

GTC

*The eDiscovery Tidal Wave is Coming:
Don't Let it Sweep You Away*

**Ira Victor, GIAC G17799 GPCI GSEC
Director, Compliance Practice**



Agenda



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Who is your speaker?
2. The recent changes in eDiscovery
3. The eDiscovery Baker's Dozen
4. Regulations and other mandates
5. Data acquisition
6. Data preservation and analysis
7. Report writing
8. Managing the eDiscovery process
9. Resources for on-going education, data acquisition tools

About Your Speaker



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

- > Information security consultant and auditor to corporations, law firms and government entities
- > Security certifications from the SANS Institute
- > Co-developer of patent-protected email security system
- > Board Member, Sierra Nevada InfraGard, a public private partnership between law enforcement and the private sector to protect critical infrastructure and stop cyber criminals. Represented InfraGard on SB410, NV Computer Forensics Bill
- > Member, Reno Lions. Provide security expertise for “computer for kids” program. Provides Intel PCs to needy children
- > Director of Compliance Practice, Data Clone Labs

Acknowledgement



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

Thank You

Wesley Ayres

Discovery Commissioner

2nd District Court

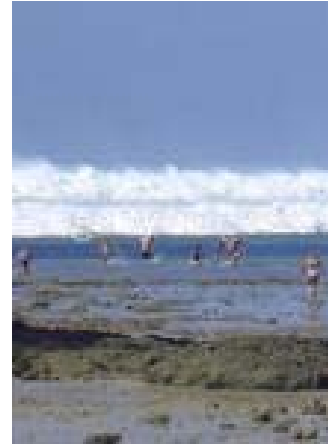
The State of Nevada

December 1, 2006

- Proximity to the anniversary of The Tsunami in December 2004 is an interesting coincidence

- Federal Rules of Civil Procedure (FRCP) amended to take into consideration the discovery of electronically stored information (ESI)

- Change the way electronic information is handled for the purposes of discovery



Tackling eDiscovery



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Legal issues
2. Compliance Evaluation and Consents
3. Technical issues
4. Management challenges in the new eDiscovery era

The eDiscovery Baker's Dozen



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Plan WITH a team that includes lawyers senior management, IT, InfoSec, Human Resources.
2. Use C.I.A.
3. Document every step you take with exacting detail
4. Identify relevant regulations and other mandates
5. Prepare encryption plan and other tactics to handle select data
6. Diagram data flow, identify where information assets are located
7. Identify the information asset hardware
8. Pay special attention to: eMail and Operating Systems
9. Gather Data
10. Watch Lists
11. Keep data loss to an absolute minimum
12. Evaluate all the data you find
13. Summarize your finding in plain English

C.I.A. Central Intelligence Agency



C. I. A. - The Standard for InfoSecurity



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. **Confidentiality**; Assurance that information is shared only with those authorized to have access to it.
2. **Integrity**; Assurance that the information is authentic and complete.
3. **Availability**; Assurance that the delivery, processing and storage of information is accessible when needed, by those who need them.

Identify and document security policies and practices



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

The lack of a CIA-based security policy may result in:

- > The unauthorized disclosure of privileged information
- > The unauthorized deletion of information
- > Difficulty accessing information critical to proving a case

eDiscovery Planning Team



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. The lawyers senior management, IT, InfoSec, Human Resources
2. Review of Government Regulations
3. Review of Contractual Mandates
4. Review of Criminal Laws
5. Your planning needs to “bake in” C. I. A. from the beginning
6. Scope of Search – including nature of information search

Government Regulations: HIPAA



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Health Information Portability and Accountability Act of 1996
2. Our Focus: Individually Identifiable Health Information that might be discovered
3. Enforcement Body: Department of Health and Human Services, Office of Civil Rights
4. Penalties Include: Fines up to \$250,000 and up to 10 yrs in Federal Prison

