in a criminal case such as??
 - Child Exploitation
 - Data Breaches/Attacks
 - Intellectual Property Theft
 - Fraud
 - Murder
 - Espionage
 - Terrorism

Digital Forensics vs E-Discovery

- In digital forensics, investigations typically involve:
(Cont.)
 - Evidence of a corporate policy violation such as??
 - Sexual harassment
 - Bribe taking & embezzlement
 - Stalking & discrimination
 - Time sheet issues
 - Incriminating or exculpatory evidence in a civil case such as??
 - Divorce or custody issues in a civil case (keyloggers, RATs, on spouse's devices)
 - Analyzing source code to determine functionality
 - Data breach cause and effect
 - Evidence spoliation

Famous Cases Involving Digital Forensics

- Dennis Rader
 - Police used EnCase to retrieve metadata identifying BTK serial killer from deleted Word document on floppy disk
- Dr. Conrad Murry
 - Investigators found documentation on his computer that he authorized lethal amounts of propofol which resulted in Michael Jackson's death

Famous Cases Involving Digital Forensics

- Casey Anthony
 - Sheriff's department processed forensic evidence of her computer but only looked at Internet Explorer artifacts
 - They failed to extract browser history from Firefox which showed searches for "how to make chloroform," "neck breaking," and "foolproof suffocation."
 - Casey was found not guilty in death of her daughter

Digital Forensics vs E-Discovery

- Digital forensics can be considered to overlap with e-discovery
 - E-discovery experts might have to call on device forensics expert to retrieve data
 - Network forensics generally do not consider e-discovery to be related to their job

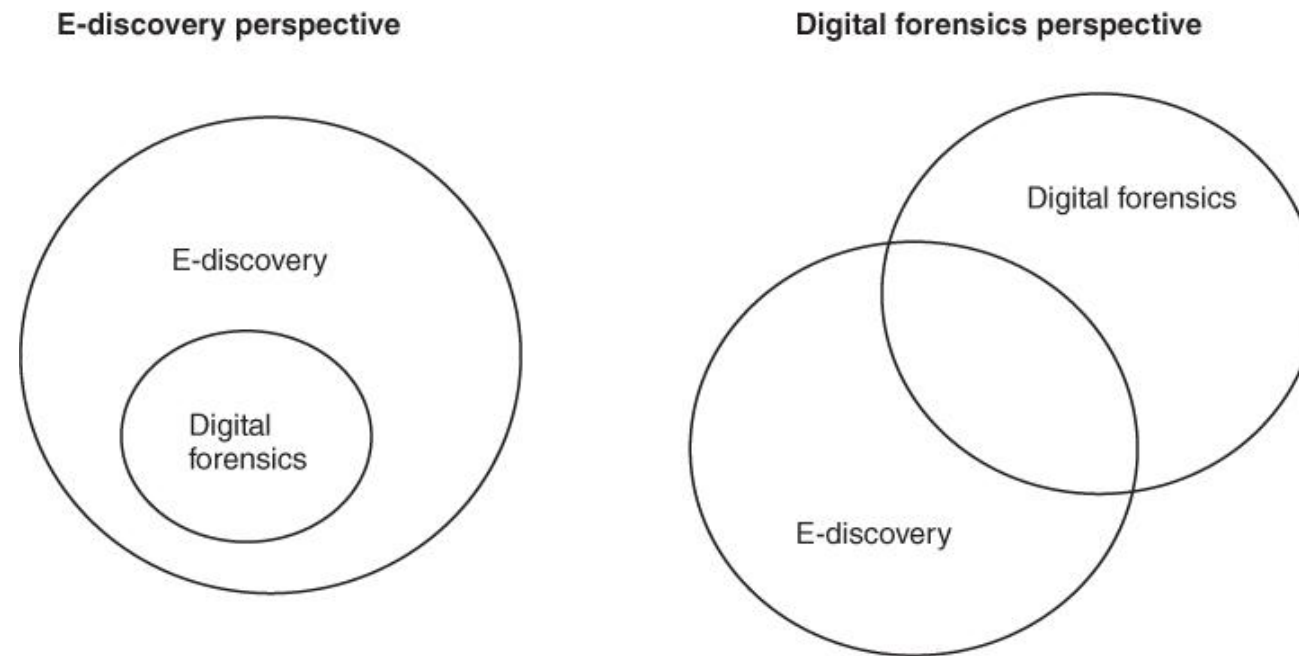


Figure 1-1 The relationship between e-discovery and digital forensics

Part II

What is Digital Evidence?

