



## Computer Forensic Capabilities



Cybercrime Lab  
Computer Crime and  
Intellectual Property Section  
United States Department of Justice



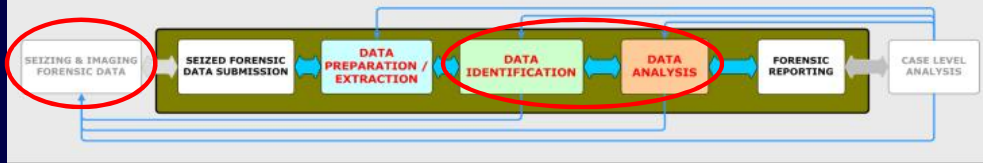
## Agenda

- What is computer forensics?
- Where to find computer evidence
- Forensic imaging
- Forensic analysis: hypothetical case
- Other training tools



## Forensic Analysis: Where Are We Now?

### PROCESS OVERVIEW



## Where to Find Computer Evidence

- Seize items specified in the search warrant.
  - Computers, laptops, Network Equipment (hubs and switches)
  - Peripherals: CDR's, DVD-R's, Digital cameras, PDA's
  - External Media: CD's, floppy disks, USB thumb drives
  - Paper notes, documentation and manuals, post-it notes.
- Document computer equipment and peripherals prior to removal.
  - Digital pictures, diagrams



## Types of Electronic Media

- Desktops to Servers



## Variety of Media



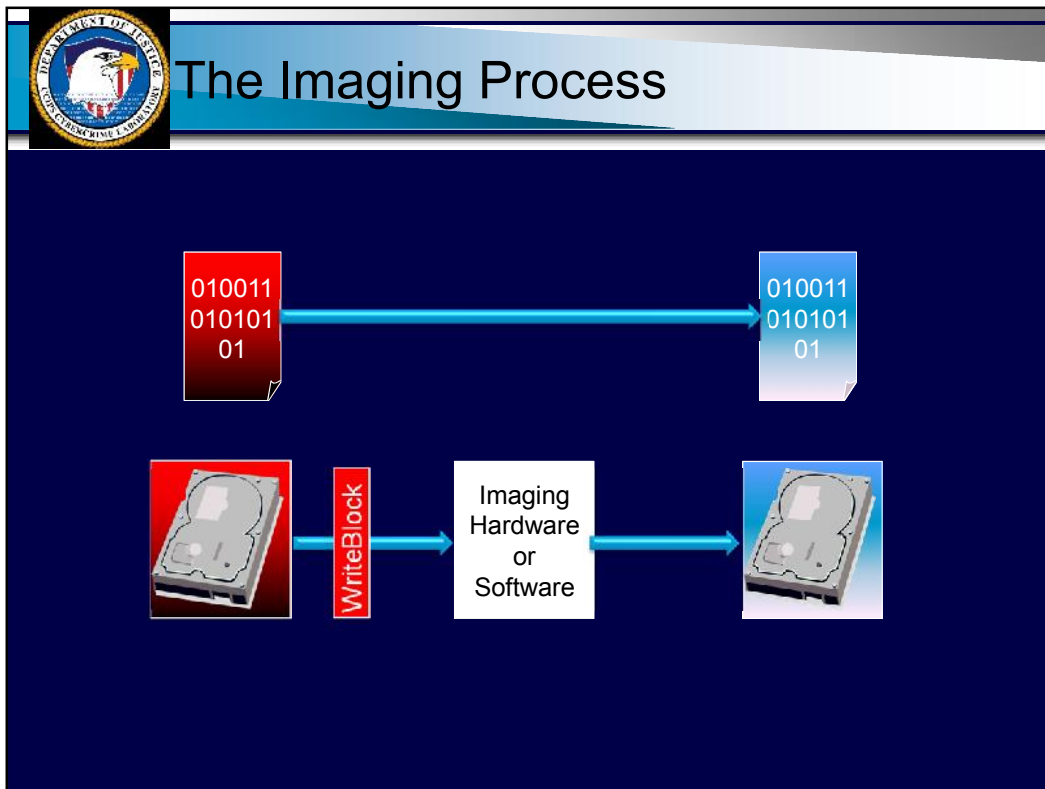


## But Wait, There's More



## What is Forensic Imaging?

- Obtained by a method which does not, in any way, alter any data on the drive being duplicated
- Duplicate must contain a copy of every bit, byte and sector of the source drive
- Duplicate will not contain any data except filler characters (for bad areas of the media) other than that which was copied from the source media.
- Accurate, Verifiable, Reproducible



The diagram features the Department of Justice seal on the left and the title "Value of Forensic Imaging" in a blue banner. Below the banner is a list of bullet points on a dark blue background.

