Computer Forensics
and Investigations

Dean R. Beal
CISA, CFE
What is Fraud?

- Any illegal act characterized by deceit, concealment or violation of trust.
- These acts are not dependent upon the threat of violence or physical force.
- Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.”

*Fraud Prevention and Detection in an Automated World, GTAG Global Technology Audit Guide (IIA, The Institute of Internal Auditors, 2009), 1.*
Impact of Fraud

U.S. organizations lose 7% of their annual revenues to fraudulent activity.

If this percentage were applied to the estimated 2010 U.S. gross domestic product of $14.307 trillion, we could project that more than 1 trillion would be lost to fraud in 2010.

Why Do People Commit Fraud?

Opportunity
- Because they can

Pressure
- Financial or occupational

Rationalization
- There is nothing wrong with it

Why Do People Commit Fraud?

- Interviews with persons who committed fraud have shown that most people do not originally set out to commit fraud.
- Often they simply took advantage of an opportunity; many times the first fraudulent act was an accident – perhaps they mistakenly processed the same invoice twice.
- But when they realized that it wasn’t noticed, the fraudulent acts became deliberate and more frequent.

Dave Coderre, author of ‘The Fraud Toolkit; ‘Fraud Detection: Using Data Analysis Techniques to Detect Fraud’ and ‘CAATTs and Other BEASTs for Auditors’
10 - 80 - 10 Law

- 10% of people will never commit fraud.
- 80% of people will commit fraud under the right circumstances.
- 10% actively seek out opportunities for fraud.

Dave Coderre, author of ‘The Fraud Toolkit; Fraud Detection: Using Data Analysis Techniques to Detect Fraud’ and ‘CAATTs and Other BEASTs for Auditors’
Goals of a Fraud Program

- Prevention
- Detection
- Deterrence
2120.A2 - The internal audit activity must evaluate the potential for the occurrence of fraud and the manner in which the organization manages fraud risk.
1210.A2 - Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

IT Related Fraud Risks

- Theft of Hardware
- Identity Theft
- Pirated Software
- Unlicensed Software
- Insider Trading
- Corporate Espionage
- Conflicts of Interest
  - Bid Rigging
  - Kickbacks
- Copyright Violations
Red Flags During IT Risk Assessment

- No Controls
- Control Weaknesses
- Not Part of SOX
- Never Audited
- Significant Changes in Technology Since Last Audit
- High Criticality Rating of Data
Red Flags During IT Audit Interviews

- Personal Problems
- Financial Problems
- Job Dissatisfaction
- Personal Relationships with External Vendors
- Complete Control
- Nobody Else to Fill In
- No Vacation
- Living Large
Red Flags During IT Audit Fieldwork

- Look Beyond Audit Checklists
- Look Beyond COBIT Guidelines
  - Denied Access to Staff
  - Denied Access to Data
  - Elevated Access Permissions
  - No Audit Logging/Monitoring
  - Logging/Monitoring without Reviewing
  - SOD
  - Overrides
  - Little or No Management Oversight
  - Excessive Trust
  - No Documentation
How Can IT Auditors Help?

Has a Fraud Occurred Here? How Did They Do It?

Can a Fraud Occur Here? How Would They Do It?

Would Anyone Know?
How Can IT Auditors Help?

Take Away Opportunities to Commit Fraud

Prevent
Detection

- Tips
- Hotline Calls
- Risk Assessments
- Audits
- Continuous Auditing/Monitoring
Detection

Reality = Reactive

Goal = Proactive
Assessing the Allegation

- Management Receives
- Management Reviews
- Management Assigns

Guidelines
- Should exist within department for outlining steps taken for performing a forensics investigation
Planning and Starting the Investigation

- Objectivity Concerns
- Timing Issues
- Game Planning
- Keywords
- Off Site/On Site
- Equipment Needs
- Interviews
The main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

Electronic Evidence

- In the mid 1990’s, most people believed that electronic evidence was of little or no value and was inherently unreliable.

- Since that time, however, it is more than likely than not to make the case. It may be the only evidence.

*The Computer & Internet Fraud Manual* (USA: Association of Certified Fraud Examiners, 2005), 140.
Locard’s Exchange Principle

- Dr. Edmund Locard’s work in the area of forensic science and crime scene reconstruction.
- When two objects come into contact, material is exchanged or transferred between them.

Harlan Carvey, *WINDOWS FORENSICS ANALYSIS* (Burlington, MA: Syngress, 2009), 4,5.
Locard’s Exchange Principle

- If you watch the popular CSI crime show on TV, you’ll hear one of the crime scene investigators refer to “possible transfer.”