What Is Digital Evidence?

- Data or files in digital format that pertain to a civil or criminal complaint
- Often referred to as ESI or Electronically Stored Information

Question??

- What are the two parts of each piece of digital evidence that are useful?
- **Data:** actual information being retrieved, such as a letter or document
- **Metadata:** information about the data
 - What are some examples of Metadata?
 - Metadata in a picture file can tell investigators the type of camera used, date of photo, and GPS coordinates where the photo was taken

Photo Metadata



IMG_6254 (1).jpg Properties

General Security Details Previous Versions

Property	Value
Light source	
Exposure program	Normal
Saturation	
Sharpness	
White balance	Auto
Photometric interpretation	
Digital zoom	
EXIF version	0221
GPS	
Latitude	41; 53; 18.73999999999907...
Longitude	87; 37; 57.19000000000022...
Altitude	202.4080810546875
File	
Name	IMG_6254 (1).jpg
Item type	JPG File
Folder path	C:\Users\Shawn\Pictures
Date created	8/22/2019 12:10 PM
Date modified	8/22/2019 12:10 PM

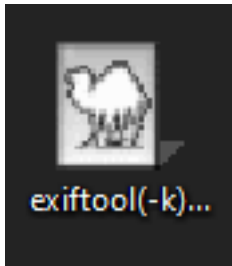
[Remove Properties and Personal Information](#)

OK Cancel Apply



Photo Metadata – ExifTool

- Some tools provide more information than others...
 - ExifTool – Download it now at: <https://exiftool.org>



```
Aperture : 1.8
Profile Copyright : Copyright Apple Inc., 2017
Brightness : 0.95045 1 1.08905
Exposure : 0.51512 0.2412 -0.00105
Matrix : 0.29198 0.69225 0.04189
Blue Matrix : 0.1571 0.06657 0.78407
Red Tone : (Binary data 32 bytes, use -b option to ex
Chromatic : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0
Blue Tone : (Binary data 32 bytes, use -b option to ex
Green Tone : (Binary data 32 bytes, use -b option to ex
Image Width : 4032
Image Height : 3024
Encoding : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Run Time Since Power Up : 3 days 16:20:35
Aperture : 1.8
Image Size : 4032x3024
Megapixels : 12.2
Scale Factor To 35 mm Equivalent : 7.0
Shutter Speed : 1/967
Create Date : 2019:08:22 12:09:02.157
Date/Time Original : 2019:08:22 12:09:02.157
Thumbnail Image : (Binary data 8315 bytes, use -b option to
GPS Altitude : 202.4 m Above Sea Level
GPS Date/Time : 2019:08:22 17:09:01Z
GPS Latitude : 41 deg 53' 18.74" N
GPS Longitude : 87 deg 37' 57.19" W
Circle Of Confusion : 0.004 mm
Field Of View : 65.5 deg
Focal Length : 4.0 mm (35 mm equivalent: 28.0 mm)
GPS Position : 41 deg 53' 18.74" N, 87 deg 37' 57.19" W
Hyperfocal Distance : 2.07 m
```

Word Document Metadata

|This is a test word doc.

This is a test word doc that I changed after putting track changes on.

This is a test word doc.

This is a test word doc.

This is a test word doc.

This is a test word doc.

This is a test word doc.

This is a test word doc.

SD

Shawn Davis

Here is a comment

Word Document Metadata – ExifTool

```
Revision Number      : 2
Create Date         : 2019:08:22 18:07:00Z
Modify Date        : 2019:08:22 18:09:00Z
Category           : Test Doc Category
Content Status      : Active Status
Template            : Normal.dotm
Total Edit Time     : 2 minutes
Pages              : 5
Words              : 499
Characters          : 2849
Application         : Microsoft Office Word
Doc Security        : None
Lines              : 23
Paragraphs         : 6
Scale Crop         : No
Heading Pairs       : Title, 1
Titles Of Parts     :
Company            : EPC
Links Up To Date    : No
Characters With Spaces : 3342
Shared Doc         : No
Hyperlink Base      : www.test.com
Hyperlinks Changed  : No
App Version         : 16.0000
```