Government Regulations: Security Breach Disclosure Laws



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Security Breach Information Act of 2003 (California, almost 40 states have similar laws in place)
2. New York State Law: A-4254
3. Safe Harbor for Encrypted Data, Important for eDiscovery!
4. Our Focus: (Varies) Credit Card, SSN, Driver's License, ATM, and Bank Account numbers
5. Enforcement Body: (Varies) Trial Lawyers
6. Penalties Include: (Varies) Linked to the number of records

Government Regulations: FERPA



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Family Educational Rights and Privacy Act of 1974
2. Our Focus: Student education records. Applies to all schools that receive Federal Funding. Includes all records directly related to a student and maintained by an educational institution or someone acting on its behalf (like a contractor).
3. Enforcement Body: United States Department of Education, Family Policy Compliance Office
4. Penalties Include: Cut off of Federal Educational Funding
5. Exception: Obtain a judicial order or subpoena directing release of the information. Student must be given notice of the subpoena prior to releasing information unless the subpoena directs otherwise.

Government Regulations: SOX



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Sarbanes-Oxley Act of 2002
2. Our Focus: SOX Section 404: Internal controls and Information Security. eDiscovery work may need extra documentation in certain circumstances.
3. Enforcement Body: Securities and Exchange Commission, Public Company Accounting Oversight Board
4. Penalties Include: Up to \$25 million in fines and up to 20 years in Federal Prison

Government Regulations: GLBA

1. Gramm-Leach-Bliley Act of 1999
2. Focus: Consumer Financial Data
3. What the organization does determines compliance
4. Enforcement Body: Federal Trade Commission
5. Penalties Include: Fines up to \$1,000,000 per incident

Contractual Mandates: PCI



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Payment Card Industry Digital Security Standard: PCI-DSS
2. Our Focus: Confidentiality of Credit Card Data
3. Accepting Credit Cards determines applicability
4. Enforcement Body: PCI Council and Banks
5. Penalties Include: Fines up to \$500,000 per incident

Criminal Law: CP



Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Possession and Distribution of Child Pornography
2. Our Focus: What to do in the first “Oh My God” moment
3. Possessing CP determines applicability
4. Enforcement Body: Local law enforcement, State Police, The Feds
5. Penalties Include: (Varies) Could bring havoc to a case

Special Handling of Select Data

A. Prepare encryption plan and/or other means to protect select data

1. Third party involvement
2. Storage and escrow of encryption keys
3. Thoroughly document all actions
4. Care attention to logging and audit trails

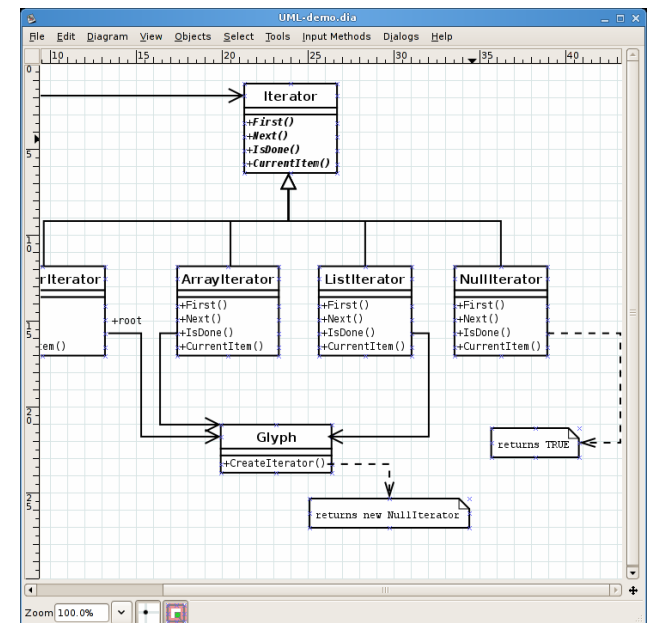
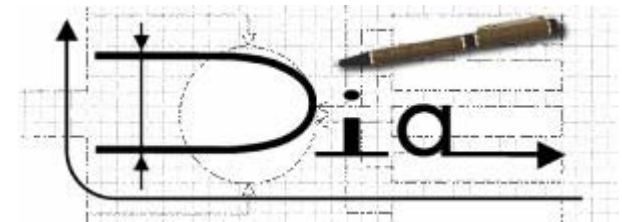
B. Prepare plan if CP or other criminal content

