ForensicsConsulting Solutions, LLC™

An FCS Smarter, Better, Faster Educational Presentation

Prepared for:

DiscoverFCS – Creating Insightful Discovery

Unlocking the Powers of eDiscovery: Computer Forensics

By: K.J. Kuchta

Date: March 17, 2017

Agenda

- Introduction
- What is Computer Forensics and Why is it important?
- When is a Forensic Exam needed?
- Data Authentication
- Metadata – Anatomy of File
- Slack Space, Risk and Evidence Collection
- Case Law
- Q&A

Why Is Computer Forensics Important?

- Authenticity / Accuracy / Reliability
- Reproducible results
- A verifiable chain of custody
- Unbiased analysis
- Evidentiary Foundation

Why Are Computer Forensics Warranted?

- It will be difficult, if not impossible, to recover critical data after the fact because changes will have occurred in the data leading to questions about its integrity

- *YOU ONLY HAVE A SMALL WINDOW TO CAPTURE A FORENSICS IMAGE BEFORE CHANGES REGISTER: WHEN IN DOUBT…ERR ON THE SIDE OF SAFETY*

Preserve Broad

Process, Review and Produce Narrow!!

When Do I Need Computer Forensics?

- When the issue involves computer-based evidence
- When there are concerns or suspicions of loss of data
- When planning matters of a technical nature
- Investigative activity involving a network intrusion
- Financial, Accounting, IP, Trade Secret and Employment investigations
- Event with potential National Security implications

Involve a forensics professional as early as possible!

What Questions Should You Ask?

- Is it important to understand the specific details about the electronic information for the events in question?
- Does the investigation have any criminal elements?
- What is the business impact of using forensics? i.e. time, cost, loss of IP, etc.

What Does a Legal Professional Need to Know to Manage a Forensics Investigation?

- Computer Forensics Overview
- Who constitutes a qualified Computer Forensics Professional
- Work Plan and methodology review of what will be used for forensic collection and examination
- Define deliverables
- Create hypotheses or questions that the Computer Forensics Professional will be expected to prove or disprove or answer

Identify When and How Computer Forensics Can Be Used

Computer Forensics allows you to obtain and analyze digital evidence in its native environment without corruption or exclusion of information.

- Establish Authenticity and Accuracy of Printed Documents
- Reconstruct a Sequence of Events
- Establish Timeframes of Activities
- Recover Intentionally Deleted Information
- Reconstruct Correspondence
- Assist in Depositions
- Assess Culpability
- Among Many Others …

Forensic Imaging

Objective: Capture electronic data in a way that it can be authenticated without altering the original data.

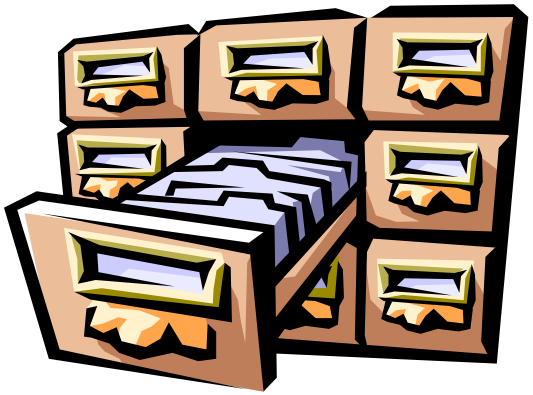
Bit-stream imaging is the process of copying data sector-by-sector exactly as it appears on a magnetic storage device, e.g. on the hard drive. This is also known as "mirror imaging."