Word Document Metadata

- A .docx file is really a ZIP archive file

```
C:\Users\Shawn\Downloads\document4349\word\document.xml:
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2: <w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/
wordprocessingCanvas" xmlns:cx="http://schemas.microsoft.com/office/drawing/2014/chartex"
xmlns:cx1="http://schemas.microsoft.com/office/drawing/2015/9/8/chartex"
xmlns:cx2="http://schemas.microsoft.com/office/drawing/2015/10/21/chartex"
xmlns:cx3="http://schemas.microsoft.com/office/drawing/2016/5/9/chartex"
xmlns:cx4="http://schemas.microsoft.com/office/drawing/2016/5/10/chartex"
xmlns:cx5="http://schemas.microsoft.com/office/drawing/2016/5/11/chartex"
xmlns:cx6="http://schemas.microsoft.com/office/drawing/2016/5/12/chartex"
xmlns:cx7="http://schemas.microsoft.com/office/drawing/2016/5/13/chartex"
xmlns:cx8="http://schemas.microsoft.com/office/drawing/2016/5/14/chartex"
xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
xmlns:a:ink="http://schemas.microsoft.com/office/drawing/2016/ink"
xmlns:am3d="http://schemas.microsoft.com/office/drawing/2017/model3d"
xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/
officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/
officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vm1"
xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing"
xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"
xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/
wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/word
xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml"
xmlns:w16cid="http://schemas.microsoft.com/office/word/2016/wordml/cid"
xmlns:w16se="http://schemas.microsoft.com/office/word/2015/wordml/symex"
xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup"
xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml"
xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape"
mc:Ignorable="w14 w15 w16se w16cid wp14"><w:body><w:p w14:paraId="60A97965"
w14:textId="36CEDB68" w:rsidR="003C3CBF" w:rsidRDefault="00E900FA"><w:r><w:t>This is a te
word doc.</w:t></w:r></w:p><w:p w14:paraId="4F48CB3F" w14:textId="189CA34F"
w:rsidR="00E900FA" w:rsidRDefault="00E900FA" w:rsidP="00E900FA"><w:r><w:t>This is a test
word doc.</w:t></w:r><w:ins w:id="0" w:author="Shawn Davis"
w:date="2019-08-22T13:07:00Z"><w:r w:rsidR="0059701C"><w:t xml:space="preserve"> that
</w:t></w:r></w:ins><w:ins w:id="1" w:author="Shawn Davis"
w:date="2019-08-22T13:08:00Z"><w:r w:rsidR="0059701C"><w:t>I changed after putting track
changes on.</w:t></w:r></w:ins></w:ins></w:p></w:t></w:r></w:p><w:p w14:paraId="36AA199D"
```

```
C:\Users\Shawn\Downloads\document4349\word\comments.xml:
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2: <w:comments xmlns:wpc="http://schemas.microsoft.com/office/word/2010/
wordprocessingCanvas" xmlns:cx="http://schemas.microsoft.com/office/drawing/2014/chartex"
xmlns:cx1="http://schemas.microsoft.com/office/drawing/2015/9/8/chartex"
xmlns:cx2="http://schemas.microsoft.com/office/drawing/2015/10/21/chartex"
xmlns:cx3="http://schemas.microsoft.com/office/drawing/2016/5/9/chartex"
xmlns:cx4="http://schemas.microsoft.com/office/drawing/2016/5/10/chartex"
xmlns:cx5="http://schemas.microsoft.com/office/drawing/2016/5/11/chartex"
xmlns:cx6="http://schemas.microsoft.com/office/drawing/2016/5/12/chartex"
xmlns:cx7="http://schemas.microsoft.com/office/drawing/2016/5/13/chartex"
xmlns:cx8="http://schemas.microsoft.com/office/drawing/2016/5/14/chartex"
xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
xmlns:a:ink="http://schemas.microsoft.com/office/drawing/2016/ink"
xmlns:am3d="http://schemas.microsoft.com/office/drawing/2017/model3d"
xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlfor
officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/
officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vm1"
xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing"
xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"
xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlfor
wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010
xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml"
xmlns:w16cid="http://schemas.microsoft.com/office/word/2016/wordml/cid"
xmlns:w16se="http://schemas.microsoft.com/office/word/2015/wordml/symex"
xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup"
xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml"
xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape"
mc:Ignorable="w14 w15 w16se w16cid wp14"><w:comment w:id="2" w:author="Shawn Davis"
w:date="2019-08-22T13:08:00Z" w:initials="SD"><w:p w14:paraId="2F842237"
w14:textId="7C689E87" w:rsidR="0059701C" w:rsidRDefault="0059701C"><w:pPr><w:pStyle
w:val="CommentText"/></w:pPr><w:r><w:rPr><w:rStyle
w:val="CommentReference"/></w:rPr><w:annotationRef/></w:r><w:r><w:t>Here is a
comment</w:t></w:r></w:p></w:comment></w:comments>
```

