Admission of Electronic Evidence

Statewide Attorneys General Conference
July 20, 2007
San Antonio, Texas

Ronald L. Chichester, Esq.
http://www.txcomputerlaw.com

Where are we?

How did we get here?

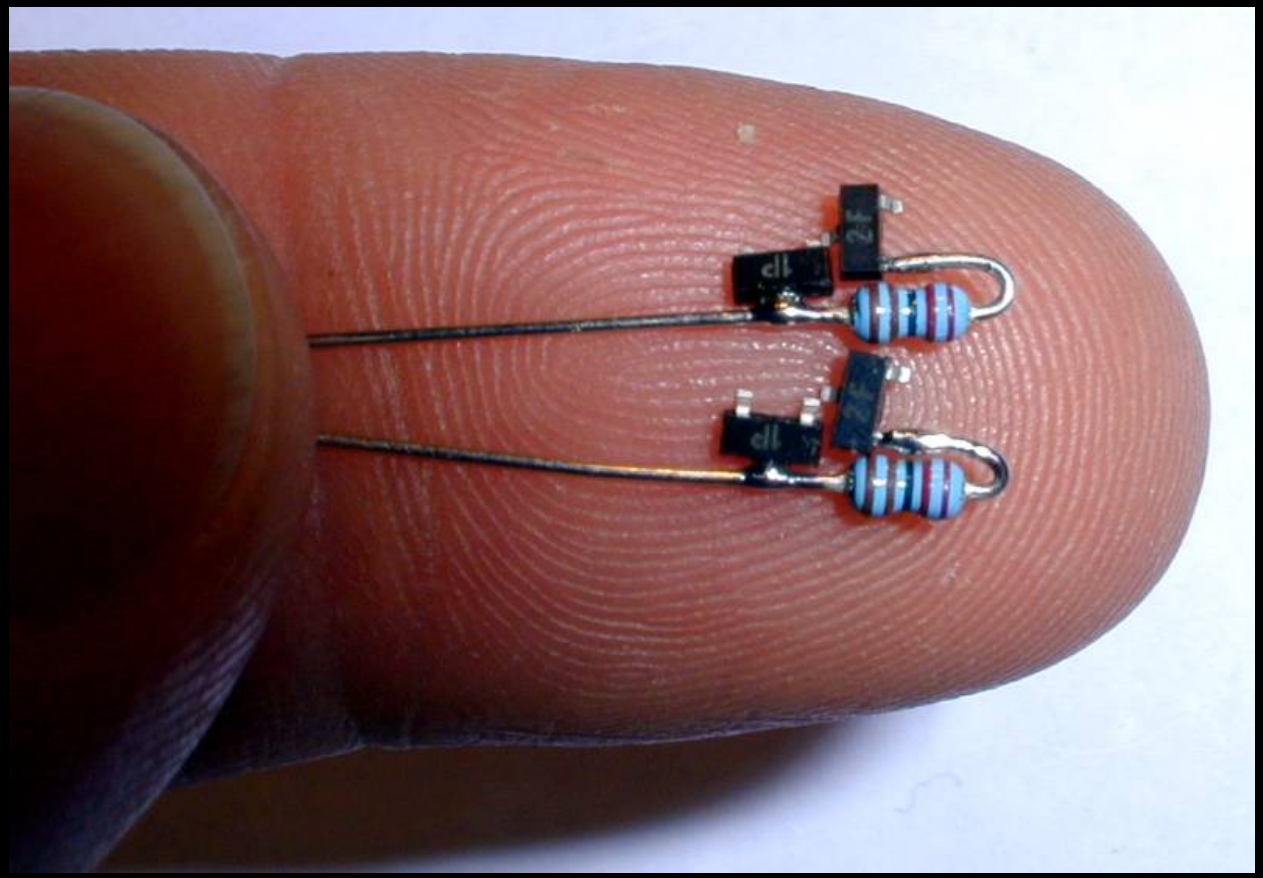
It all started with...

Wait

Actually, it started with...

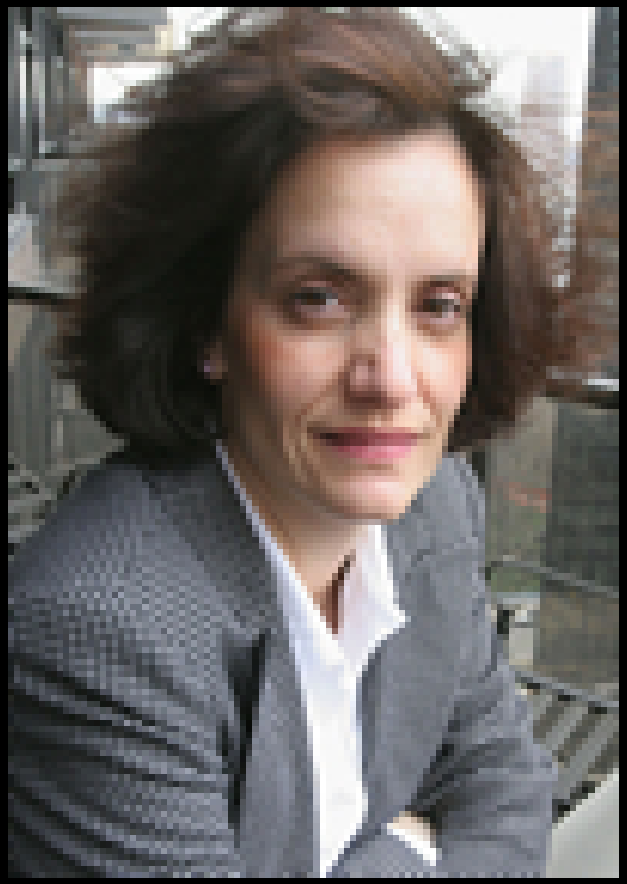
... which led to this...

... which led to this...

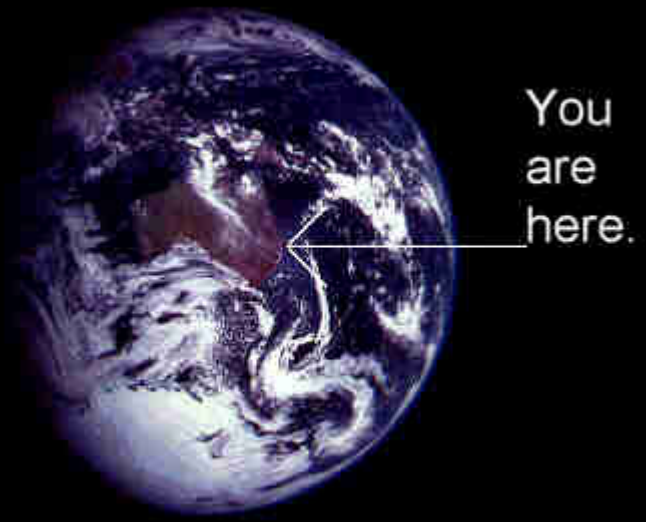


... which led to this...

... and eventually brought us to



So where are we?


You
are
here.

Where we are...

Where we are...

- Electronically Stored Information ("ESI") is discoverable.

Where we are...

- Electronically Stored Information (“ESI”) is discoverable.
- ESI can be admitted into evidence

Where we are...

- Electronically Stored Information ("ESI") is discoverable.
- ESI can be admitted into evidence *if you do it correctly*.

What does “correctly” mean?

What has changed with the Meet and Confer?

What's the two-tiered inaccessibility analysis?

What is horizontal and vertical de-duplication?

What is hashing?

What is metadata?

Produce in Native? TIFF? PDF?

Do I have to keep
Exception Logs?

Will I need a forensic image?

Fighter Pilot's Motto

Fighter Pilot's Motto

Fighter Pilot's Motto

Fighter Pilot's Motto

In Litigation

In Litigation

- Find it

In Litigation

- Find it
- Get it

In Litigation

- Find it
- Get it
- Have it admitted

What if something goes wrong?

Opps!

Opps!

- Loss of Privileged Documents

Opps!

- Loss of Privileged Documents
- Spoliation

Opps!

- Loss of Privileged Documents
- Spoliation
- Sanctions

Opps!

- Loss of Privileged Documents
- Spoliation
- Sanctions
  - Adverse Inference

Opps!

- Loss of Privileged Documents
- Spoliation
- Sanctions
  - Adverse Inference
  - Monetary

Opps!

- Loss of Privileged Documents
- Spoliation
- Sanctions
  - Adverse Inference
  - Monetary
  - Dismissal
    - Claims
    - Defenses

Find It

Find It

- Passive

Find It

- Passive
- Aggressive

Find It

- Passive
  - Google
- Aggressive

Find It

- Passive
  - Google
  - Cybersleuthing
- Aggressive

Find It

- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive

Find It

- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive
  - Discovery

Find It

- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive
  - Discovery
    - Devices

Find It

- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive
  - Discovery
    - Devices
    - Subpoenas

Find It

- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive
  - Discovery
    - Devices
    - Subpoenas
    - Third Parties

Find It

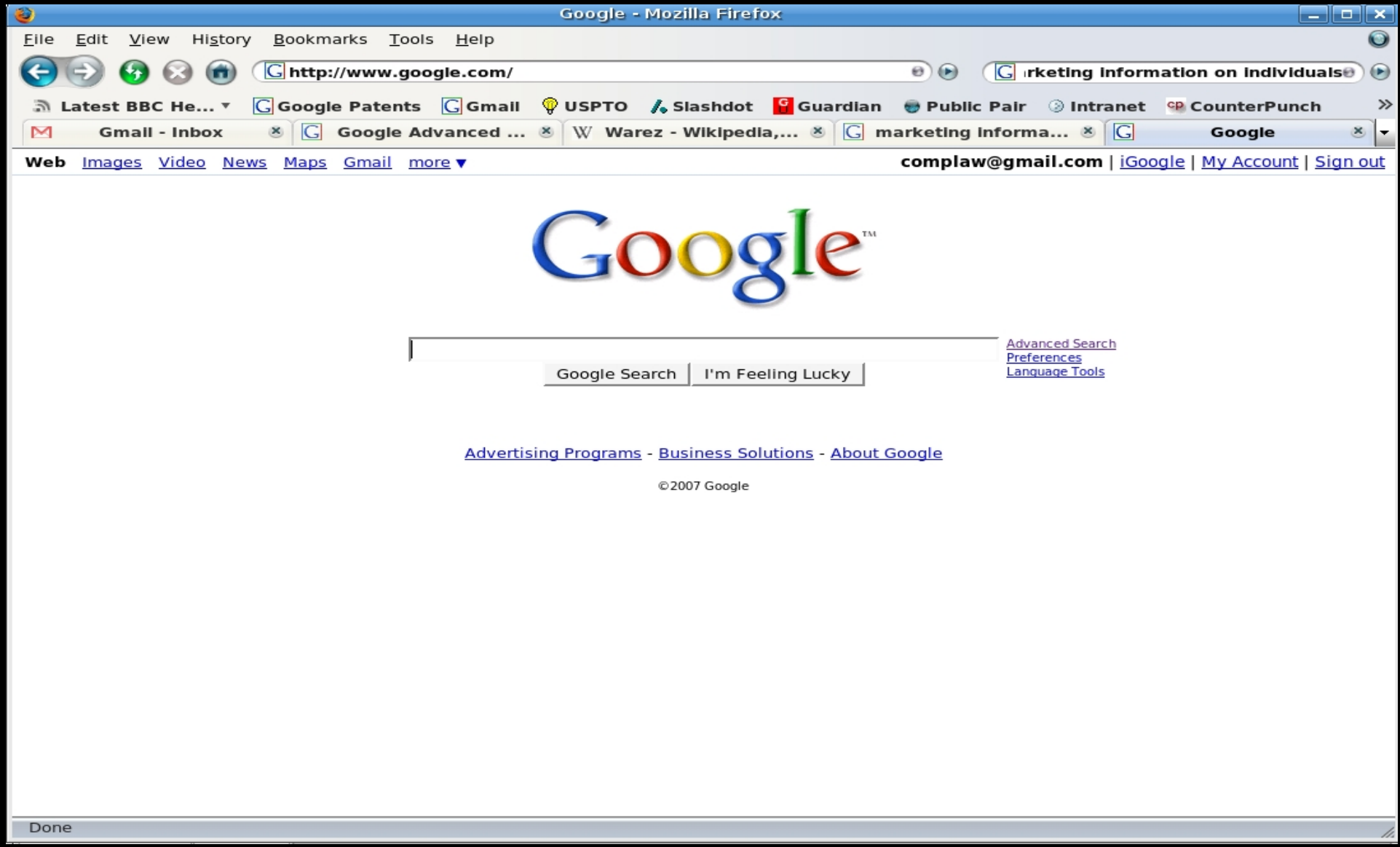
- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive
  - Discovery
    - Devices
    - Subpoenas
    - Third Parties
  - Surreptitious