Data Authentication

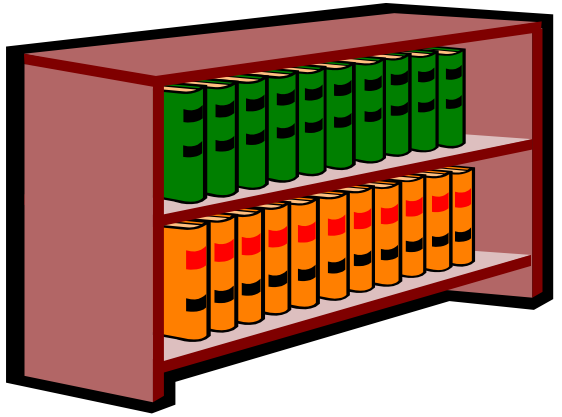
Hashing tools are applications that create a mathematical algorithm or value which has billions of combinations. i.e. MD5, RSA. This becomes the document “fingerprint”

Forensics Professionals create a hash value before the imaging takes place and after imaging is complete. If the values match, the image accurately reflects the original data.

Logical vs. Physical files



Removing the index card does NOT remove the book!



Deleting a File removes the pointer… NOT the File

Hidden and Deleted Files

Files that have lost their pointers

- (books WITHOUT index cards)

Windows' copy feature only captures logical files

- (books WITH index cards)

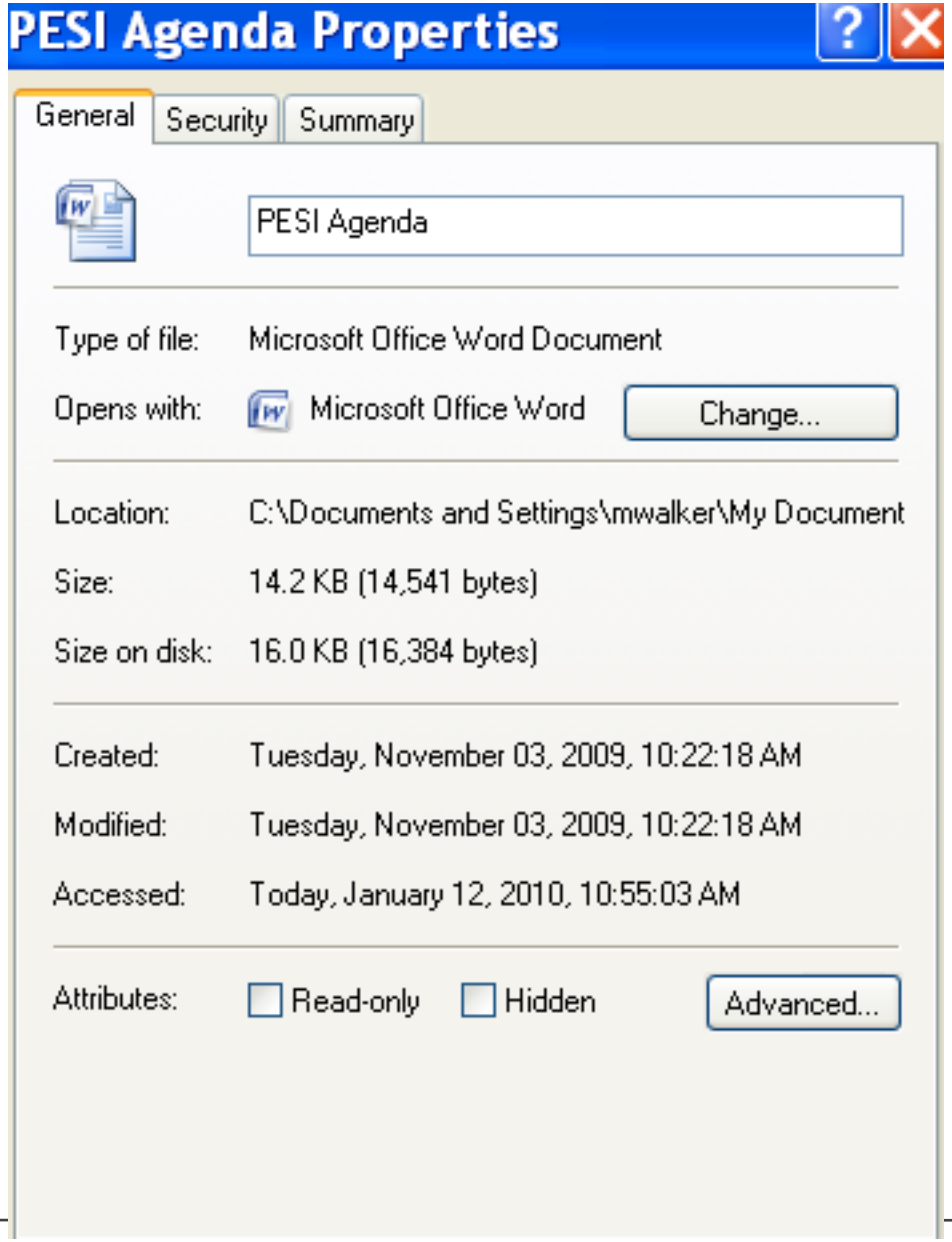
A good librarian can help you find books without index cards!