PDF Document Metadata

- Acrobat / File / Properties

Document Properties

Description Security Fonts Initial View Custom Advanced

Description

File: Diabold red team report.pdf

Title: Executive Summary

Author: j stauffer

Subject:

Keywords:

Created: 7/27/2007 2:37:07 PM

Modified: 7/27/2007 2:44:49 PM

Application: Acrobat PDFMaker 7.0.7 for Word

Additional Metadata...

Advanced

PDF Producer: Acrobat Distiller 7.0.5 (Windows)

PDF Version: 1.4 (Acrobat 5.x)

Location: C:\Users\Shawn\Downloads\

File Size: 498.55 KB (510,511 Bytes)

Page Size: 8.50 x 11.00 in

Number of Pages: 17

Tagged PDF: Yes

Fast Web View: Yes

Help OK Cancel

Diabold red team report.pdf

Description Advanced

Description

Document Title: Executive Summary

Author: j stauffer

Author Title:

Description:

Diabold red team report.pdf

Description Advanced

PDF Properties (pdf, <http://ns.adobe.com/pdf/1.3/>)

- pdf:Producer: Acrobat Distiller 7.0.5 (Windows)

<http://ns.adobe.com/pdfx/1.3/>

- pdfx:SourceModified: D:20070727172959

XMP Core Properties (xmp, <http://ns.adobe.com/xap/1.0/>)

- xmp:CreatorTool: Acrobat PDFMaker 7.0.7 for Word
- xmp:ModifyDate: 2007-07-27T14:44:49-07:00
- xmp:CreateDate: 2007-07-27T14:37:07-07:00
- xmp:MetadataDate: 2007-07-27T14:44:49-07:00

XMP Media Management Properties (xmpMM, <http://ns.adobe.com/xap/1.0/mm/>)

- xmpMM:DocumentID: uuid:3a2c8c20-2bd7-421e-8eda-f5d8bec09134
- xmpMM:InstanceID: uuid:1abd10cc-d98f-4f23-a5c7-e5ee24cf3352
- xmpMM:VersionID (seq container)
 - [1]: 11

Dublin Core Properties (dc, <http://purl.org/dc/elements/1.1/>)

- dc:format: application/pdf
- dc:title (alt container)
 - [x-default]: Executive Summary
- dc:creator (seq container)
 - [1]: j stauffer

Adobe Photoshop Properties (photoshop, <http://ns.adobe.com/photoshop/1.0/>)

- photoshop:headline (seq container)
 - [1]

Replace All... Append All... Save... Delete All

OK Reset

PDF Document Metadata - ExifTool

```
C:\Users\Shawn\Desktop\exiftool(-k).exe
ExifTool Version Number      : 11.63
File Name                    : Diabold red team report.pdf
Directory                    : C:/Users/Shawn/Downloads
File Size                    : 499 kB
File Modification Date/Time   : 2019:07:31 13:46:25-05:00
File Access Date/Time        : 2019:07:31 13:46:25-05:00
File Creation Date/Time      : 2019:07:31 13:46:24-05:00
File Permissions              : rw-rw-rw-
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.4
Linearized                   : Yes
Tagged PDF                   : Yes
XMP Toolkit                   : 3.1-701
Producer                     : Acrobat Distiller 7.0.5 (Windows)
Source Modified               : D:20070727172959
Creator Tool                  : Acrobat PDFMaker 7.0.7 for Word
Modify Date                   : 2007:07:27 14:44:49-07:00
Create Date                   : 2007:07:27 14:37:07-07:00
Metadata Date                 : 2007:07:27 14:44:49-07:00
Document ID                   : uuid:3a2c8c20-2bd7-421e-8eda-f5d8bec09134
Instance ID                   : uuid:1abd10cc-d98f-4f23-a5c7-e5ee24cf3352
Version ID                    : 11
Format                       : application/pdf
Title                        : Executive Summary
Creator                       : j stauffer
Subject                       :
Headline                      :
Page Count                    : 17
Page Layout                   : OneColumn
Author                        : j stauffer
```