Find It

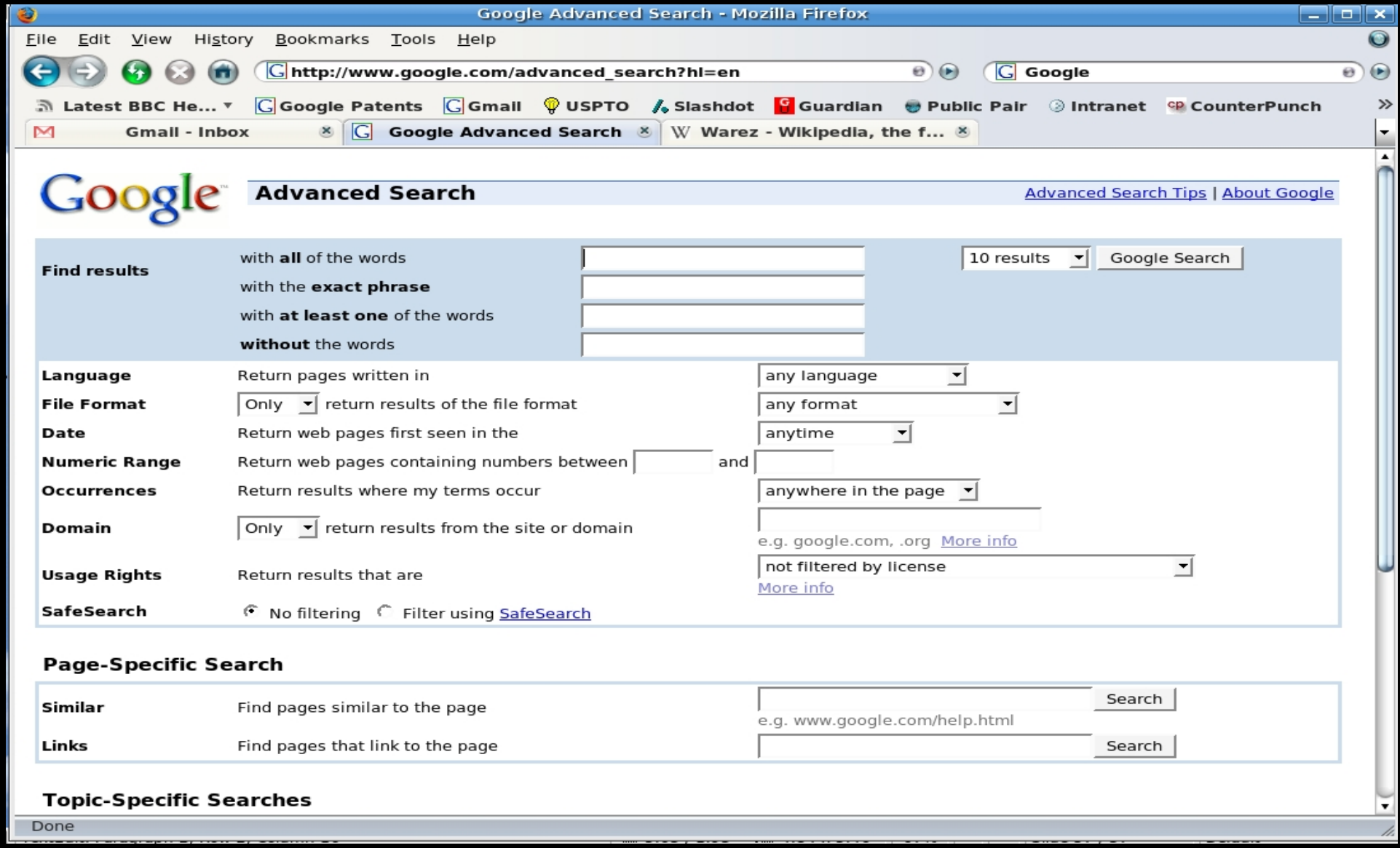
- Passive
  - Google
  - Cybersleuthing
  - Purchase the Data
- Aggressive
  - Discovery
    - Devices
    - Subpoenas
    - Third Parties
  - Surreptitious
    - Spyware
      - O'Brien v. O'Brien

Find It (Passive)

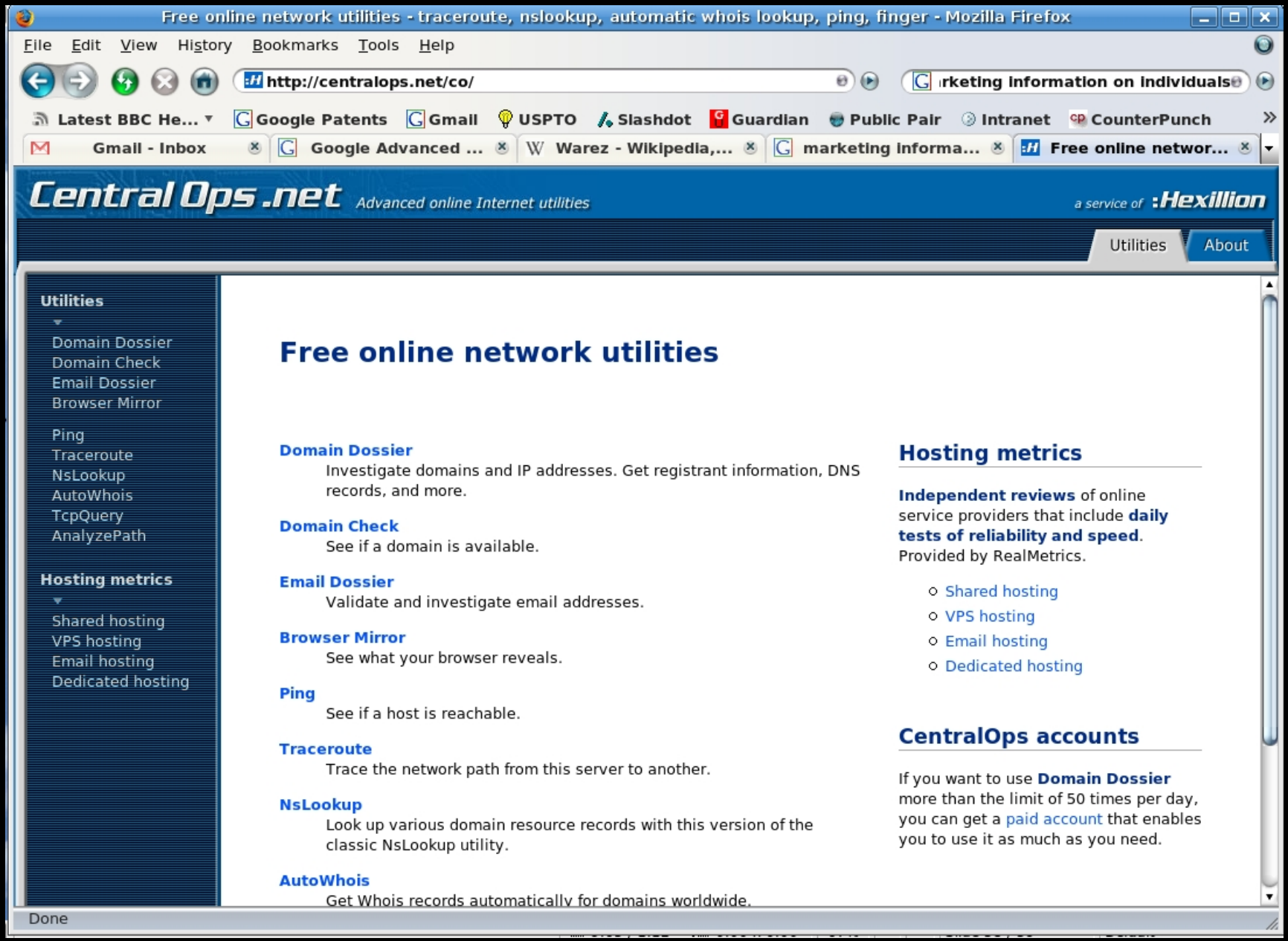
Find It (Passive)



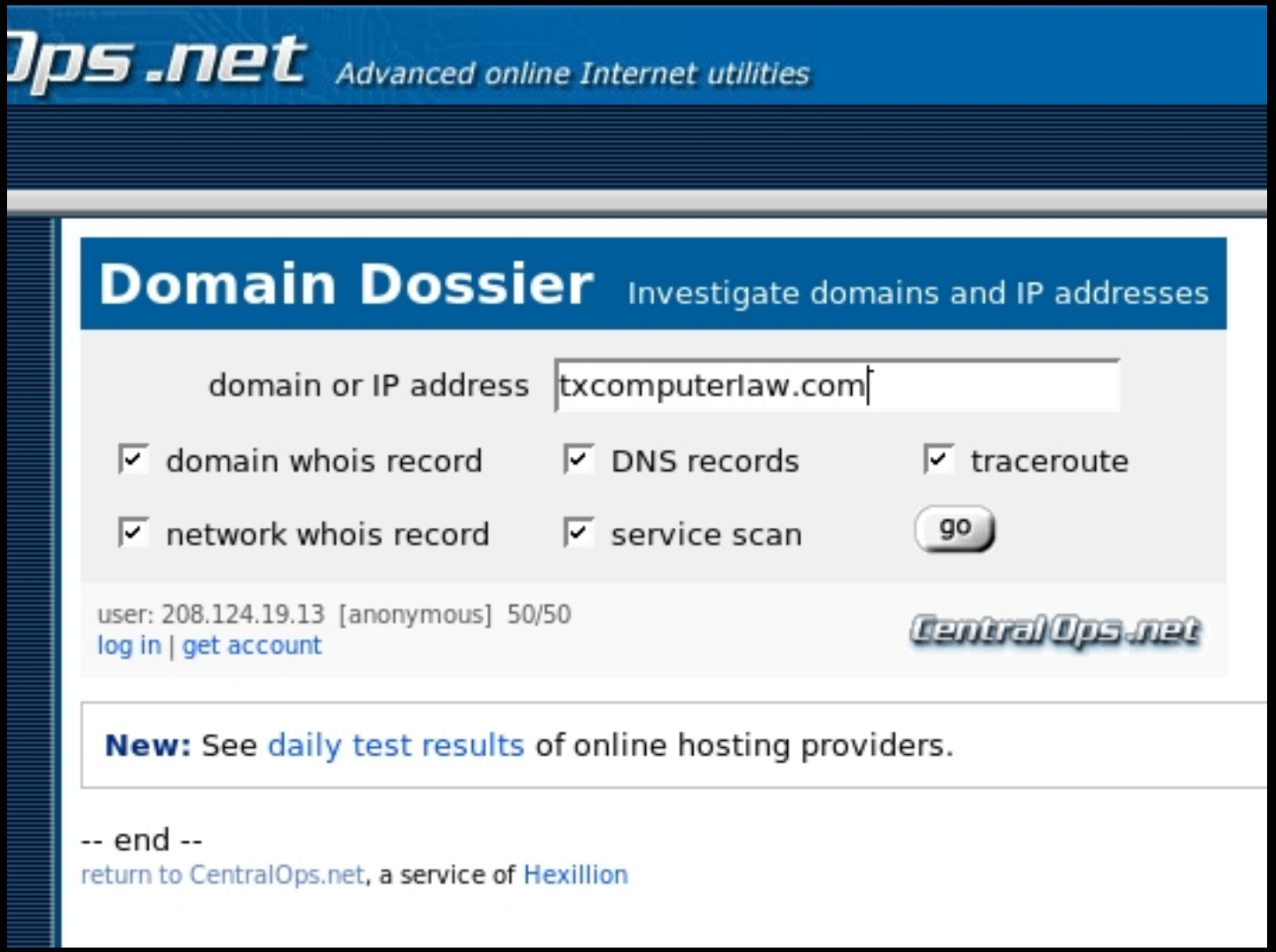
Find It (Passive)