- This usually occurs after a scene in which a car hits something or when an investigator examines a body and locates material that seems out of place.

Harlan Carvey, *WINDOWS FORENSICS ANALYSIS* (Burlington, MA: Syngress, 2009), 4,5.
Locard’s Exchange Principle

- The same principle applies to the digital realm.
  - Two computers communicate over a network. Information from each will appear in process memory or log files on the other.
  - Removable storage device is attached to a computer. Information about the device will remain resident on the computer.

*Harlan Carvey, WINDOWS FORENSICS ANALYSIS* (Burlington, MA: Syngress, 2009), 4,5.
Locard’s Exchange Principle

- When we interact with a live system, whether as the user or as the investigator, changes will occur on that system.

- Changes will occur simply due to the passage of time, as processes work, as data is saved and deleted, as network connections time out or are created, and so on.

Harlan Carvey, *WINDOWS FORENSICS ANALYSIS* (Burlington, MA: Syngress, 2009), 4-5.
Types of Data Collected in Computer Forensics

- **Volatile data** is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off.

- **Persistent data** is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off.

Tools

- Forensics Tool Kit (FTK)
- EnCase
- ProDiscover
- Data Wiping Tools
- Data Storage
- PC Tool Kit
A bit stream image is an exact duplicate of a computer’s hard drive in which the drive is copied from one drive to another, bit by bit.

Bit Stream Image

- "Bit" Means at the Binary Level
  01000001 = A
  01100001 = a

- Everything is Copied
  - Deleted Files
  - Fragments of Files
Backup Copy

- **Backup software can only copy or compress files that are stored in a folder or share a known file type.**

- **Backup software cannot copy deleted files or e-mail messages or recover file fragments.**

Acquiring the Forensics Image

Network
“Snapshot”

Physical
“Static”
CIA Triad

- Confidentiality
- Integrity
- Availability

Can connect to any computer on the network.
- By IP address
- By computer name

Install remote agent executable.

Captures image of hard drive over the network.

Runs in the background as a Service.

User does not know they are being imaged.
Write Blockers

Write Blockers

Suspect Hard Drive → Hardware Write Blocker → Forensics PC → Forensics Hard Drive

Reads

Writes

IDE/SATA

FireWire or USB

USB
Forensic Toolkit® (FTK™) version 1.81.5

Release Date: October 7, 2009
AccessData FTK

Thank you for evaluating AccessData's Forensic Toolkit® (FTK®). This is a demonstration version of FTK. The following limitation is in effect:

- A maximum of 5000 file items can be analyzed

If you wish to purchase a full version of FTK, please contact AccessData at 800-574-5199 or 801-377-5410 or visit our website at http://www.accessdata.com.
FTK Case Log

Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

- Case and evidence events
- Error messages
- Bookmarking events
- Searching events
- Data carving / Internet searches
- Other events

Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.

Events related to any error conditions encountered during the case.

Events related to the addition and modification of bookmarks.

Events related to searching. All search queries and resulting hit counts will be recorded.

Events related to special data carving or internet keyword searches that are performed during the case.

Other events not related to the above, such as copying, viewing, and ignoring files.
FTK Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

- **MD5 Hash**: An MD5 hash is a 16-byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
- **SHA1 Hash**: A SHA1 hash is a 20-byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
- **KFF Lookup**: KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
- **Entropy Test**: For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
- **Full Text Index**: The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
- **Store Thumbnails**: Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
- **Decrypt EFS Files**: Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
- **File Listing Database**: Create a Microsoft Access (.Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
- **HTML File Listing**: Create an HTML version of the File Listing.
- **Data Carve**: Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
- **Registry Reports**: Generate common registry reports during preprocessing.
Data Carving

Select the file types to carve:
- BMP Files
- GIF Files
- JPEG Files
- PNG Files
- Enhanced Windows Meta Files (EMF)
- PDF Files
- HTML Files
- OLE Archive Files (Office Documents)
- AOL/AIM Buddy Lists

Automatically Add Carved Items to Case

Carved Image Exclusion Options:
- Minimum Size (in Pixels): Width 130, Height 130
- Minimum File Size 12 KB

Pixel Help, Cancel, OK
Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add
- File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- KEF ignorable files (files found by KEF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- Extract files from KEF ignorable containers

Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria
- Deletion Status:
  - Deleted
  - Not deleted
  - Either
- Encryption Status:
  - Encrypted
  - Not encrypted
  - Either
- Email Status:
  - From email
  - Not from email
  - Either
- Include Duplicate Files
- OLE Streams

File Type Criteria
- Documents
- Spreadsheets
- Databases
- Executables
- Archives
- Folders
- Graphics
- Other Known
- Multimedia
- Email msgs
- Unknown
FTK Refine Index

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don’t get indexed initially can be indexed later by clicking on “Analysis Tools” under the “Tools” menu item.