Types of Digital Evidence

- Metadata has to be handled carefully
- Recent court cases have cited or fined companies for deleting metadata
- It is also important to be familiar with the various cloud service models to understand how data may be stored

Cloud Computing and Digital Evidence

- List and describe the three service models for cloud computing:
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service (IaaS)
- List and describe the four deployment methods for cloud computing:
 - Private, Community, Public, and Hybrid

Cloud Computing and Digital Evidence

- SaaS refers to applications provided for customers
 - Offers convenience of file access from any location and sharing with any location
 - Two common SaaS providers: Dropbox and Google Docs
- PaaS is more of a business model where users select a platform and install their own applications or software
- In IaaS, users get a “bare metal” environment where they install their own OSs, applications, tools, etc

Cloud Computing and Digital Evidence

- Most secure deployment method is the private cloud
 - Client owns hardware and has physical access
- A community cloud is for people or organizations with similar interests or similar business types
- Public cloud: a person's files are on the same physical machine as another person's files
- Hybrid cloud: users keep some files in the cloud and the rest on their own servers for data security

Part III

Factors Affecting Evidence Acquisition

Factors Affecting Evidence Acquisition

- In civil cases, evidence is acquired by issuing an RFP (Request For Production)
 - One company requests physical or electronic documents and the second company produces them
- Criminal cases require strict adherence to chain of custody
 - To ensure evidence hasn't been tampered with or altered in the process
 - Requires use of search warrants, subpoenas, etc

Factors Affecting Evidence Acquisition

- In digital forensics, a forensic image of a hard drive or other media device allows an investigator to:
 - Retrieve deleted files, deleted emails, file fragments, and other information not included in a simple file copy
- Because hard drives are increasing in size, live acquisitions are common
 - Live acquisitions are done while machines are running
 - Question before the courts is that the results of a live acquisition might not be reproducible (violates forensics standards)

Digital Forensics – Civil vs. Criminal Cases

- Criminal Cases
 - Warrants lead do devices seized by law enforcement
 - Digital forensics analysts find surface and deleted evidence
- Civil Cases
 - Subpoenas are issued where each side provides requested files with metadata
 - Digital forensics isn't used as often except for in certain cases/situations