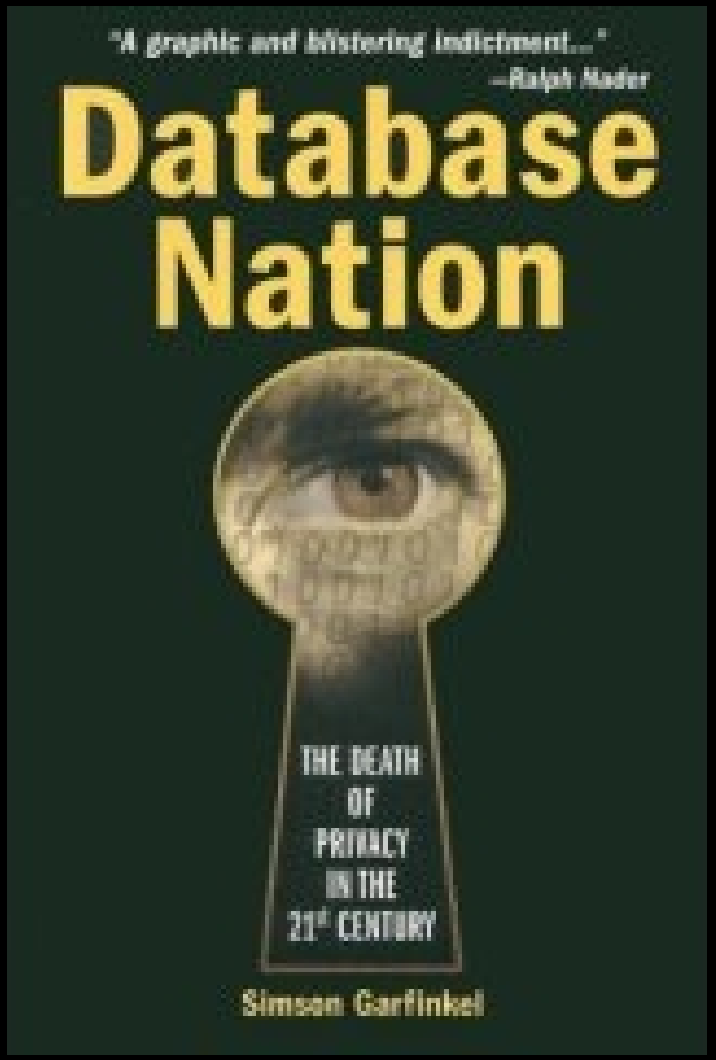
Find It (Passive)



Find It (Passive)

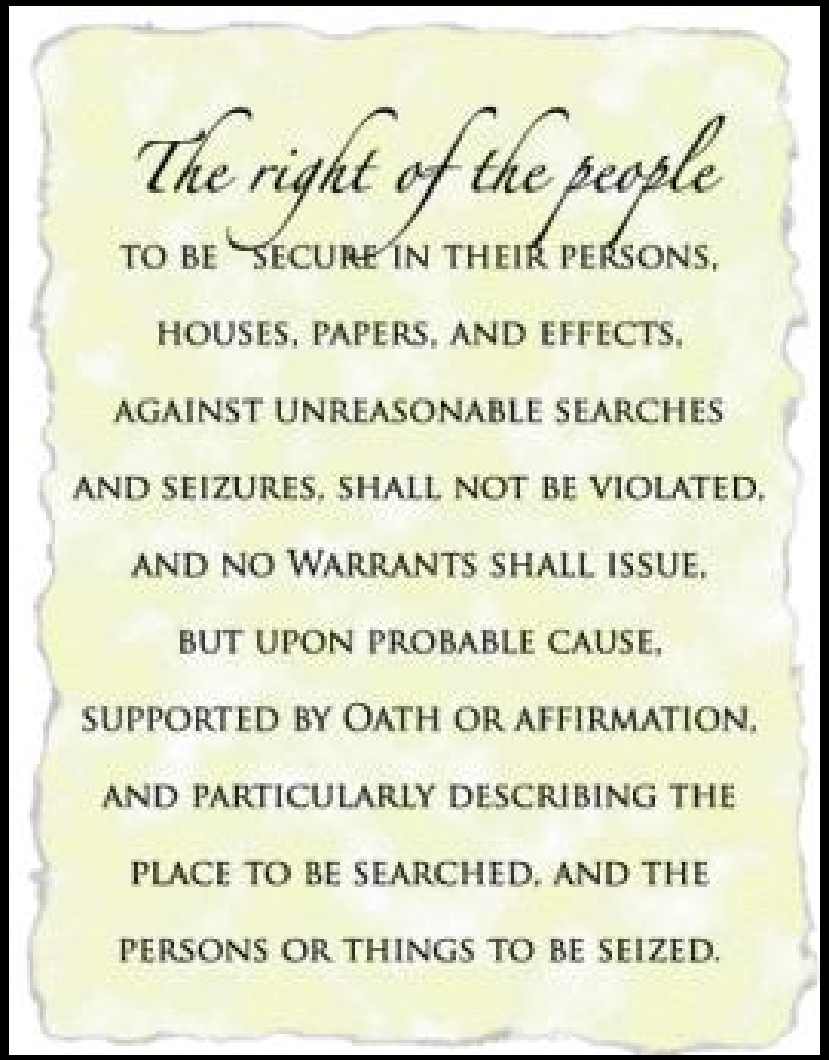


Find It (Passive)



- Buy the Data

Find It (Passive)



- Buy the Data
- No (real) Fourth Amendment Issues when purchased from Third Parties
  - Purchase the data like any other company would.

Find It (Passive)

- Buy the Data
  - Grocery Stores

Find It (Passive)

- Buy the Data
  - Grocery Stores
  - Gas Cards

Find It (Passive)

- Buy the Data
  - Grocery Stores
  - Gas Cards
  - City Records
    - Real Estate Transactions
    - Births

Find It (Passive)

- Buy the Data
  - Grocery Stores
  - Gas Cards
  - City Records
    - Real Estate Transactions
    - Births
  - Pharmacies

Find It (Passive)

- Buy the Data
  - Grocery Stores
  - Gas Cards
  - City Records
    - Real Estate Transactions
    - Births
  - Pharmacies
  - Direct Marketing Companies

Find It (Aggressive)

- Discovery

Find It (Aggressive)

- Discovery
  - Variety of Devices

Find It (Aggressive)

- Discovery
  - Variety of Devices
  - PC and DVR's

Find It (Aggressive)

- Discovery
  - Variety of Devices
  - PC and DVR's
  - Cell Phones/PDAs

Find It (Aggressive)

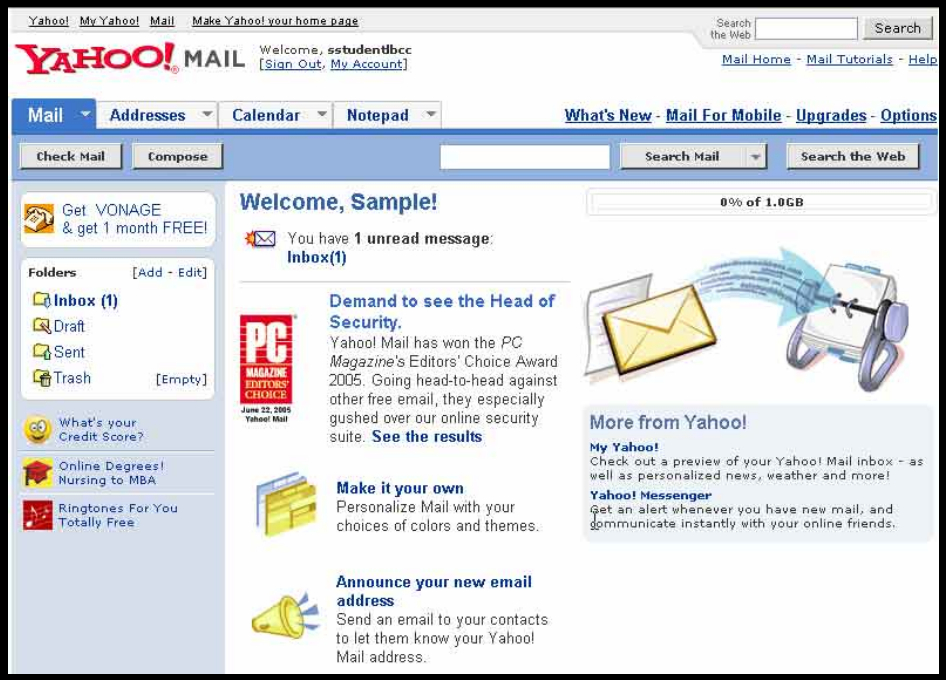
- Discovery
  - Variety of Devices
  - PC and DVR's
  - Cell Phones/PDAs
  - Thumb Drives (aka Flash Drives)

Find It (Aggressive)

- Discovery
  - Variety of Devices
  - PC and DVR's
  - Cell Phones/PDAs
  - Thumb Drives (aka Flash Drives)
  - External Hard Disks

Find It (Aggressive)

- Discovery
  - Variety of Devices
  - PC and DVR's
  - Cell Phones/PDAs
  - Thumb Drives (aka Flash Drives)
  - External Hard Disks
  - Third Party Email



Find It (Aggressive)

- Discovery
  - Variety of Devices
  - PC and DVR's
  - Cell Phones/PDAs
  - Thumb Drives (aka Flash Drives)
  - External Hard Disks
  - Third Party Email
  - CDs and DVDs

Find It (Aggressive)

And many, *many* other devices!

A Word About Forensics

A Word About Forensics

- “Delete”

A Word About Forensics

- “Delete”
  - Dictionary says:
    - “To blot out; to erase; to expunge; to dele; to omit.”

A Word About Forensics

- “Delete”
  - Dictionary says:
    - “To blot out; to erase; to expunge; to dele; to omit.”
  - In “Windows”:
    - Simply to “forget” about it.

A Word About Forensics

- “Delete”
  - Dictionary says:
    - “To blot out; to erase; to expunge; to dele; to omit.”
  - In “Windows”:
    - Simply to “forget” about it.
- The implications:

A Word About Forensics

- “Delete”
  - Dictionary says:
    - “To blot out; to erase; to expunge; to dele; to omit.”
  - In “Windows”:
    - Simply to “forget” about it.
- The implications:
  - Forensic tools can be used to recover deleted files.

A Word About Forensics

- “Delete”
  - Dictionary says:
    - “To blot out; to erase; to expunge; to dele; to omit.”
  - In “Windows”:
    - Simply to “forget” about it.
- The implications:
  - Forensic tools can be used to recover deleted files.
  - Files may be overwritten before recovery.

A Word About Forensics

- “Imaging” the drive preserves evidence.

A Word About Forensics

- “Imaging” the drive preserves evidence.
- Federal courts reluctant to allow imaging unless there is some special showing.

A Word About Forensics

- “Imaging” the drive preserves evidence.
- Federal courts reluctant to allow imaging unless there is some special showing.
- Thus, it behooves the attorney to be wary of, and act upon “tripwires” for imaging

A Word About Forensics

- “Imaging” the drive preserves evidence.
- Federal courts reluctant to allow imaging unless there is some special showing.
- Thus, it behooves the attorney to be wary of, and act upon “tripwires” for imaging
  - Analysis of files or system logs indicates:
    - changes to files and/or file metadata;
    - deletion of seemingly important files; or
    - indications of other illicit activity such as wiping.

Get It

Get It

- Requests for Production, etc.

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers

Get It


Civil Subpoena Polic
File Edit View History Bookmarks Tools Help
http://legal.web.aol.com/aol/aolpol/civilsubpoena.html
Latest BBC He...
Google Patents
Gmail
USPTO
Slashdot
Gmail - Re: Computer L...
Patents — Ronald Chich...
texas cour
AOL Legal Department
Legal Resources
Decisions & Litigation
Junk E-Mail
Intellectual Property
Policy & Public Affairs
AOL Information
Feedback
--- AOL Information ---
AOL Policies
Civil Subpoena Policy
AOL's Terms of Service provide that AOL will release account information or information sufficient to identify a member only to comply with valid legal process such as a search warrant, subpoena or court order . If you seek such identity or account information in connection with a civil legal matter, you must serve AOL with a valid subpoena.
AOL is headquartered in Loudoun County, Virginia and subject to the jurisdiction of Loudoun County Circuit Court and the United States District Court for the Eastern District of Virginia. For applicable requirements governing the issuance of foreign state subpoenas or

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers
- Don't forget...