Unconditionally Index
- File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- KFF ignorable files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria
- Deletion Status:
  - Deleted
  - Not deleted
  - Either
- Encryption Status:
  - Encrypted
  - Not encrypted
  - Either
- Email Status:
  - From email
  - Not from email
  - Either
- Include Duplicate Files
- OLE Streams

File Type Criteria
- Documents
- Spreadsheets
- Archives
- Databases
- Folders
- Graphics
- Multimedia
- Email msgs
- Executables
- Other Known
- Unknown

< Back Next > Cancel
FTK Add Evidence

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:
- Acquired image of drive: Several formats supported: can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Display Name | Source | Name/Number | Type | Refined | Time Zone | Comment
---|---|---|---|---|---|---

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...
FTK Add Evidence
FTK Add Evidence

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported: can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced.

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Source</th>
<th>Name/Name</th>
<th>Type</th>
<th>Refined</th>
<th>Time Zone</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ashley</td>
<td>C:\Documents...</td>
<td>Ashley</td>
<td>Contents of...</td>
<td>N</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:
C:\Documents and Settings\Dad\Desktop\FTK Demo

Number of Evidence Items: 1

Processes to be Performed:
- File Extraction: Yes
- File Identification: Yes
- MD5 Hash: Yes
- SHA1 Hash: Yes
- KFF Lookup: Yes
- Entropy Test: Yes
- Full Text Index: Yes
- Store Thumbnails: Yes
- Decrypt EFS Files: Yes
- File Listing Database: Yes
- File Listing HTML: Yes
- Data Carving: Yes
- Registry Reports: Yes

Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.

Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.

Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence
FTK Processing

Processing Files...

Current Evidence Item:
C:\Documents and Settings\Ashley

Current File Item:
C:\Documents and Settings\Ashley\Application Data\Microsoft\...\08E382DC40DC2B571439BB7A5449C239

Current File Item Status
Action: Filtering Text
File Type: Unknown File Type
Item Size: 727,284
Progress: 655,205

Total Process Status
Elapsed Time: 0:00:00:14
Total Items Examined: 28
Total Items Added: 28
Total Items Indexed: 26

Log the case/system status every 10 minutes

Log extended information

Cancel
An unknown author once wrote:

The human spirit needs places where nature has not been rearranged by the hand of man.

During the years before 1872, this very thought was what crossed United States citizens minds as to whether or not a certain tract of land between Montana and Wyoming territories should be created into a national park. As time continued, and as more politicians, geologists, and other individuals involved themselves with the question at hand, the push for an answer was moving along rather quickly. Evidence of the area, which would be called Yellowstone National Park, soon proved to be suitable land for a treasure that the whole nation could share. The creation of the first U.S. National Park (Yellowstone) was a significant event in American history because it protected the natural wonders of the immediate era, because it gave tourists an interesting place and experience to discover, and because it caused other parks and acts to be created in the future. Before the act that established Yellowstone National Park was ever created, there were many events that had led up its beginnings. The first of these was the Louisiana Purchase. After this occurred, much of the land remained unexplored and undeveloped. Native American tribes such as the Blackfoot, Crow, and Shoshone still roamed the area freely. As French trappers entered the territory, they began naming it after...
FTK E-Mail
FTK Bookmark
Processing the Forensics Image

- Data Carving
- File Types
- KFF
- Key Words
- Bookmarks
- Graphics
- Deleted Files
- Metadata
Processing the Forensics Image

- Password Protected Files
- Encrypted Files
- File Slack
- Windows Registry
- index.dat
index.dat
Regular Expressions

Allows forensics analysts to search through large quantities of text information for patterns of data such as the following:

- Social Security Numbers
- Telephone Numbers
- Computer IP Addresses
- Credit Card Numbers

Regular Expressions

- Perl
- Regex++

\<\d\d\d\[\-\ ]\d\d\[\-\ ]\d\d\d\d\d\d\> Social Security Numbers

\<\d\d\d\d(\-| )\d\d\d\d(\-| )\d\d\d\d(\-| )\d\d\d\d\d\> Credit Card Numbers
dtSearch Search Requests

- A natural language search is any sequence of text, such as a sentence or a question.