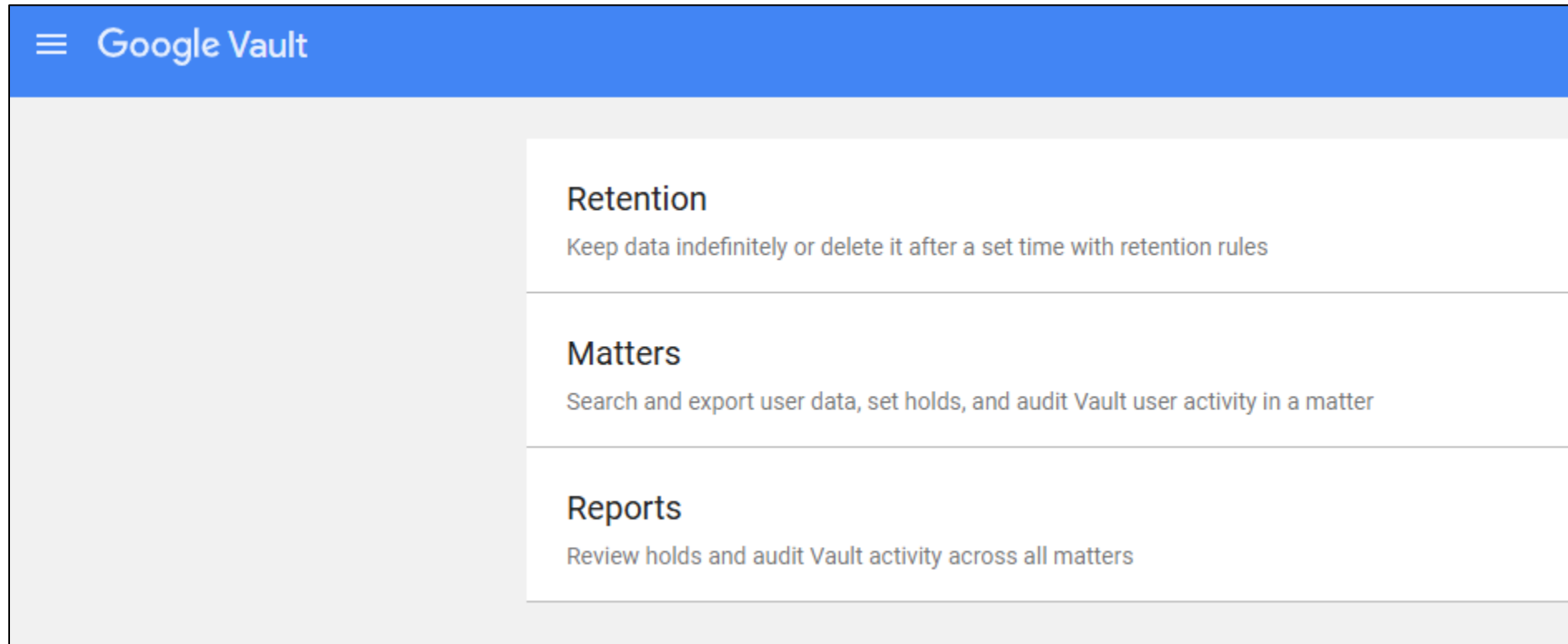
Overview of E-discovery Tools

- If a company has its own digital forensics team and legal team
 - Their efforts can be correlated easily with these tools
 - Legal team can view results at the e-discovery level
 - If it is determined that more analysis is needed, the forensics team can search deeper
- Major e-discovery tools are discussed in more detail in Chapter 3 of the course textbook

Cost and Time Considerations

- Large multinational corporations may be able to afford expensive packages to handle e-discovery
 - Small and medium firms may not have the budget
 - Freeware and shareware products can be used
 - On-prem and cloud solutions available
 - Office 365 and Google Apps have built in E-discovery platforms

Google Apps - Vault



Google Apps - Vault

SEARCH

HOLDS

EXPORTS

Search

SAVE

CLEAR

Service

 Gmail

Source

All data

Entity

Specific accounts

Account email addresses

Enter email addresses separated by commas

Time zone

(GMT-06:00) Central Time – Chicago

Date sent (optional)

Start date

End date

Example: 2019-03-31

Example: 2019-05-22

Terms (optional)

Query terms

Example: from:username1 subject:Hello has:attachment

☐ Exclude email drafts

SEARCH

COUNT

EXPORT

0365 - Exchange

Information governance

Labels Label policies Import Retention Archive

Email, documents, Skype and Teams conversations. Your users generate a lot of content every day. Take control of it by sett

+ New retention policy ↓ Export ↻ Refresh ✉ Inactive mailbox

Name

Data classification

Overview Trainable classifiers (preview) Content explorer Activity explorer

Get snapshots of how sensitive info and labels are being used across your organization's locations. [Learn more](#)

Top sensitive info types

Sensitive info types used most in your content



■ International Classification of Diseases (ICD-10-CM) ■ International Classification of Diseases (ICD-9-CM)

■ New Zealand Ministry of Health Number ■ U.S. Driver's License Number ■ EU Tax Identification Number (TIN)

■ EU National Identification Number

Cost and Time Considerations

- E-discovery can be time consuming
 - Going through all the information stored on a terabyte hard drive could take a legal team years
- Cost and time can be reduced by:
 - Asking “Which information is needed to prove a case”
 - Be specific and narrow the focus
 - Automated review with AI