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers
- Don't forget...
  - About all the myriad devices containing data

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers
- Don't forget...
  - About all the myriad devices containing data
  - Litigation hold notices to prevent spoliation

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers
- Don't forget...
  - About all the myriad devices containing data
  - Litigation hold notices to prevent spoliation
  - Metadata issues

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers
- Don't forget...
  - About all the myriad devices containing data
  - Litigation hold notices to prevent spoliation
  - Metadata issues
  - Ask for ALL email accounts and IM/Chat accounts and activities

Get It

- Requests for Production, etc.
- Subpoena of Third Parties/Employers
- Don't forget...
  - About all the myriad devices containing data
  - Litigation hold notices to prevent spoliation
  - Metadata issues
  - Ask for ALL email accounts and IM/Chat accounts and activities
  - Passwords and encryption algorithms

Get It

- Don't forget...
  - Get the hash values for the data files

What is a hash value?

Get It

- A hash value is a “digital fingerprint” of the data file.

Get It

- A hash value is a “digital fingerprint” of the data file.
- Same sized files may have different hash values.

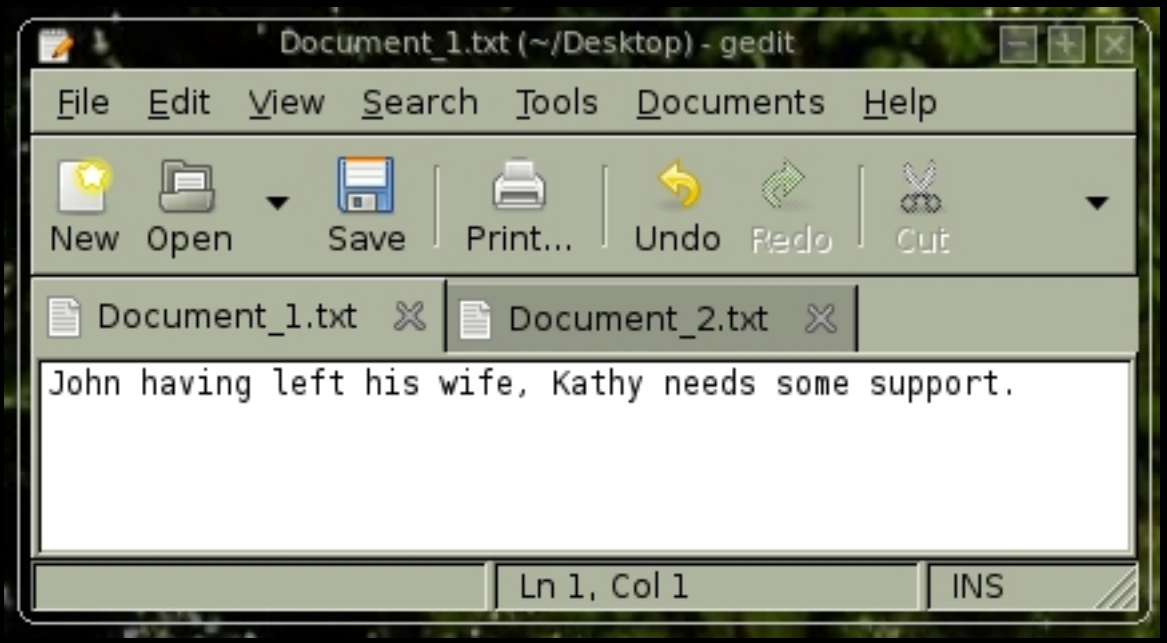
Get It

- A hash value is a “digital fingerprint” of the data file.
- Same sized files may have different hash values.
- If hash values are different, *something* is different about the files.

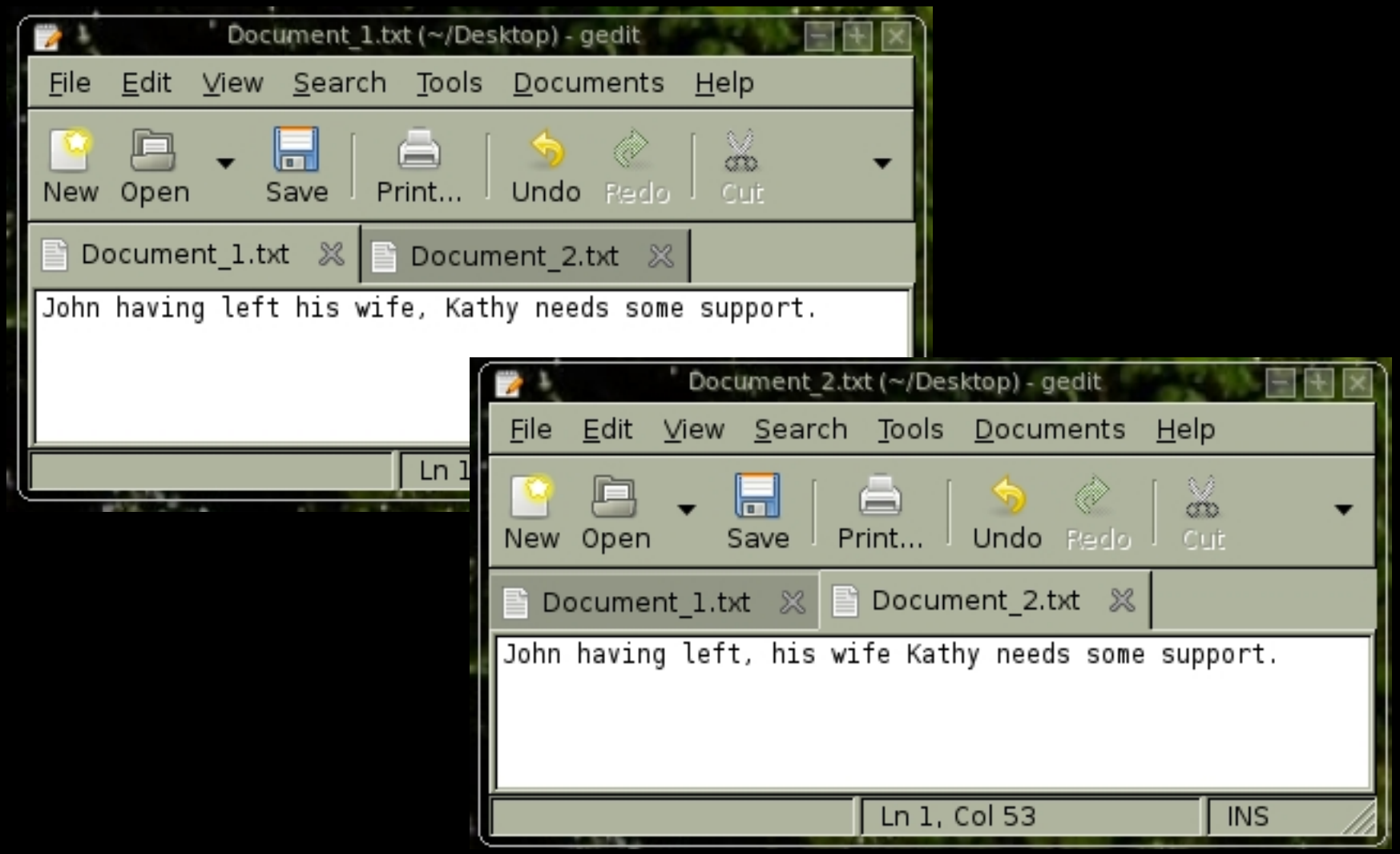
Get It

- A hash value is a “digital fingerprint” of the data file.
- Same sized files may have different hash values.
- If hash values are different, *something* is different about the files.
- Hash value may be crucial to get the data file admitted.

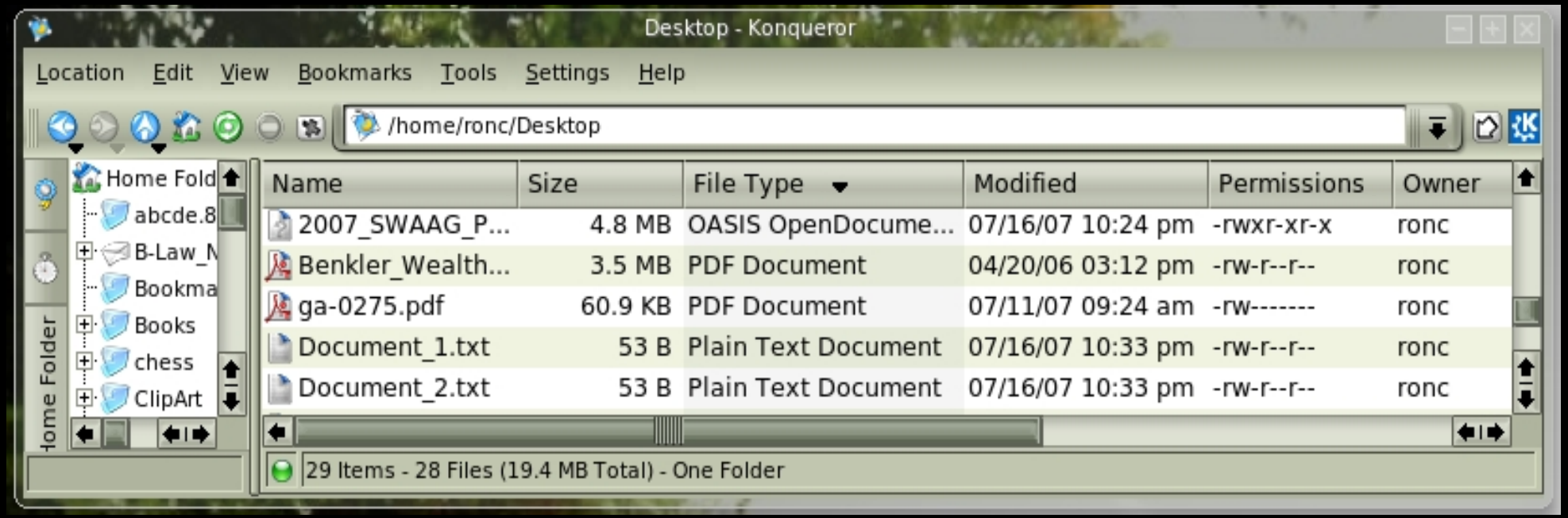
Get It


Document_1.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left his wife, Kathy needs some support.
Ln 1, Col 1
INS

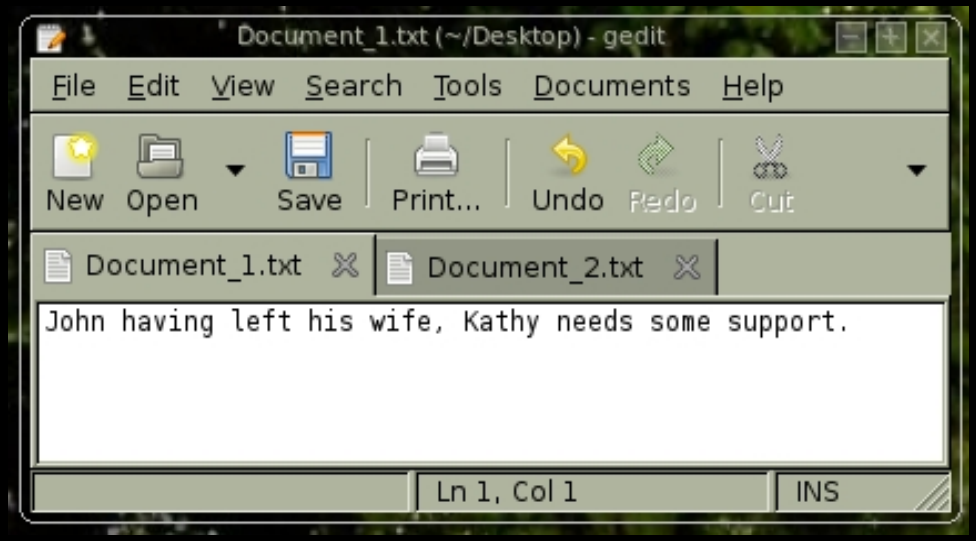
Get It


Document_1.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left his wife, Kathy needs some support.
Ln 1
Document_2.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left, his wife Kathy needs some support.
Ln 1, Col 53
INS