1. Lawyers, officers of the court
2. Special handling instructions

C. Good C. I. A.

Map Data Flows

1. Diagrams the data as it flows through an organization's information assets
2. Include all the assets that the information "touches"
3. In the case of eDiscovery, might include the systems of the other party in a lawsuit, if that information is known.
4. Open Source Tool for making Data Flow Diagrams: Dia
5. BOTH Linux and Windows versions can be downloaded from this address:
live.gnome.org/Dia



Identify The Sources of eData



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

Identify the information asset hardware

- > Servers
- > PCs
- > Laptops
- > PDAs
- > Mobile Phones
- > Smart Phones
- > Thumb Drives
- > Network Equipment
- > Log Systems
- > Any other information asset capable of retaining information

Discovery data may be in a variety of systems and locations

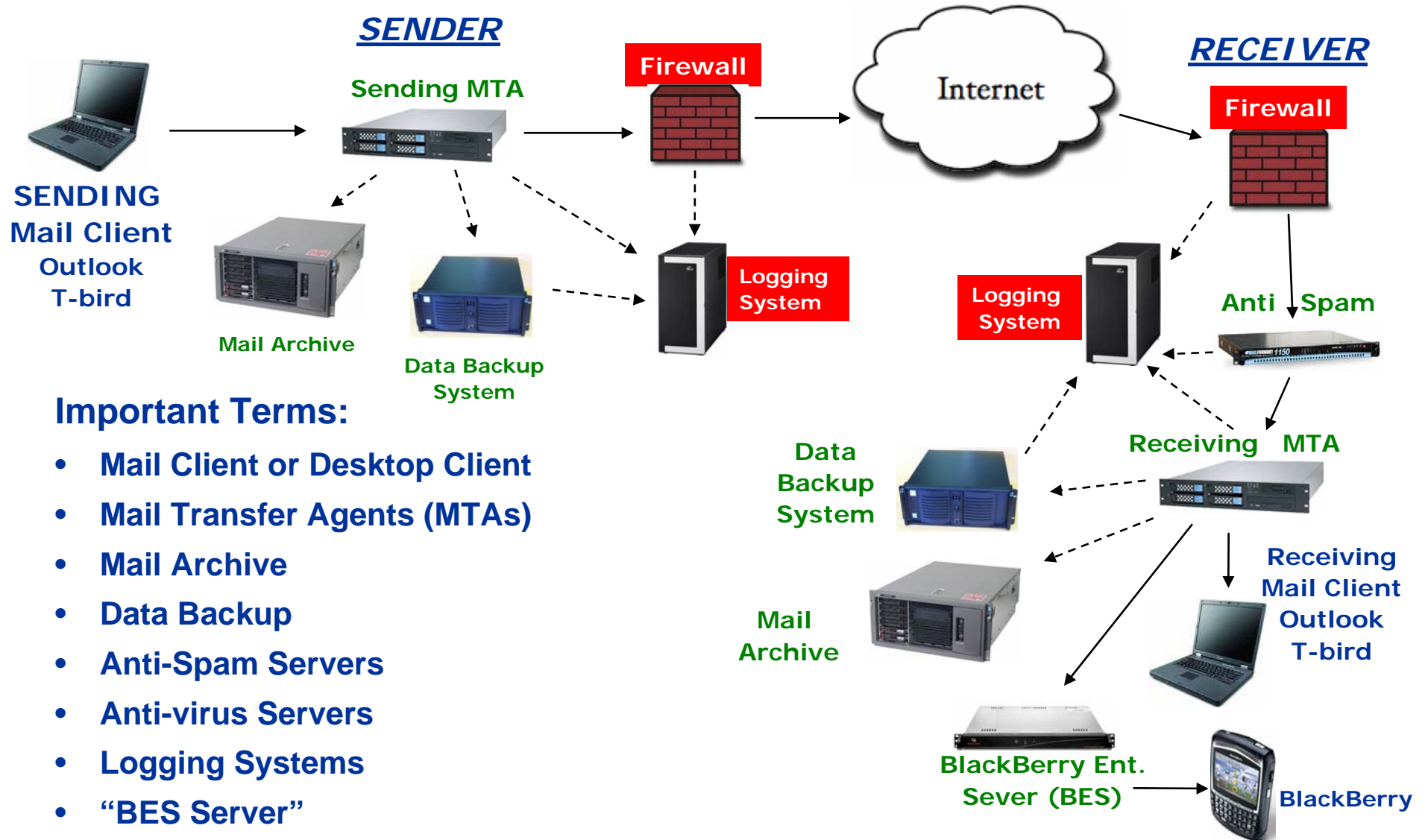


Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

- > Financial Accounting Systems
- > Customer Relationship Management Systems
- > CAD-CAM
- > Shared networks
- > Web page code
- > Software development code
- > Voicemail systems
- > Video teleconferencing systems
- > Anti-spam and anti-virus systems
- > Instant Messages
- > Groupware
- > Calendaring systems
- > Time clock systems
- > Email systems
- > And other Systems not on this list

Special Attention: eMail



Important Terms:

- Mail Client or Desktop Client
- Mail Transfer Agents (MTAs)
- Mail Archive
- Data Backup
- Anti-Spam Servers
- Anti-virus Servers