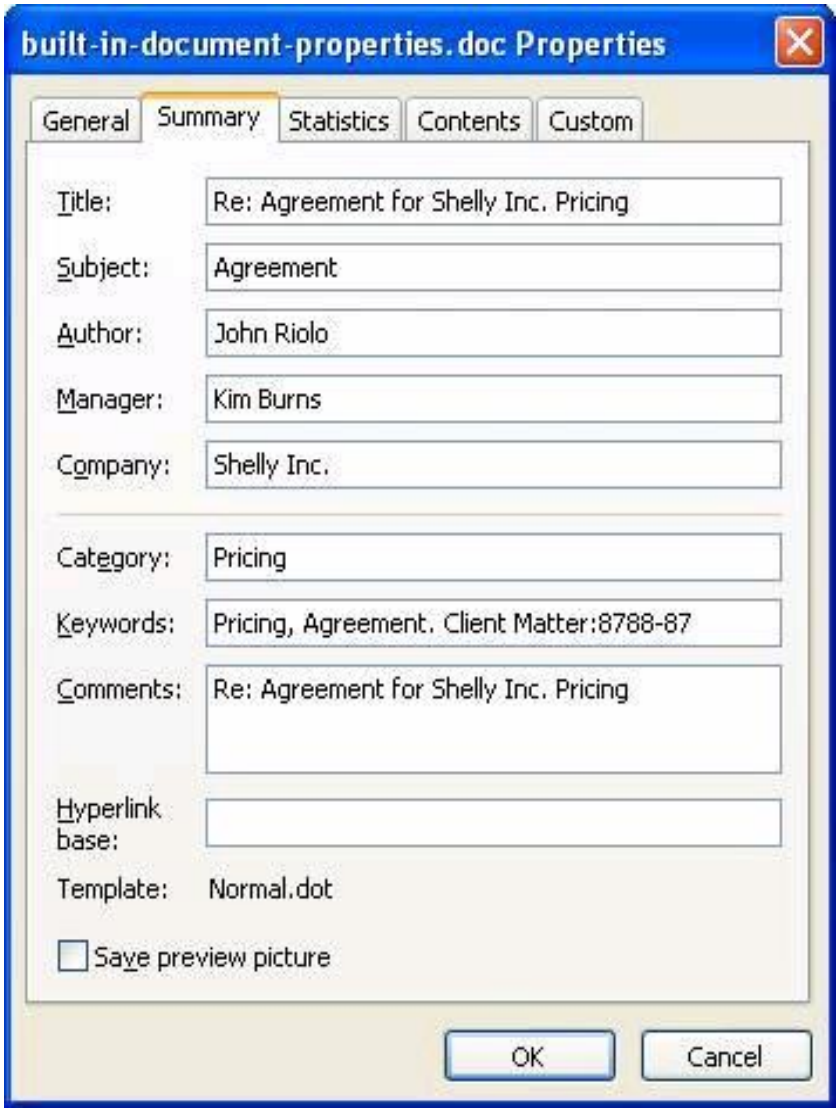
What is Metadata?

Metadata is descriptive data or information *about* data. It's not the content, it's a description of the content and other information about the document. For example, MS Outlook email contains almost 100 different metadata fields.