Part IV

Federal Rules in U.S. Courts

Federal Rules in U.S. Courts

- Three sets of rules govern the conduct of federal court cases:
 - Federal Rules of Civil Procedure (FRCP)
 - Federal Rules of Criminal Procedure (FRCrP)
 - Federal Rules of Evidence (FRE)
- Each state has its own interpretation of these rules

The Federal Rules of Civil Procedure

- Established in 1938 by the U.S. Supreme Court
- Those involved with e-discovery need to be aware of the following rules:
 - FRCP Rule 16
 - FRCP Rule 26
 - FRCP Rule 33
 - FRCP Rule 34
 - FRCP Rule 37

The Federal Rules of Civil Procedure

- FRCP Rule 16
 - Pretrial conferences
 - Improves quality of trial and expedites the process by discouraging wasteful pretrial activities
 - Scheduling
 - Judge issues scheduling order as soon as practicable
 - May modify timing and extent of discovery
 - Management
 - Obtaining admissions and stipulations about facts or documents
 - Identifying witnesses and documents

The Federal Rules of Civil Procedure

- FRCP Rule 26
 - Duty to disclose
 - Provide contact info of individuals likely to have discoverable information as well as subjects of that information
 - Disclosure of expert testimony
 - Identify any witnesses and if they will provide a written report
 - Scope and limits of the discovery
 - Protective orders
 - 26f Conference to develop a proposed discovery plan

The Federal Rules of Civil Procedure

- FRCP Rule 33
 - Interrogatories to parties
 - A party can usually serve no more than 25 written interrogatories to another party
 - Rules for responding, timing, objections, etc.

Interrogatory Example

- <https://www.justice.gov/atr/case-document/file/494026/dl>
- What are the three sections??
 - Definitions
 - Instructions
 - Interrogatories

The Federal Rules of Civil Procedure

- FRCP Rule 34
 - Producing documents (RFPs)
 - How Electronically Stored Information should be produced
 - Native
 - Tiff
 - PDF
 - Etc.
 - Tangible things or permit an inspection

The Federal Rules of Civil Procedure

- FRCP Rule 37
 - Party can move to compel disclosure or a response if other party fails to make or to cooperate in discovery relating to
 - RFPs
 - Interrogatories
 - Depositions
 - Sanctions for violations
 - Often monetary

The Federal Rules of Criminal Procedure

- Established in 1944 by the U.S. Supreme Court
- FRCrP rules specify that when dealing with someone charged in a criminal case:
 - The rights of the individual take precedence
 - <https://www.law.cornell.edu/rules/frcrmp>

The Federal Rules of Criminal Procedure

- Main rule that addresses digital evidence is:
 - Rule 41: Search and Seizure
- 2002: the Department of Justice “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations” document
 - https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf

The Federal Rules of Evidence

- Drafted by the U.S. Supreme Court and became law in 1975
 - Applies to all evidence presented in court for both civil and criminal cases
 - <https://www.law.cornell.edu/rules/fre>

The Federal Rules of Evidence

- Introduction of digital evidence hasn't changed the FRE extensively
 - Does add many new interpretations of old rules
 - Example: Hearsay rule
 - Text messages and emails might prove the recipient had been told something; however, messages can't prove the information's accuracy

The Federal Rules of Evidence

- FRE rules that have an impact on how e-discovery is preformed:
 - Article I, Rule 103 – Rulings on Evidence
 - Article I, Rule 105 – Limited Admissibility
 - Article I, Rule 106 – Remainder of Related Writings or Recorded Statements
 - Article IV – Relevancy and Its Limits
 - Article VII – Opinions and Expert Testimony
 - Article VIII - Hearsay
 - Article X – Contents of Writings, Recordings, and Photographs

Article VII – Opinions and Expert Testimony

- A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
 - The expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
 - The testimony is based on sufficient facts or data;
 - The testimony is the product of reliable principles and methods; and
 - The expert has reliably applied the principles and methods to the facts of the case

Part V

Rules and Policies Governing Digital Evidence

Rules and Policies Governing Digital Evidence

- Important aspect of ESI is its overwhelming volume
 - Digital information may be stored in several physical locations or moved to indeterminate locations as a result of load balancing
- Location of data can affect which country's laws are in effect for e-discovery purposes
 - Emails can potentially be transmitted to anywhere in the world