- Logging Systems
- “BES Server”

ID and Documenti the Various OSs and Versions in the Diagram(s)



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

Must determine the operating systems, versions, role, owner/user, function in order to access the information asset

Examples:

Windows Vista vs. Windows98 vs. Red Hat Linux vs. BSD

IMPORANT:

It may not be economical to access the information on an older system

Different procedures and terminologies for different operating systems

Gathering Data: Most Volatile vs. Least Volatile



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

Most Volatile: Mostly destroyed when the power is turned off:

1. RAM Memory
2. Network connections
3. Running Processes

Least Volatile: Mostly retained even when power is turned off:

4. Hard drives
5. Removable Media: USB drives, firewire, SD cards, Smartphones, CD/DVD, floppies

Gathering of Data (con't)

A. Most Important:

Minimize Data Loss when you gather evidence

Steer clear of adding data when gathering evidence

B. How does one steer clear of adding data?

Acquire forensically sound images; use a software or hardware write blocker

What is a software write blocker? What is a hardware write blocker?

Gathering of Data (con't)

Write Blockers:
Hardware Example



Software Example:



Example: Software Write Blocker, Imager, and Eraser



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

AIR - Automated Image and Restore, by Steve Gibson

GUI front-end to dd/dcfldd designed for easily creating forensic bit images
<http://air-imager.sourceforge.net>