Metadata Can Include

- Date and time stamps (Creation, Accessed and Modification)
- Author(s) for original document and revisions
- Copied or Printed to (or where) data was saved





Swap & Temporary Files

Swap Files: Created when the computer needs to free some memory by placing a "page" of data temporarily on the hard drive; it can later be copied from the disk back into memory.

Temporary Files: Files that are created by the Windows operating system to save temporary data from copied files or applications. A temporary file may or may not be deleted when the operating system is shutdown.

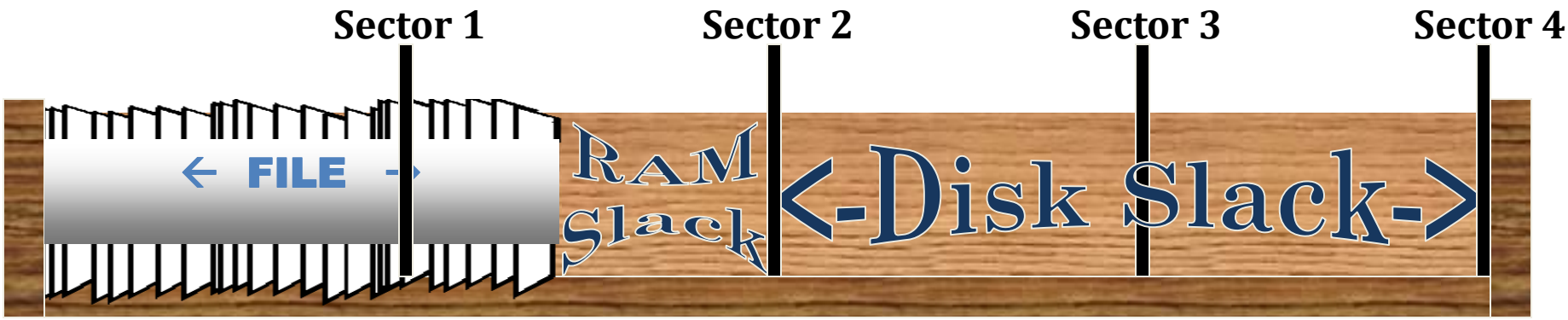
File Slack Types

RAM Slack: the space between the end of file and the end of the sector.

Disk Slack: the space between the end of the last sector of a file and the end of the cluster.

Table File Slack- the space within, as an example, a PST file

Imagine Sectors as book holders dividing each shelf into 4 Sections



What is the Risk of Not Getting a Forensics Image?

- **Boot Process/Start Up:** Modifies tens of thousand of files when the computer is started
- **Best Evidence Rule:** If we work on original evidence, we risk modification of original data
- **Authentication:** Easy answer to questions of authenticity of evidence in court

Evidence Collection

- Sequester evidence quickly
- Consider simply imaging critical drives for later investigation
- In the alternative, consider sequestering a hard drive for a period of time and doing the forensic image later if needed
- Document the collection with unique information
- Maintain the evidence in a secured location
- Maintain chain of custody information

Case Law: Forensic Imaging

Sample Recent Decisions on Forensic Imaging

Weatherford U.S., L.P. v. Innis, No. 4:09-cv-061, 2011 WL 2174045 (D.N.D. June 2, 2011) (Court grants a Motion to Compel forensic imaging of defendant's computers.)

- Defendant acknowledged copying trade secret information to a jump drive from previous employer but denied accessing the data after copying it. Plaintiff's expert found that to be untrue. Court agreed to plaintiff's forensic expert imaging all of defendant's computers and giving defense counsel first pass for privilege exclusion of data.

Adhi v. Twp. of W. Pikeland, 2010 WL 1047894 (E.D. Pa. Mar. 16, 2010) (Court orders forensic examination of plaintiff's computers due to an inability to deny that pertinent emails may have existed at one point.)