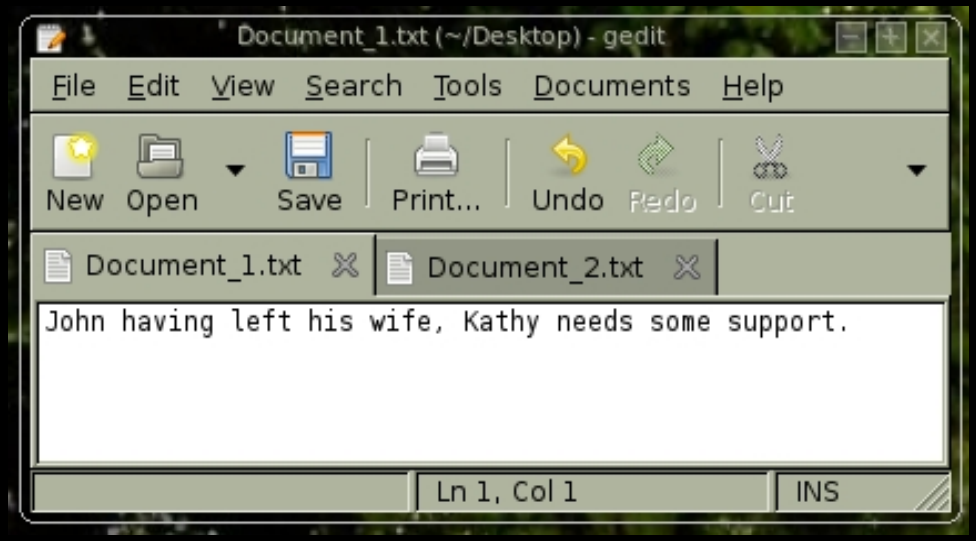
Get It

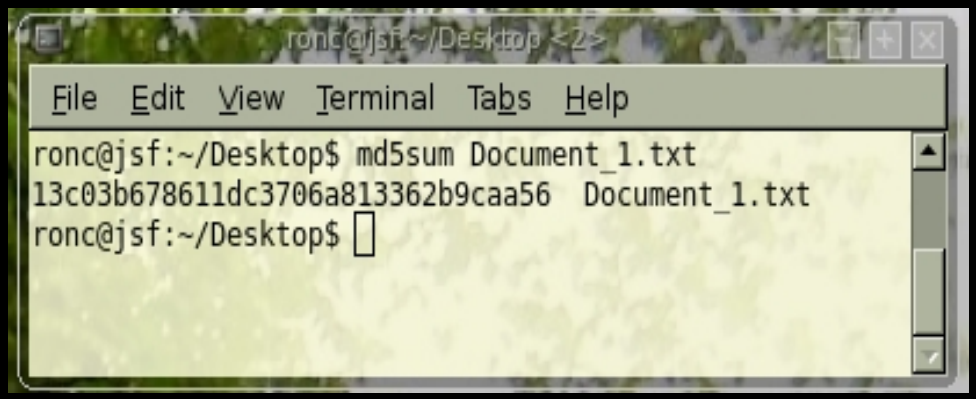

Desktop - Konqueror
Location Edit View Bookmarks Tools Settings Help
/home/ronc/Desktop
Home Fold
abcde.8
B-Law_N
Bookma
Books
chess
ClipArt
Home Folder
Name Size File Type Modified Permissions Owner
2007_SWAAG_P... 4.8 MB OASIS OpenDocume... 07/16/07 10:24 pm -rwxr-xr-x ronc
Benkler_Wealth... 3.5 MB PDF Document 04/20/06 03:12 pm -rw-r--r-- ronc
ga-0275.pdf 60.9 KB PDF Document 07/11/07 09:24 am -rw------- ronc
Document_1.txt 53 B Plain Text Document 07/16/07 10:33 pm -rw-r--r-- ronc
Document_2.txt 53 B Plain Text Document 07/16/07 10:33 pm -rw-r--r-- ronc
29 Items - 28 Files (19.4 MB Total) - One Folder

Get It

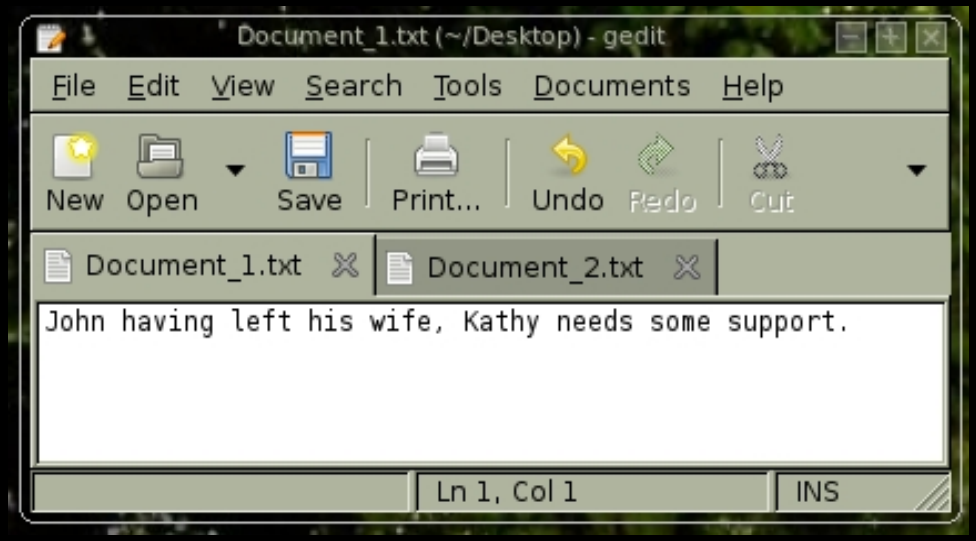

Document_1.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left his wife, Kathy needs some support.
Ln 1, Col 1
INS

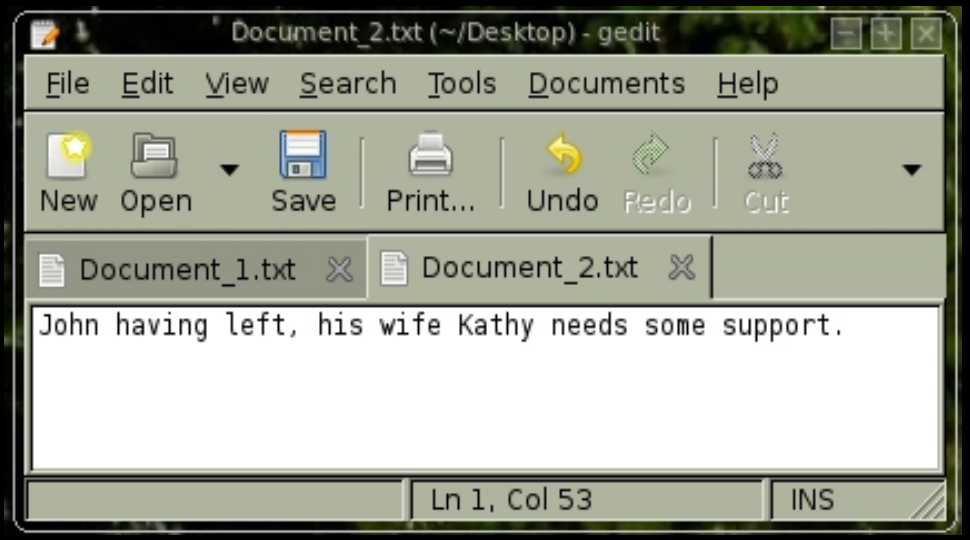
Get It

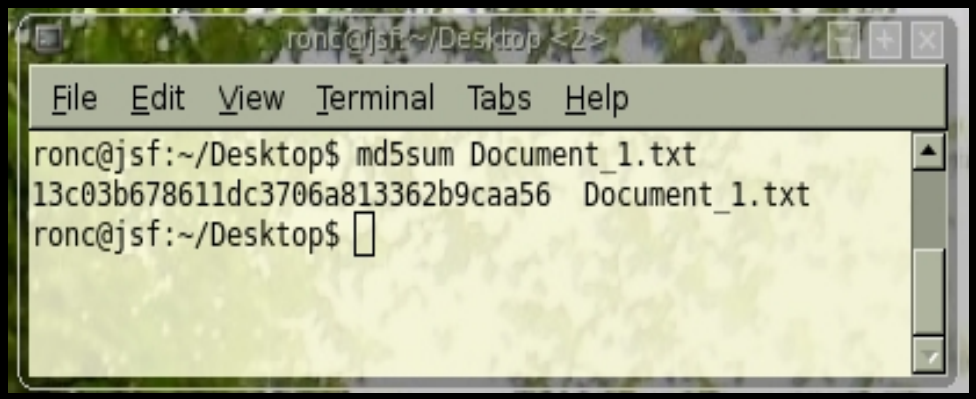

Document_1.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left his wife, Kathy needs some support.
Ln 1, Col 1
INS


File Edit View Terminal Tabs Help
ronc@jsf:~/Desktop$ md5sum Document_1.txt
13c03b678611dc3706a813362b9caa56 Document_1.txt
ronc@jsf:~/Desktop$

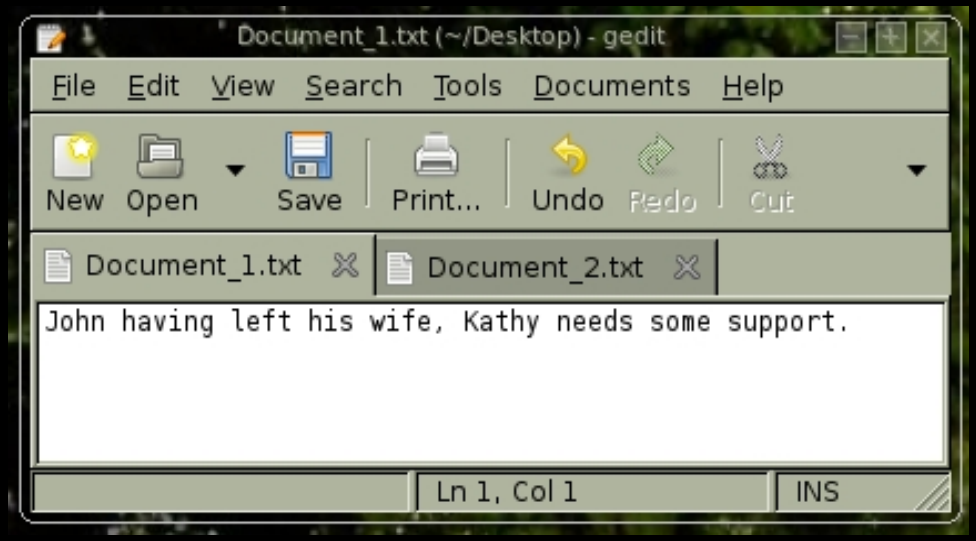
Get It

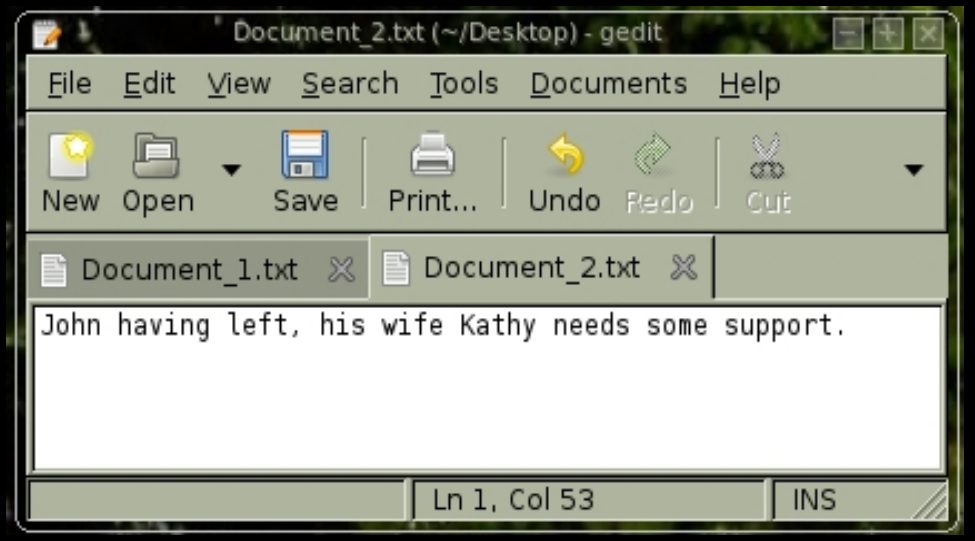

Document_1.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left his wife, Kathy needs some support.
Ln 1, Col 1
INS