- dtSearch sorts retrieved documents based on their relevance to your search request.

dtSearch Search Requests

- FTK
- Sherpa Software

- Boolean Searches
  - or
  - and
  - not
  - *
  - ?
  - %
  - &
Compiling Electronic Evidence

- **Secured Area**
- **Can be Time Consuming**
  - Target and Forensic Hard Drive Capacities
Rules of Electronic Evidence

Records stored in computers can be divided into three categories: non-hearsay, hearsay, and records that include both hearsay and non-hearsay.

Non-hearsay records are created by a process that does not involve a human assertion. Conduct is a command to a system, not an *assertion*, and thus is not hearsay.

http://www.cybercrime.gov/ssmanual/05ssma.html#A
Rules of Electronic Evidence

Hearsay records contain assertions by people, such as: a personal letter; a memo; bookkeeping records; and records of business transactions inputted by persons.

Rules of Electronic Evidence

Mixed hearsay and non-hearsay records are a combination of the first two categories, such as: email containing both content and header information; a file containing both written text and file creation, last written, and last access dates; chat room logs that identify the participants and note the time and date of "chat".

Rules of Electronic Evidence

Authentication

- Before a party moves for admission of an electronic record or any other evidence, the proponent must show that it is authentic. That is, the proponent must offer evidence "sufficient to support a finding that the matter in question is what its proponent claims."

Rules of Electronic Evidence

Authorship

- Although handwritten records may be penned in a distinctive handwriting style, computer-stored records do not necessarily identify their author. This is a particular problem with Internet communications, which can offer their authors an unusual degree of anonymity.

http://www.cybercrime.gov/ssmanual/05ssma.html#A
Rules of Electronic Evidence

The Best Evidence Rule

- The best evidence rule states that to prove the content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required.

Rules of Electronic Evidence

- Federal Rule of Evidence 901(b)(4) is helpful to prosecutors who seek to introduce electronic records obtained from seized storage media.


http://www.cybercrime.gov/ssmanual/05ssma.html#A
A prosecutor introducing a hard drive seized from a defendant's home and data from that hard drive may employ a two-step process.

- First, the prosecutor may introduce the hard drive based on chain of custody testimony or its unique characteristics (e.g., the hard drive serial number).


http://www.cybercrime.gov/ssmanual/05ssma.html#A
A chain of custody is the accurate documentation of the movement and possession of a piece of evidence, from the time it is taken into custody until it is delivered to the court.

This documentation helps prevent allegations of tampering.

It also proves that the evidence was stored in a legally accepted location, and it documents who is in custody and control of the evidence during the forensic testing phase.

Chain of Custody Form

Physical Evidence

- Case Number
- Investigating Organization
- Investigator
- Nature of Case
- Location Where Evidence was Obtained
- Evidence Recovered By
- Date and Time
- Description of Evidence
- Vendor Name
- Model Number
- Serial Number
- Location Where Evidence is Currently Stored
- Evidence Processed by Item Number
- Disposition of Evidence/Date/Time
- Signatures

Chain of Custody Form

Image Evidence

- Case Number
- Investigating Organization
- Investigator
- Nature of Case
- Image Type
- Image Method
- Date and Time
- Description of Evidence
- MD5 Hash Totals
- Location Where Evidence is Currently Stored
- Disposition of Evidence/Date/Time
- Signatures
Rules of Electronic Evidence

• Second, prosecutors may consider using the "hash value" or similar forensic identifier assigned to the data on the drive to authenticate a copy of that data as a forensically sound copy of the previously admitted hard drive.

• Similarly, prosecutors may authenticate a computer record using its "metadata" (information "describing the history, tracking, or management of the electronic document").


http://www.cybercrime.gov/ssmanual/05ssma.html#A
Hash Values

- Hashes use cryptographic algorithms to create a message digest of the data and represent it as a relatively small piece of data.
- The hash can be used to compare a hash of the original data to the forensic copy.
- When the hashes match, it is accepted as proof that the data is an exact copy.

Hash Values

Original MD5 Hash Value:
6f8e3290e1d4c2043b26552a40e5e038

Imaged MD5 Hash Value:
6f8e3290e1d4c2043b26552a40e5e038
:Verified

MD5 Hashes
- Image Level
- File Level
Other Electronic Evidence

- **Scope Creep**
  - New Evidence Discovered

- **Personal or Private Property**

- **Internet/Social Networking**
  - Google Hacking
Other Concerns

- Evidence Locker
- Hard Drive Storage
- Retention
- Destruction
**Wiping**

Wiping a disk will permanently erase all the data stored on it. MediaWiper will format the drive after wiping it, making it ready for re-use.