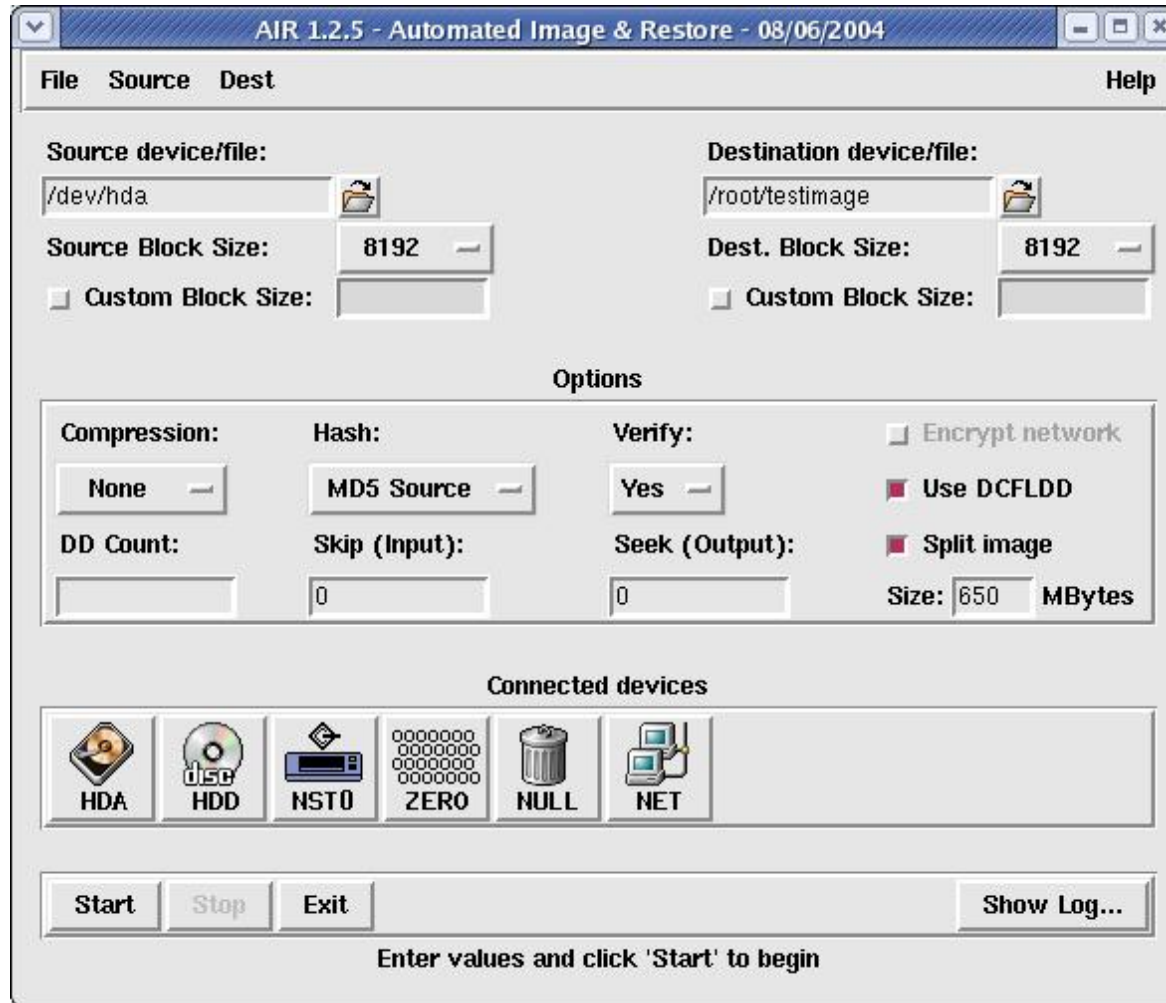
Important AIR Features

1. Auto-detection of IDE and SCSI drives, CD-ROMs, and tape drives
2. Choice of using either dd or dcfldd
3. Image verification between source and copy via MD5 or SHA1
4. Image compression/decompression via gzip/bzip2
5. Image over a TCP/IP network via netcat/cryptcat
6. Wiping (zeroing) drives or partitions
7. Detailed logging with date/times and complete command-line used

Can also just use Linux command line tool and get the same results:
dd or dcfldd

AIR - Automated Image and Restore

<http://air-imager.sourceforge.net>



AIR 1.2.5 - Automated Image & Restore - 08/06/2004

File Source Dest Help

Source device/file: /dev/hda

Destination device/file: /root/testimage

Source Block Size: 8192

Dest. Block Size: 8192

Custom Block Size:

Custom Block Size:

Options

Compression: None

Hash: MD5 Source

Verify: Yes

Encrypt network

Use DCFLDD

DD Count:

Skip (Input): 0

Seek (Output): 0

Split image

Size: 650 MBytes

Connected devices

HDA HDD NST0 ZERO NULL NET

Start Stop Exit Show Log...