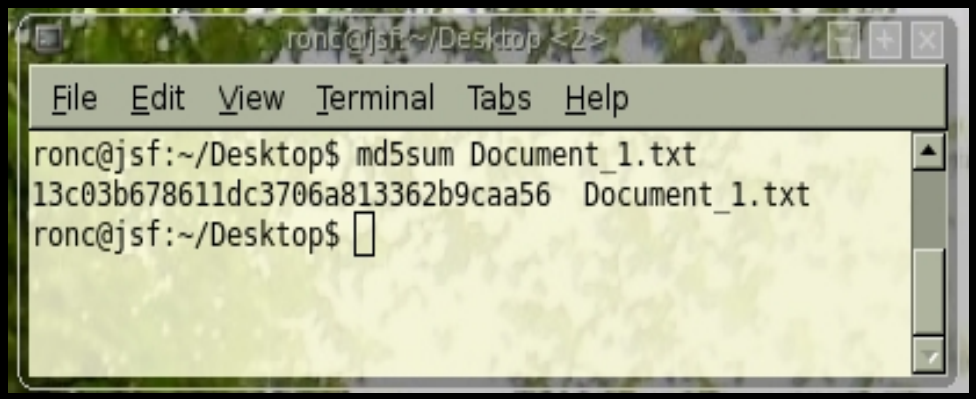

Document_2.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left, his wife Kathy needs some support.
Ln 1, Col 53
INS

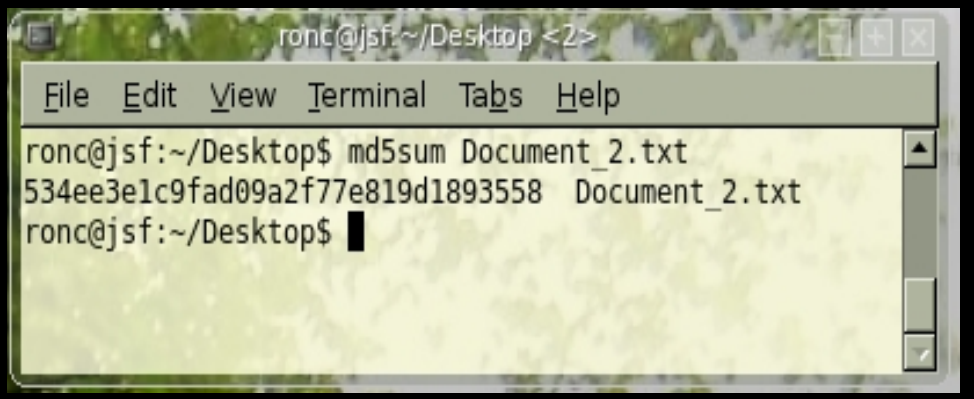

File Edit View Terminal Tabs Help
ronc@jsf:~/Desktop$ md5sum Document_1.txt
13c03b678611dc3706a813362b9caa56 Document_1.txt
ronc@jsf:~/Desktop$

Get It


Document_1.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left his wife, Kathy needs some support.
Ln 1, Col 1
INS


Document_2.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut
Document_1.txt
Document_2.txt
John having left, his wife Kathy needs some support.
Ln 1, Col 53
INS


ronc@jsf:~/Desktop <2>
File Edit View Terminal Tabs Help
ronc@jsf:~/Desktop$ md5sum Document_1.txt
13c03b678611dc3706a813362b9caa56 Document_1.txt
ronc@jsf:~/Desktop$


ronc@jsf:~/Desktop <2>
File Edit View Terminal Tabs Help
ronc@jsf:~/Desktop$ md5sum Document_2.txt
534ee3e1c9fad09a2f77e819d1893558 Document_2.txt
ronc@jsf:~/Desktop$

More Extensive Request re PC

More Extensive Request re PC

- Operating System and Patch Level

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps
- Registry Data

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps
- Registry Data
- Browser History and Cookies

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps
- Registry Data
- Browser History and Cookies
- Login History

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps
- Registry Data
- Browser History and Cookies
- Login History
- System Event Logs

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps
- Registry Data
- Browser History and Cookies
- Login History
- System Event Logs
- User Accounts

More Extensive Request re PC

- Operating System and Patch Level
- File System Time and Date Stamps
- Registry Data
- Browser History and Cookies
- Login History
- System Event Logs
- User Accounts
- Presence of Wiping/Hacking/Snooping SW

Limiting Discovery

Limiting Discovery

- Objection – Undue Burden or Expense

Limiting Discovery

- Objection – Undue Burden or Expense
- Solutions:

Limiting Discovery

- Objection – Undue Burden or Expense
- Solutions:
  - Sampling

Limiting Discovery

- Objection – Undue Burden or Expense
- Solutions:
  - Sampling
  - Limited Searching

Limiting Discovery

- Objection – Undue Burden or Expense
- Solutions:
  - Sampling
  - Limited Searching
  - Use of Filters

Limiting Discovery

- Objection – Undue Burden or Expense
- Solutions:
  - Sampling
  - Limited Searching
  - Use of Filters
  - Cost Allocation

Limiting Discovery

- Objection – Undue Burden or Expense
- Solutions:
  - Sampling
  - Limited Searching
  - Use of Filters
  - Cost Allocation
  - On-site or Limited Inspection Only

2-Tiered Inaccessibility Analysis

2-Tiered Inaccessibility Analysis

- Requesting Party asks for data
  - “Produce all email having keyword 'Grand Slam' sent in 1999.”

2-Tiered Inaccessibility Analysis

- Requesting Party asks for data
  - “Produce all email having keyword 'Grand Slam' sent in 1999.”
- “No. Not reasonably accessible”

2-Tiered Inaccessibility Analysis

- Requesting Party asks for data
  - “Produce all email having keyword 'Grand Slam' sent in 1999.”
- “No. Not reasonably accessible”
- Requesting Party moves to compel

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court
  - Responding Party must *identify nature and location* of the data and <u>prove</u> that the data is not reasonably accessible.

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court
  - If court finds the data is inaccessible, then the Requesting Party must show good cause

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court
  - If court finds the data is inaccessible, then the Requesting Party must show good cause
  - Court can order production (with conditions)

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court
  - If court finds the data is inaccessible, then the Requesting Party must show good cause
  - Court can order production (with conditions)
    - Restoration of some/all of the data

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court
  - If court finds the data is inaccessible, then the Requesting Party must show good cause
  - Court can order production (with conditions)
    - Restoration of some/all of the data
    - Require the Requesting Party to pay

2-Tiered Inaccessibility Analysis

- Dispute now goes before the court
  - If court finds the data is inaccessible, then the Requesting Party must show good cause
  - Court can order production (with conditions)
    - Restoration of some/all of the data
    - Require the Requesting Party to pay
    - Or even split the costs between the Parties

Admit It

- Evidentiary Issues
- Preliminary Questions
- Remainder of or Related Writings or Recorded Statements
- Judicial Notice
- Relevancy
- Testimony and Opinions of Experts and Lay Witnesses

Admit It

- Special Types of Computer Evidence
  - Email
  - Computerized Business Records
  - Web Pages
  - Photographs
  - Other
    - Chat Rooms
    - Text Messaging
    - Newsgroups
    - Listservs

Evidentiary Issues

- Tex. R. Evid. and Fed. R. Evid.
  - Is the evidence relevant?
  - Is there sufficient evidence for the court to grant preliminary admission of the evidence?
  - Can the evidence be properly authenticated?
  - Is the evidence hearsay and not subject to an exception?
  - Does the Best Evidence Rule require the original of the document to be produced?

Preliminary Questions

- Rule 104
- ESI can be admitted.
- However, court can refuse to admit ESI that lacks proper authentication.
  - *American Exp. Travel Related Servs. v. Vinhnee*, No. CIV.04-1284, 336 B.R. 437, 443, 447 (Bankr. Fed. App. 2005).

Preliminary Questions

- Moreover, court has authority to determine preliminary questions of law to preclude expert testimony.
  - *Daubert v. Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579 (1993).

Preliminary Questions

- Court can also consider Motions in Limine to find that certain documents (such as emails and other ESI) meet the threshold proof of Rule 104.
  - *Commerce Funding Corp. v. Comprehensive Habilitation Services, Inc.*, No. CIV.0103796, 2004 WL 1970144, at *4 (S.D.N.Y. Sept. 3, 2004).

Remainders

- Rule 106
- Be prepared to ask for (or produce) the remainder of related ESI.
- *Williams v. Sprint/United Mgmt. Co.,* 230 F.R.D. 640, 652-653 (D. Kan. 2005) (Court, ordered the production of electronic spreadsheets with metadata intact and cells unlocked).

Judicial Notice

- Rule 201
- *Wible v. Aetna Life Ins. Co.*, CIV.04-04219, 2005 WL 1592907 (C.D.Cal. Jun. 20, 2005) (ERISA case where the court took judicial notice of website evidence from an Amazon.com web page and a page from the website of the American Academy of Allergy Asthma & Immunology).

Relevancy

- Rules 401 – 403
- ESI *can* be relevant..
- *Williams v. Sprint/United Mgmt. Co.,* 230 F.R.D. 640, 652-653 (D. Kan. 2005) (Court, in deeming metadata relevant, ordered metadata to be produced).

Testimony and Opinions by Experts and Lay Witnesses

- Rules 701 – 705
- Lay Witness (Rule 701) has particular impart with ESI.
  - *Bazak Int'l. Corp. v. Tarrant Apparel Group*, 378 F. Supp. 2d 377, 392 (D.N.Y. 2005) (Court noted that authenticity of e-mail could not be determined by witness affidavit where a witness was not designated as an “expert witness” and failed to meet the “lay witness” requirements of Rule 701).

Testimony and Opinions by Experts and Lay Witnesses

- Expert Testimony (Rules 702 – 705)
  - Forensic Expert Credentials and Qualifications
  - The Good
    - *Galaxy Computer Services, Inc. v. Baker*, 2005 WL 1278956 (E.D. Va. May 27, 2005); *MGE UPS Sys. v. Fakouri Elec. Eng'g., Inc.*, 2006 U.S. Dist. LEXIS 14142 (D. Tex. Mar. 16, 2006)
  - The Bad
    - *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90 (D. Colo. 1996); *Taylor v. State*, 93 S.W. 3d 487 (Tex.App. 2002)

Hearsay

- Rules 801 – 805 and 807
- Hearsay Rule applies to ESI.
- However, similar to conventional paper documents, if an electronic document is offered for the truth of its contents, it would be hearsay and inadmissible in the absence of an applicable exception.

Authentication

- Rules 901 – 902
- Authentication is a necessary condition precedent to admission.
  - *American Exp. Travel Related Servs. v. Vinhnee*, No. CIV.04-1284, 336 B.R. 437, 443, 447 (Bankr. Fed. App. 2005) (Court refused to admit creditor credit card information for failure to authenticate).