**Verify Media**
MediaWiper can verify that a disk is clean by checking to ensure that it does not contain any file information.

**View Media Sectors**
You can select to view and inspect individual sectors on a disk to see the data they contain.
Email

- Warning Banners
- Real Time
- Back-ups
- Can See It All
Acquiring Data

- Know Corporate Applications and Systems
- Make Friends with IT
  - Loss of Confidentiality
- Gain Direct Access Corporate Source Data
  - Less Hands in the Cookie Jar
- Write Queries
- CIA
Data Analytics

- ACL
- TOAD
- FOCUS
- QMF
- Adabas
- Cognos
- Microsoft Access
- SQL Server

Data Analytics

- Fixed Length
- Variable Length
- Delimited
- Multiple Record
- HL7
- EDI
- PDF
- DBF

Closing the Investigation

- Criminal Violations
- Corporate Risk and Liability
- Policy Violations
Closing the Investigation

- Report Preparation
- Support the Allegation
- Refute the Allegation
- Consult with Law
- Consult with Management
- Consult with Senior Executives
Conclusion

- Corporate Policies and Procedures
- International
  - EU Safe Harbor
- Federal
  - HIPAA
  - FCPA (Foreign Corrupt Practices Act)
  - FTC
- State
  - Security Breaches
- Other
  - BSA (Business Software Alliance)
  - PCI
  - RIAA (Recording Industry Association of America)
  - SIAA (Software & Information Industry Association)
Conclusion

- Remain fair and objective
- Present the facts as discovered
- Document everything you do
- Get access to corporate source data
- Reactive is good, proactive is better
Data Hiding

A sector is the smallest physical storage unit on the disk.

A cluster can consist of one or more consecutive sectors. Cluster size can be changed to optimize file storage. A larger cluster size reduces the potential for fragmentation, but increases the likelihood that clusters will have unused space.

http://www.ntfs.com/hard-disk-basics.htm#Hard
Data Hiding

http://explorerplusplus.com/blog/54-file-slack
The Slacker tool is the first “tool that allows you to hide files within the slack space of the NTFS file system.”

Hey here's that picture I promised. I fixed it so nobody else can see it!
Data Hiding
Data Hiding
Data Hiding

Hey here’s that confidential information I promised. It’s in the bottle!
Data Hiding

Enter secret message

Here are the company trade secrets I promised!
Data Hiding

Message in a Bottle #1

Message in a Bottle #2

Which One Contains the Company Trade Secrets?
Data Hiding

[Image of two software interfaces showing hash calculation features with different hash algorithms selected and their corresponding hash values displayed.]
The Steganography SearchPak was created from hash values extracted from the latest version of the Steganography Application Fingerprint Database (SAFDB) created and maintained in Backbone’s Steganography Analysis and Research Center (SARC). SAFDB is the world’s largest commercially available hash set exclusive to steganography applications. Digital forensic examiners around the world are using hash values from SAFDB to detect the presence of steganography applications on seized media. Detecting the presence of steganography applications is a strong indication the application may have been used to conceal digital evidence. When files associated with steganography applications are detected, users have the option of contacting Backbone for further assistance with finding and extracting the hidden evidence using advanced steganalysis tools developed in the SARC.

What’s Ahead

The Cloud

December 15, 2009

- Our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the “cloud,” on servers owned by internet service providers.

What’s Ahead

- The challenge of traditional forensics and larger hard drives is that the acquisition typically takes hours -- sometimes days -- depending on the size and number of drives. After authentication, forensic investigators then have to dig through the massive amount of data, which can take a significantly long time. If you've ever done full-text indexing of a large drive, then you know it's not a quick process.

- Now's the time to start preparing because tomorrow might be the day you get the call about a case involving a dozen computers in which each one contains one to four 1.5 terabyte hard drives and a server containing about 10 terabytes of data.

What’s Ahead

The Crime Scene Evidence You’re Ignoring

October 2009

- New storage and entertainment devices are constantly released to the mass market. Files can be stored on anything that a computer sees as a "drive." It may be tempting to leave a digital camera at a crime scene because the investigator sees nothing on the screen.

- The point then is not to think about which devices to seize, or even which kinds of evidence (video, e-mail, documents, etc.) to look for. The key word is "anything:" any kind of device, any kind of evidence.

http://www.officer.com/print/Law-Enforcement-Technology/The-crime-scene-evidence-youre-ignoring/1$48858