Enter values and click 'Start' to begin

Watch Word Lists and Document the Location of the Data



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. What are the key words or phrases that the lawyers would like to find? This must be done at the planning phase
2. What are the types of documents do the lawyers want to see?
3. Where do the lawyers think these documents might reside? You might want to add more places to this list, using your IT knowledge and skills

Preserving eDiscovery Data



Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Make certain there have been no alterations to the original data
2. Make certain you have bit-images of data sources
3. Council should have charge of the originals
4. **IMPORTANT:** Make cryptographic hashes of original evidence and copies
5. MD5 and SHA1 for hashes

MD5 and SHA1 hashes



Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Hashes are one-way mathematical function
2. Hashes are designed to make it impossible to have two different images with identical hashes
3. Integrity part of C. I. A.
4. Flaws have been discovered in the lab, but unlikely to see these results in every day practice. Counter-measure: use two hashing algorithms on the same file

CIA Example: Removable media

The lack of proper software and controls on removable media can also result in:

- > The unauthorized disclosure of privileged information
- > The unauthorized deletion of information
- > Difficulty accessing information critical to proving your case

“Digital Shredding” and CIA



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

NIST Special Publication 800-88 “Guidelines for Media Sanitization”
September, 2006, Page 6

“Advancing technology has created a situation that has altered previously held best practices regarding magnetic disk type storage media. Basically the change in track density and the related changes in the storage medium have created a situation where the acts of clearing and purging the media have converged. That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack.”

Bottom Line: One pass with zeros is considered destroyed

Other Data Classification Terms



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Active Data: What is visible to the naked eye
2. Latent Data: Metadata in a file, and “deleted data”

Metadata: “Data about the data.” Meta data is Information stored by a system or application. Many times it includes the history of a document, the users who have saved and or modified it, the names of printers it was printed on, and other data.

When is deleted data NOT deleted?

3. Archival Data: data backed up to disc or tape.

Also includes purpose-built archive and search systems like email archive and document management systems

Reporting Your eDiscovery Results



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

Proper report writing to accepted standards:

1. Keep DETAILED notes on every task that you do, accuracy is key
2. Be sure your report can be read by another person who can repeat the tests and get the same results
3. Don't make claims you can't prove
4. Write in plain English, and stick to the facts
5. Document the techniques you used to preserve original data
6. Write your report as if you needed to testify – because you may!
7. Tip: Document who you spoke with and what you said. You are allowed to bring notes when you testify, to help your recollection

Managing The Process: ALL THE STAKEHOLDERS



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

1. Senior management
2. Legal – including any paralegals
3. Human Resources
 - May need to include consultants and past employees
 - They have the authority to hire/fire
4. Information Technology Staff
5. Information Security Staff

Managing The Process... (con't)



Ira Victor GIAC GPCI G17799 GSEC

DataCloneLabs.com

- > **IMPORTANT:** Encourage Senior Management to select a legal team member with good diplomatic skills to work with the non-legal people
- > If you can be an IT or InfoSec staffer with good diplomatic skills, your value to the organization will be very high
- > The paralegals are many times over worked and under appreciated, reach out to them when you can, they might be among your best ally

Relevant Links

- www.ediscoverylaw.com
- www.thesadonaconference.org
- www.craigball.com/cf.pdf
- www.discoveryresources.com

GTC

*The eDiscovery Tidal Wave is Coming:
Don't Let it Sweep You Away*

Q&A

ira@dataclonelabs.com

**Ira Victor, GIAC G17799 GPCI GSEC
Director, Compliance Practice**