Authentication

- Can be hard to trace who is indeed the author of the ESI.
  - Use of Shared Network Drives
  - Multiple Users on a particular PC
  - Collaborative Software

Authentication

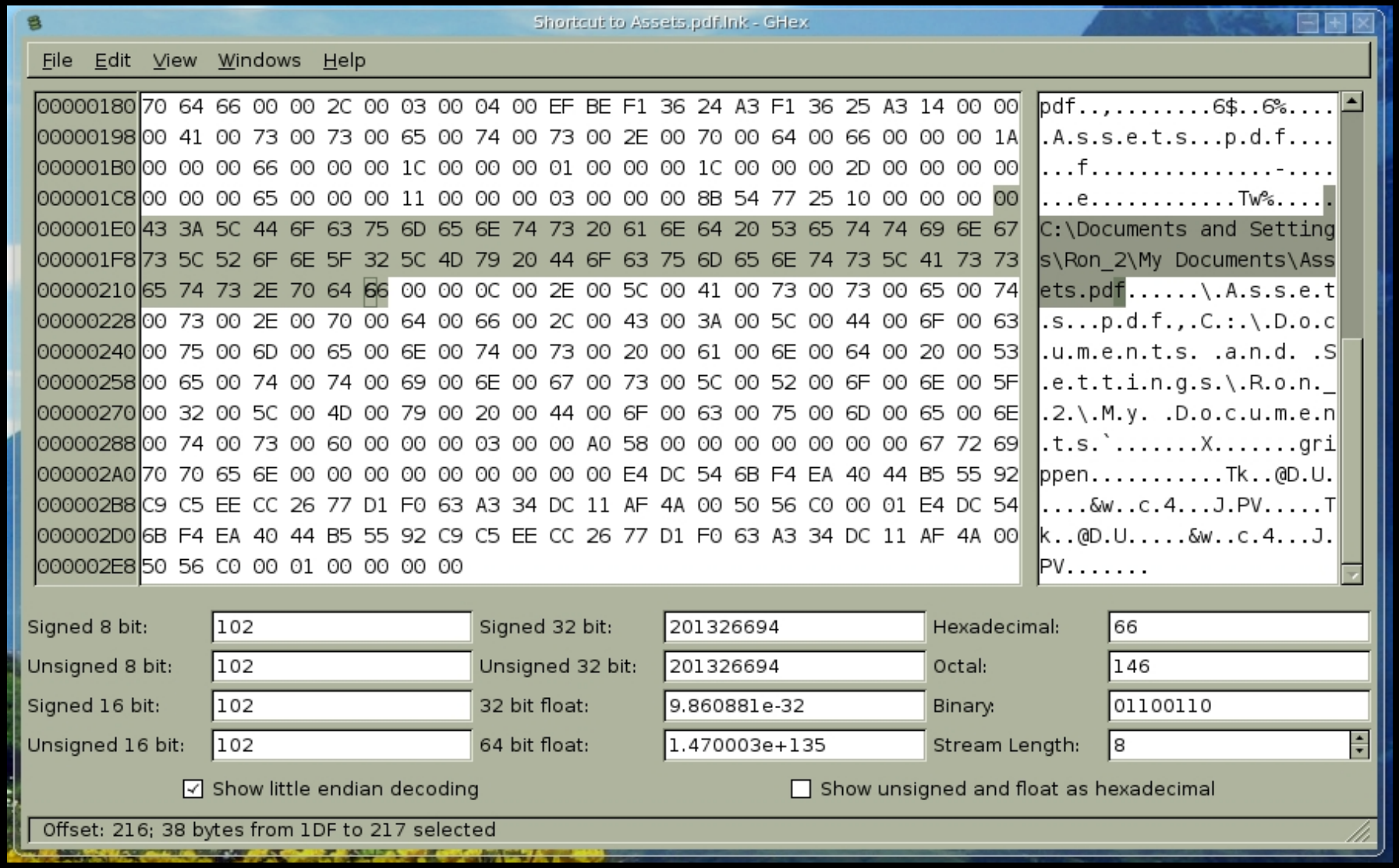
- Authentication can be derived from direct or circumstantial evidence.
  - Direct
    - Testimony from the author of the ESI
  - Circumstantial
    - Corporate markings
    - Unique writing characteristics
    - Computer audit trails and logs
    - Hash values / Chain of custody
    - Authentication intermediaries

Example

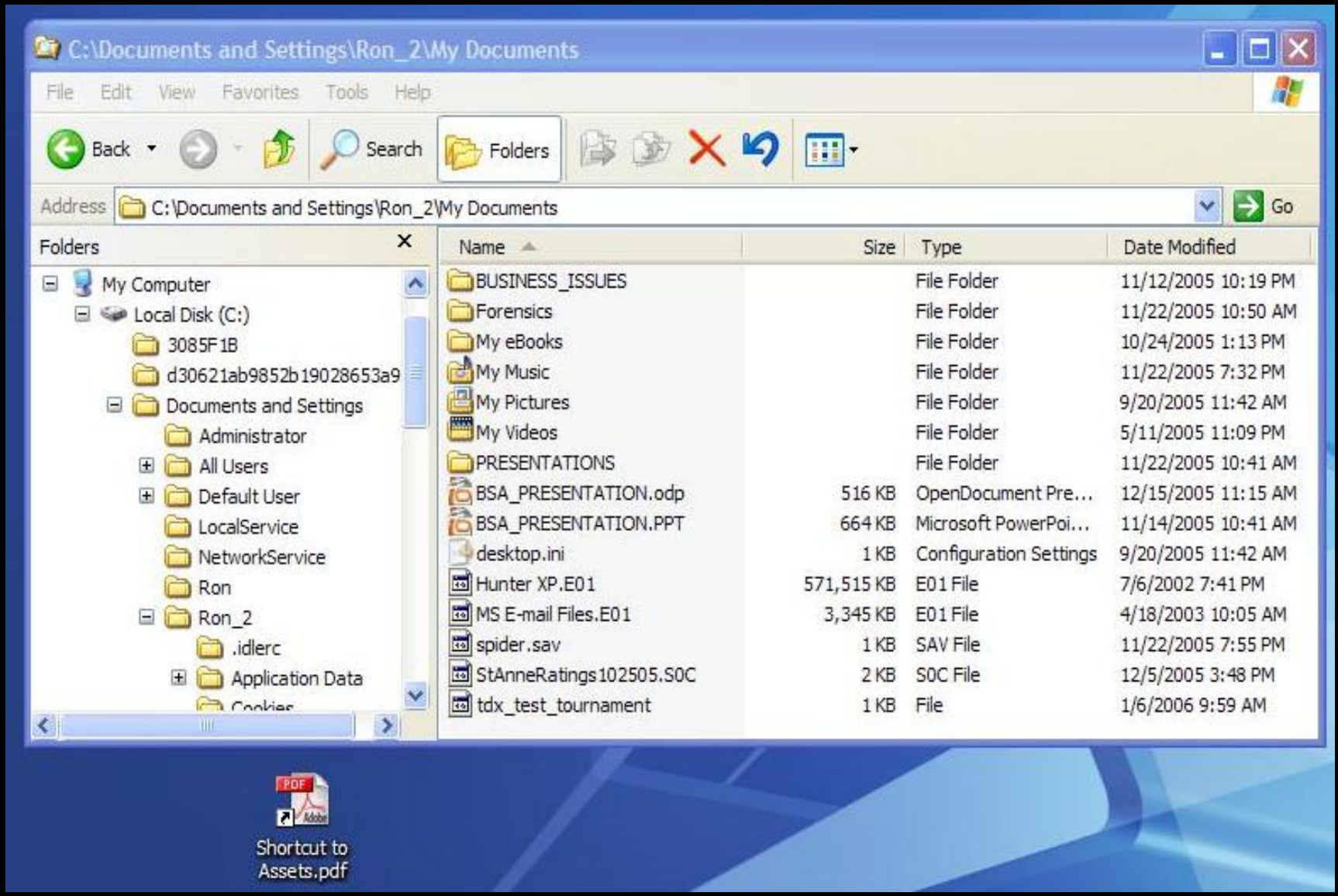
- Child Support Case
  - State asked for all electronic data files from the Father that deal with his assets.
  - Smart AAG also asked for all Desktop Shortcuts, Browser activity files, cookies, etc.
    - potentially relevant; and
    - reasonably accessible
  - One of the documents produced was called: “Shortcut to Assets.pdf.lnk”

Example

Example


Shortcut to Assets.pdf.lnk - GHex
File Edit View Windows Help
00000180 70 64 66 00 00 2C 00 03 00 04 00 EF BE F1 36 24 A3 F1 36 25 A3 14 00 00
00000198 00 41 00 73 00 73 00 65 00 74 00 73 00 2E 00 70 00 64 00 66 00 00 00 1A
000001B0 00 00 00 66 00 00 00 1C 00 00 00 01 00 00 00 1C 00 00 00 2D 00 00 00 00
000001C8 00 00 00 65 00 00 00 11 00 00 00 03 00 00 00 8B 54 77 25 10 00 00 00 00
000001E0 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67
000001F8 73 5C 52 6F 6E 5F 32 5C 4D 79 20 44 6F 63 75 6D 65 6E 74 73 5C 41 73 73
00000210 65 74 73 2E 70 64 66 00 00 0C 00 2E 00 5C 00 41 00 73 00 73 00 65 00 74
00000228 00 73 00 2E 00 70 00 64 00 66 00 2C 00 43 00 3A 00 5C 00 44 00 6F 00 63
00000240 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53
00000258 00 65 00 74 00 74 00 69 00 6E 00 67 00 73 00 5C 00 52 00 6F 00 6E 00 5F
00000270 00 32 00 5C 00 4D 00 79 00 20 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E
00000288 00 74 00 73 00 60 00 00 00 03 00 00 A0 58 00 00 00 00 00 00 00 67 72 69
000002A0 70 70 65 6E 00 00 00 00 00 00 00 00 00 E4 DC 54 6B F4 EA 40 44 B5 55 92
000002B8 C9 C5 EE CC 26 77 D1 F0 63 A3 34 DC 11 AF 4A 00 50 56 C0 00 01 E4 DC 54
000002D0 6B F4 EA 40 44 B5 55 92 C9 C5 EE CC 26 77 D1 F0 63 A3 34 DC 11 AF 4A 00
000002E8 50 56 C0 00 01 00 00 00 00
pdf..,.....6$..6%....
.A.s.s.e.t.s...p.d.f....
...f.............-....
...e.....Tw%....
C:\Documents and Setting
s\Ron_2\My Documents\Ass
ets.pdf.....\.A.s.s.e.t
.s...p.d.f.,.C.:.\.D.o.c
.u.m.e.n.t.s. .a.n.d. .S
.e.t.t.i.n.g.s.\.R.o.n._
.2.\.M.y. .D.o.c.u.m.e.n
.t.s.`.....X.....gri
ppen.....Tk..@D.U.
....&w..c.4...J.PV.....T
k..@D.U.....&w..c.4...J.
PV.....
Signed 8 bit: 102
Signed 32 bit: 201326694
Hexadecimal: 66
Unsigned 8 bit: 102
Unsigned 32 bit: 201326694
Octal: 146
Signed 16 bit: 102
32 bit float: 9.860881e-32
Binary: 01100110
Unsigned 16 bit: 102
64 bit float: 1.470003e+135
Stream Length: 8
Show little endian decoding
Show unsigned and float as hexadecimal
Offset: 216; 38 bytes from 1DF to 217 selected

Example


C:\Documents and Settings\Ron_2\My Documents
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Ron_2\My Documents
Go
Folders
My Computer
Local Disk (C:)
3085F1B
d30621ab9852b19028653a9
Documents and Settings
Administrator
All Users
Default User
LocalService
NetworkService
Ron
Ron_2
.idlerc
Application Data
Name Size Type Date Modified
BUSINESS_ISSUES File Folder 11/12/2005 10:19 PM
Forensics File Folder 11/22/2005 10:50 AM
My eBooks File Folder 10/24/2005 1:13 PM
My Music File Folder 11/22/2005 7:32 PM
My Pictures File Folder 9/20/2005 11:42 AM
My Videos File Folder 5/11/2005 11:09 PM
PRESENTATIONS File Folder 11/22/2005 10:41 AM
BSA_PRESENTATION.odp 516 KB OpenDocument Pre... 12/15/2005 11:15 AM
BSA_PRESENTATION.PPT 664 KB Microsoft PowerPoi... 11/14/2005 10:41 AM
desktop.ini 1 KB Configuration Settings 9/20/2005 11:42 AM
Hunter XP.E01 571,515 KB E01 File 7/6/2002 7:41 PM
MS E-mail Files.E01 3,345 KB E01 File 4/18/2003 10:05 AM
spider.sav 1 KB SAV File 11/22/2005 7:55 PM
StAnneRatings102505.S0C 2 KB S0C File 12/5/2005 3:48 PM
tdx_test_tournament 1 KB File 1/6/2006 9:59 AM
Shortcut to Assets.pdf

Example

- Based on shortcut to missing file (Assets.pdf), able to ask the court for permission to image the Father's hard disk.
  - Want to make the image before data is overwritten.
  - Court may impose conditions...
    - Designate who makes the image.
    - Who gets what data.

Authentication

- BEST PRACTICES...
- When you receive electronic files, there should be an audit or accounting of every file throughout the discovery, conversion and presentation process.
- The report should reflect every step of the intake and final production of the information to ensure verification.

Authentication

- At a minimum, the report should include:
  - The type of the original storage media;
  - Description of the different directories and subdirectories;
  - The number of bytes (kilo, mega, giga) and description of different computer files on the storage medium;
  - The number of files within each piece of storage medium;

Authentication

- The report should further include:
  - The number of files where data was extracted and converted to database, full text or images;
  - Hash values for each file (and each complete medium)
  - Extraction data specifying:
    - By whom,
    - from,
    - where, and
    - when

Authentication

- The report should further include:
  - The number of images that were rendered from this conversion; and
  - A listing of those files not converted (and an explanation why they weren't converted).