- Defendant moved to compel production of ESI from plaintiff after only 4 emails produced as responsive. Plaintiff indicated that even if responsive emails had existed, they were deleted in the ordinary course of business. Defendants argued that the "mere deletion of an email doesn't make it lost forever". Court agreed and allowed defendant's forensic expert to inspect plaintiff's computers/servers at defense expense.

Social Media Concerns

- Prompt action to prevent loss of potentially relevant information
- Key custodians and potential witnesses in litigation matters:
  - Use of social media sites
  - Discussion of work matters in personal email
  - Internet screen names, email addresses, and passwords

Social Media Concerns

Information a party should seek regarding social media data includes but is not limited to:

- Identification of any Social Media Sites
- Account user names
- Blog posting and associated user names
- Any web-based sites opposing party stores data
- Social media archival
- Screen shots of any postings that evidence, refer or relate to the allegations in the complaint
- Printouts of any pictures stored on Social Media Sites, or other shared location which evidence, refer or relate to the allegations in the complaint

Case Law: Social Media

EEOC v. Simply Storage Mgmt., LLC

- Court compelled production of relevant content from social media sites.
- Court stated discovery of social media site data simply "requir[ing] the application of basic discovery principles in a novel context."
- Court found that any privacy concern therein was lessened due to the fact the information had already been shared.

Romano v. Steelcase Inc.

- Discovery of current and deleted postings.
- Private postings not accepted.
- Contradictory information on public sections gives rise to reasonable belief of relevant information on private sections.
- Facebook and MySpace policies: "no expectation of privacy."

CSI ….. Cases Have Turned on Forensics Investigations

HIPAA Fraud Uncovered

A complaint was received alleging the use of "up coding" by a medical facility for routine tests.

A review of insurance Explanation of Benefits (EOB) and witness interviews led to a search warrant of the medical facility and the computer system.

The forensic analysis of the computer identified a series of deleted files. Further analysis revealed that the files contained code designed to alter billing codes for a duration of 6 weeks. At the conclusion of each six week period a new file was loaded and a different billing code was "up coded."

Armed with this new information the investigator was able to conduct additional interviews. During these interviews the system administrator revealed that about every six weeks a disk arrived from corporate. His instructions were to load the data from the disk. He thought it was a routine system upgrade.

Embezzlement Uncovered

A request was received to determine if any accounting records could be identified.

A signature analysis of all files was completed. The signature analysis revealed that one of the computer systems database files had a mismatched signature. An analysis identified that the file was an executable file that started the install process for an accounting system. From this the examiner was able to identify the accounting program. A clean install of the accounting program and subsequent install of the database files revealed the accounting records. The records were them provided to a forensic accountant for further analysis.

Intellectual Property Patent Protected

Major corporation developed a patented transponder technology. Investor left the corporation and started a competing company and began recruiting out engineers from corporation and began producing the same patented technology.

- Upon conducting a forensic examination of the corporate email system, FCS demonstrated the engineering "KEYS" for the patented technology were emailed to Chief Engineer's personal email account who had been recruited out. This was an important factor which the Judge used to grant a TRO and Site Inspection of the competing investor's new company, giving the Engineer notice of the Inspection the prior day.
- Upon collecting the data from the competing company, FCS was able to put together the evidence trail which showed the Chief Engineer changed his system clock on his computer, saved the engineering files on the patented technology, manually corrupted the file and deleted the logical references to the information. This action hid the file from the normal user and then set the system clock back to the correct time.
- Result: FCS was able to demonstrate deception and substantiate possession of the Patented Technology. Major corporation prevailed in achieving its legal remedy.

Summary

- What is Computer Forensics and Why is it important?
- When is a Forensic Exam needed?
- Data Authentication
- Metadata – Anatomy of File
- Slack Space, Risk and Evidence Collection
- Case Law
- Q&A

Questions?

Thank you for your time today!

For More information contact:

Kelly “K.J.” Kuchta
Forensics Consulting Solutions, LLC.
2600 N. Central Ave. #700
Phoenix, AZ 85004
kkuchta@discoverfcs.com
602-354-2799
www.discoverfcs.com