Sedona Principles

- Sedona Principles - created by a group of lawyers and other professionals as guidelines for handling electronic documents
 - Emerged from a conference held in 2007
 - Designed to ease the burden of e-discovery and speed the process along
 - Lists 14 principles that link to the FRCP
 - Lay the framework for what a company must do to prepare for possible litigation

FRCP Amendments

- April 2006: U.S. Supreme Court ordered that the FRCP be amended to address e-discovery
 - Require companies to protect data that might be subject to discovery in anticipated litigation
- The Advisory Committee on Civil Rules incorporated the Sedona Principles into the 2006 amendments

FRCP Amendments

- Rule 26(b)(2) - permits parties to avoid discovery of ESI that isn't reasonably accessible because of "undue burden or cost"
 - Includes electronic information that has to be converted or recovered to be usable
- 2015 amendment now states that information is discoverable if it is relevant to the party's claim or defense and is proportional to the needs of the case

FRCP Amendments

- FRCP Rule 34(b) - dictates that ESI be provided in a form that is readily usable
 - If requesting party specifies another form, the producing party has the option of objecting to the form and proposing its own form
- Organizations that scan paper documents and replace them with electronic documents in PDF or TIFF formats:
 - Improve information-management capabilities
 - Are better positioned to handle litigation

FRCP Amendments

- Besides scanning documents, some organizations index the text
 - Using **optical character recognition (OCR)** software
- OCR software examines scanned pictures of documents and “recognizes” letters and numbers

FRCP Amendments

- Use of PDF-scanned copies instead of a native file is disputed in the legal community
 - Native files can be searched without further processing and metadata still exists

FRCP Amendments

- Lawyers have a duty to preserve evidence that's relevant to actual or potential litigation
- Amended FRCP Rule 37 (f) states the court can't impose sanctions when a party destroys ESI as part of its "routine, good faith" operations
 - Spoliation: a party wrongfully destroying evidence

FRCP Amendments

- Companies should put their ESI retention policies in writing and be able to prove that the policies are followed routinely
 - Procedures should also be drafted to place a “litigation hold” on all potentially relevant ESI

FRCP Amendments

- FRCP clarifies how ESI is handled during discovery
- ESI should be destroyed when it's no longer legally or operationally required
 - ESI retention might be affected by IRS rules, corporate policy, or ongoing projects
- Policies and procedures should be reviewed and updated as needed

State Amendments Related to ESI

- Many states have adopted provisions to address procedural issues with e-discovery
 - Texas developed rules for ESI discovery even before the FRCP amendments were passed

State Amendments Related to ESI

- States' rules can be more stringent than federal rules but not more lenient
- 30 states have adopted e-discovery procedural rules reflecting the 2006 FRCP amendments
 - 8 other states have some form of e-discovery legislation pending

**Note

- The course text mentions evidentiary laws of various countries
- To reduce confusion, we will only focus on laws within the U.S. in this course

Summary

- E-discovery is the accumulation of digital information for use in litigation
- Digital evidence can be found in a variety of forms and on a wide range of devices
- The methods used to acquire digital evidence can determine its effectiveness and admissibility in court
- A number of software tools are designed for e-discovery
- Cost and time considerations affect what tools a company selects for e-discovery and ESI retention

Summary

- In the US, the Federal Rules of Civil Procedure, along with laws such as the Sarbanes-Oxley Act, govern the ways in which corporations preserve data and data is presented or exchanged during legal proceedings
- The Federal Rules of Evidence in the US have a direct bearing on how evidence is collected and maintained in both civil and criminal cases
- The Federal Rules of Criminal Procedure take into account the U.S. Constitution and defendants' rights under the Bill of Rights

Summary

- The Sedona Principles are 14 rules that can be used to help mitigate costs and preserve evidence in e-discovery cases

Text References

- Phillips, A., Godfrey, R., Steuart, C., & Brown, C. (2014). E-discovery: An Introduction to Digital Evidence. Boston, MA: Cengage Learning.

Homework

- Review and understand this slide deck on Canvas
- Read Chapter 8 before next class
- Once the topic choices are graded you will receive which topic was selected
- Research paper outline due in 3 weeks before midnight on Monday, 2/16
 - The assignment details and rubric will be posted soon

Questions???