Authentication

- Chain of Custody
  - Used to prove that the evidence has not been altered or changed
    - from the time it was collected through
    - to the time it is produced in court.

Authentication

- Chain of Custody
  - Testimony would include how the data was:
    - gathered;
    - transported;
    - analyzed; and
    - preserved for production.
  - *See, e.g.*, *Galaxy Computer Services, Inc. v. Baker*, 2005 WL 1278956 (E.D. Va. May 27, 2005) (discussing gaps in the chain of custody).

Authentication

- Forensic Examiners will (should):
  - Refrain from altering the original evidence, both in the collection, storage and analysis
  - Document procedures used in the collection, storage and analysis, including:
    - What type of evidence was collected;
    - Where the evidence was collected;
    - Who handled the evidence before it was collected, while it was stored, and after it was examined
    - How the evidence was collected and stored; and
    - When the evidence was collected.

Authentication

- Document and explain any changes to the evidence, and establish auditable procedures
- Maintain the continuity of evidence
- Make a complete copy of the data in question
- Utilize a reliable copy process (e.g., independently verifiable (e.g. hash values))
- Employ security measures (e.g., tamperproof storage, write protection)
- Properly label time, date, source (+ tracking)
- Limiting and documenting the persons with access to the data

Authentication

- Representative cases:
  - *United States v. Scott-Emuakpor*, 2000 WL 288443 (W.D. Mich. Jan. 25, 2000) (discussing authentication of evidence from defendant's computers); *United States v. Smith*, 609 F.2d 1294 (9th Cir. 1979) (e-document authorship); *United States v. Troeano*, 252 F.3d 653 (2nd Cir. 2001) (authentication of audio tapes); In the Interest of F.P., --- A.2d ---, 2005 WL 1399264 (Pa.Super., June 15, 2005) (authentication of instant messages).

Authentication

- Representative cases:
  - Krumwiede v. Brighton Assocs., L.L.C., 2006 WL 1308629 (N.D. Ill. May 8, 2006) (alteration of computer files changed file metadata to the point that it was impossible for defendant to authenticate documents);

Authentication

- Rules 1001 – 1008 (Best Evidence Rule)
  - Printouts, an “electronic image” (such as a TIFF or PDF replica) should meet the Best Evidence Rule, even if the metadata is stripped off in the process. See, e.g., *In re Bristol-Meyers Squibb Securities Litigation, 205 F.R.D. 437 (D.N.J. 2002).*

Authentication

- Best Evidence Rule
  - *Broderick v. State*, 35 S.W.3d 67 (Tex. App. 2000). In child sex abuse prosecution, the court affirmed the trial court's admission of a duplicate of defendant's hard drive, in place of the original. The court concluded that the state's best evidence rule did not preclude admission because the computer expert testified that the copy of the hard drive exactly duplicated the contents of the hard drive.

Authentication

- Best Evidence Rule
  - *United States of America v. Seifert*, __ F.3d __ (8th Cir. April 19, 2006) (Defendant argued (unsuccessfully) that digitally enhanced video surveillance footage should not have been admitted because it violated the Best Evidence Rule).

Authentication

- Best Evidence Rule and Metadata
  - Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993) (Stripping of metadata by reduction of body to paper "dismembered" the document).

Email Authentication

- Traditional rules apply
  - Computer-generated evidence, like e-mail, must be authenticated prior to admission and consideration by the trier of fact. *Uncle Henry's, Inc. v. Plaut Consulting inc.*, 240 F. Supp. 2d 63, 71 (D. Me. 2002) (“e-mails (like letters and other documents) must be properly authenticated or shown to be self-authenticating.”).

Email Authentication

- Judge, pursuant to Rules 104 and 901, makes a preliminary determination as to authentication.
  - Evidence as to weight comes later, to prove whether the e-mail is what it purports to be and whether there is a connection between the e-mail and a particular individual.

Email Authentication

- Rule 901 sets guidance for authentication
  - Authentication by testimony of a witness with knowledge “that a matter is what it claims to be.” (e.g., the witness may have actually observed the person creating and sending e-mail and can testify as to its authentication.)
  - Evidence can be authenticated by the presence of “distinctive characteristics and the like.” (e.g., appearance, contents, substance, internal patterns, or other distinctive characteristics, per circumstances.

Email Authentication

- Rule 901(b)(10) allows for authentication by “methods provided by statute or rule.”
- Rule 902(7) allows for self-authentication by “trade inscriptions, signs, tags, or labels purporting to have been *affixed in the course of business* and indicating ownership, control or origin.
  - Particularly useful for self-authentication of business communications.

Email Authentication

- Authentication may involved testimony...
  - Can the author, recipient or a third party identify a printout of the email?
  - Does the email printout accurately reflect what was in the computer?
  - Can someone testify as to the identity of the author/sender of the email?
  - Was a password required to be entered before sending or receiving email by either the author or the recipient?

Email Authentication

- Authentication may involved testimony...
  - Did the recipient receive the email?
  - Describe the contents of the email.
  - Does the message show the origin of the email – such as the author's name and/or email address?
  - Was the author using the computer on that particular day? (e.g., reference PC user logs)
  - Did the body of the email contain the typewritten name or nickname of the author?

Email Authentication

- Authentication may involved testimony…
  - Were the facts discussed in the email known only to the individual (such as the author) that sent it or other people?
  - Were there any distinguishing writing characteristics of the author? Did the author have a particular word choice or sentence structure?
  - Was the purported author likely to know the information that was reflected in the message?

Email Authentication

- Authentication may involved testimony…
  - Was there any subsequent conversation or action regarding the email?
  - After receiving the email, did someone have a conversation with the author that reflected his knowledge of the contents and connection with the email?
  - Did the author take action consistent with the content of the message?
    - Delivery of merchandise? Firing of employee?

Email Authentication

- Authentication may involved testimony…
  - Was it necessary to enter a password to gain access to the computer or email program?
    - Was there a requirement that the password be kept secret, frequently changed and/or a prohibition against using the same password?
  - Did the body of the email contain textual or graphical trademarks, signs, tags or labels that are affixed to the message by the company email server?

Email Authentication

- Authentication may involved testimony...
  - Was the identity of a business reflected in the header [metadata] or in the body of the email?
    - E.g., sender email address of al@defendant.com would provide evidence that the email was sent from Al at the defendant corporation. (Self-authentication under Rule 902(7)).
  - Did the customer or entity receive the email?
    - Can the email be connected to the business?

Email Authentication

- Was Public/Private Key Encryption used?
- The Reply Letter Doctrine
  - Reply to email provides some evidence of authentication
  - See, e.g., *United States v. Reilly*, 33 F.3d 1396 (3rd Cir. 1994).
- Expert Testimony and Header [Metadata] Information
  - Traceroute, Message ID, etc.

Email Authentication

- Challenges to Authentication
  - Were there any steps taken to safeguard the information from being falsified?
  - Could the header and other information [metadata] have been altered?
  - How were the contents of the email transmitted and stored during the discovery process? Were they stored on read-only CD's and DVD's?

Email Authentication

- Challenges to Authentication
  - Did a neutral expert retrieve the electronic information?
  - On what type of system was the information stored prior to retrieval?
  - How was the email retrieved?
  - Is there a sufficient chain of custody to eliminate questions of manipulation, alteration, substitution or spoilage?

Chat Room Authentication

- Third party subpoena often required
- When authenticating, focus on:
  - Information from the owner of the chat room or newsgroup regarding signing up or subscription to the site or listgroup. Often, an individual when signing up for access to a chat room will have to disclose his name, address and other personal information.

Chat Room Authentication

- When authenticating, focus on:
  - Information pertaining to the name that the individual used while participating in the chart room, newsgroup or listserv
    - Such as “IluvBz” “TooCwl”, etc.
  - If you are inviting the person to enter a chat room, then evidence showing that a person with the particular screen name entered the room and participated in conversation.
    - Important in child molestation cases
    - Trade secret misappropriation

Chat Room Authentication

- When authenticating, focus on:
  - Evidence pertaining to other indicia such as the person using a particular screen name, real name, street address, email address or other facts connecting the individual participating in the chat room with their identity.
  - If possible, conduct a forensic examination of the computer that the individual purportedly used to engage in the conversations.

Chat Room Authentication

- When authenticating, focus on:
  - Note, the person who has been invited to the chat room, newsgroup or listserv may disclose information that had been provided by the police or business owners.
    - The information may be unique to the police officer or business and may provide some connection to the participant.
  - Evidence on paper or in the computer showing the user ID, password and pseudonym or a screen name for the person.

Web Page Authentication

Web Page Authentication

- Need to determine if site is “static” or “dynamically generated”
- When requesting information about the website, request:
  - The directory, subdirectories and files of the relevant part of the website be provided
  - The raw data and web page generator.
- Consider using the WabBack Machine
  - http://www.archive.org/

Web Page Authentication

- Check for domain ownership particulars
  - http://centralops.net and whois services
- View the source code for the page to look for copyright notices or telltale coding.
- Find a Website Witness
  - Who entered the the URL into a browser
  - Viewed the contents of the website through the navigation tools (hyperlinks, searches)
  - Noted the logos, inscriptions, labels, etc.

Web Page Authentication

- Use a Website Witness
  - Who made a printout or other exhibit of what was viewed on the website.
    - Better if URL/date appears on footer of printout.
  - As him/her if the printed exhibit fairly and accurately reflect what the witness saw?
  - If the witness purchased something from the website, have them testify that they
    - Visited the webite; ordered the goods; and
    - Received the goods (course of conduct)

Web Page Authentication

- Contracts for goods and services may come under “E-SIGN” or “UETA” with corresponding Business-to-Consumer records requirements.
  - Such evidence may be admissible as business records
- Judicial Notice may be available for some sites.
- Request website through ordinary document production

Sanctions

Sanctions

- Rule 37

Sanctions

- Rule 37
- Three types of sanctions

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary
  - Adverse Inference

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary
  - Adverse Inference
  - Dismissal

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary
  - Adverse Inference
  - Dismissal
    - of Claims

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary
  - Adverse Inference
  - Dismissal
    - of Claims
    - of Defenses

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary
  - Adverse Inference
  - Dismissal
    - of Claims
    - of Defenses
- Assignment of costs is possible

Sanctions

- Rule 37
- Three types of sanctions
  - Monetary
  - Adverse Inference
  - Dismissal
    - of Claims
    - of Defenses
- Assignment of costs is possible
  - But not considered a sanction, per se.

Sanctions

- Sanctions can be imposed for:

Sanctions

- Sanctions can be imposed for:
  - Bad faith conduct (client and/or attorney)

Sanctions

- Sanctions can be imposed for:
  - Bad faith conduct (client and/or attorney)
  - Lack of diligence in executing litigation hold

Sanctions

- Sanctions can be imposed for:
  - Bad faith conduct (client and/or attorney)
  - Lack of diligence in executing litigation hold
- Note, criminal sanctions are available for cases involving the government

Sanctions

- Sanctions can be imposed for:
  - Bad faith conduct (client and/or attorney)
  - Lack of diligence in executing litigation hold
- Note, criminal sanctions are available for cases involving the government
  - Obstruction of Justice
    - Sarbanes Oxley
    - Etc.

Sanctions

- Rule 37 (Fed. R. Civ. P.) includes a “safe harbor” provision for parties that act reasonably in discharging preservation obligations

Sanctions

- Rule 37 (Fed. R. Civ. P.) includes a “safe harbor” provision for parties that act reasonably in discharging preservation obligations
  - The Rule tempers the sanctions that may be assessed after certain *routine* loss of ESI

Sanctions

- Rule 37 (Fed. R. Civ. P.) includes a “safe harbor” provision for parties that act reasonably in discharging preservation obligations
  - The Rule tempers the sanctions that may be assessed after certain *routine* loss of ESI
  - No rule-required sanction if parties acted in “good faith” in executing preservation obligations

Sanctions

- Rule 37 (Fed. R. Civ. P.) includes a “safe harbor” provision for parties that act reasonably in discharging preservation obligations
  - The Rule tempers the sanctions that may be assessed after certain *routine* loss of ESI
  - No rule-required sanction if parties acted in “good faith” in executing preservation obligations
  - Exclusion from “safe harbor” requires showing of more than mere negligence

Summary

- ESI is discoverable
- Litigants must preserve/produce ESI
- Lawyers must understand how to request, protect, review, produce, and admit ESI
- Courts have the tools to rectify abusive or obstructive electronic discovery

Questions?