- Incident Response/Forensic Imaging is the **MOST IMPORTANT** step in the entire electronic investigation
- Failure can invalidate or make inadmissible all further information gathered from the digital evidence
  - Or at least give attorneys a headache



## Physical Write Blocks

- What Are They?
  - Physical device that prevents writes to the evidence drive
  - BEST method of imaging



## Attaching Write Block

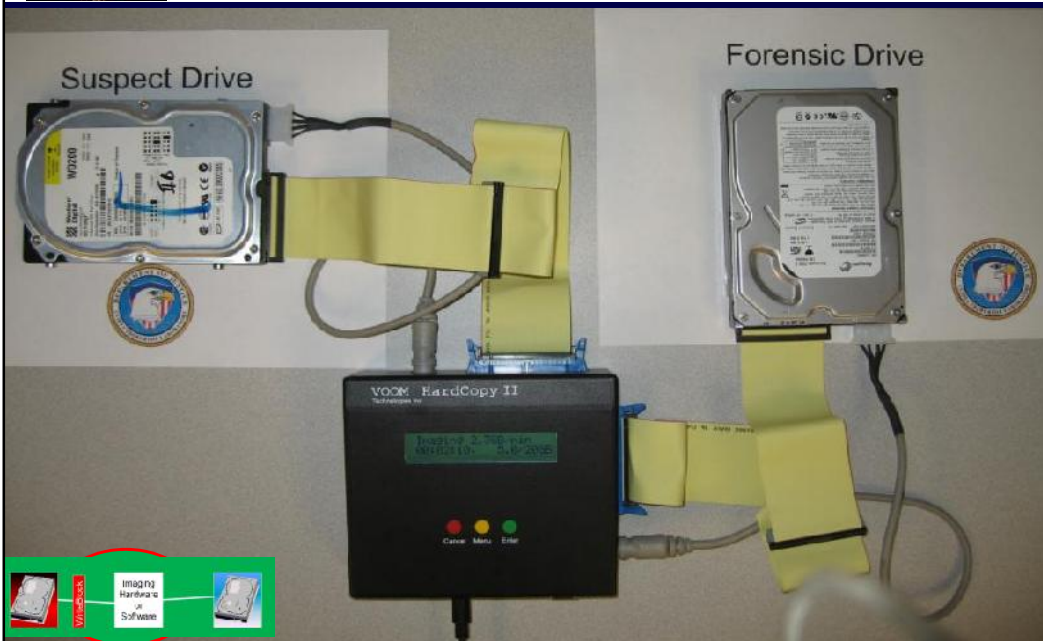





## Attaching Write Block






## Hardware Imager










## Software Imaging

- Bootable CDs or floppies
- Control computer so it only issues read commands to the drive, never write
- Examples:
  - FTK Imager
  - EnCase
  - DD
  - Ghost
  - Others






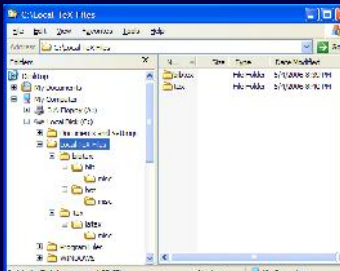







## Physical vs. Logical

- Physical data structure refers to the actual organization of data on a storage device. Physical imaging gets all the zeros and ones possible from the device.
- Logical data structure refers to how the information appears to a program or user as seen through the operating system. Logical imaging misses data from areas not seen by the operating system.



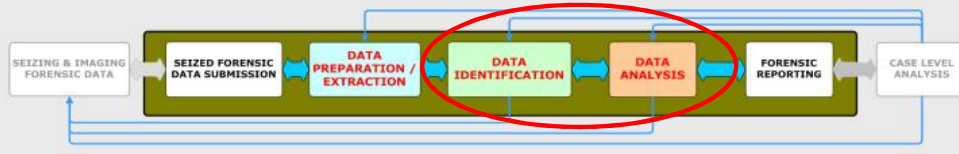






## Forensic Analysis: Where Are We Now?

### PROCESS OVERVIEW



## Case Scenario

- Victim: Heather Miller, daughter of designer Herman Miller
- Abducted by two men, June 2007, from the bus stop in front of Goldf...
- The men were wearing masks
- She was tied up with white rope
- She was told she was going to be killed
- She overheard one of their names
- She was made to drink a liquid
- She woke up in a field near her home
- She received a threatening letter

If you want to keep breathing you better stop talking to the cops!!!



Tell them you made the whole thing up and Drop all charges or **you will die**.

We grabbed you before – we can do it again, only this time you will not live.

Police seized 1



## Case Scenario

- Police have seized one computer system from “Peter Swift”, an individual on parole who matches the height and weight description of one of the subjects
- Swift has a prior arrest and conviction for kidnapping and rape

What would you request



## Forensic Request from Case Agent

- Evidence of defendant’s involvement with abduction
- Search for victim’s name
- Pictures of victim
- Evidence of threatening letter sent to victim
- Evidence of references to date rape drugs
- Evidence of conspirator
- Activity on the computer during time of crime
- User attribution

Key word searches



## Getting Started

- Keyword Searches
- What is a String Search/Key Word Search
  - Like Westlaw & LexisNexis
- Drawbacks to key word searches
  - Adobe PDF documents
  - Faxes
  - Excel
  - Registry
  - Compound/Compressed Files
  - Several others

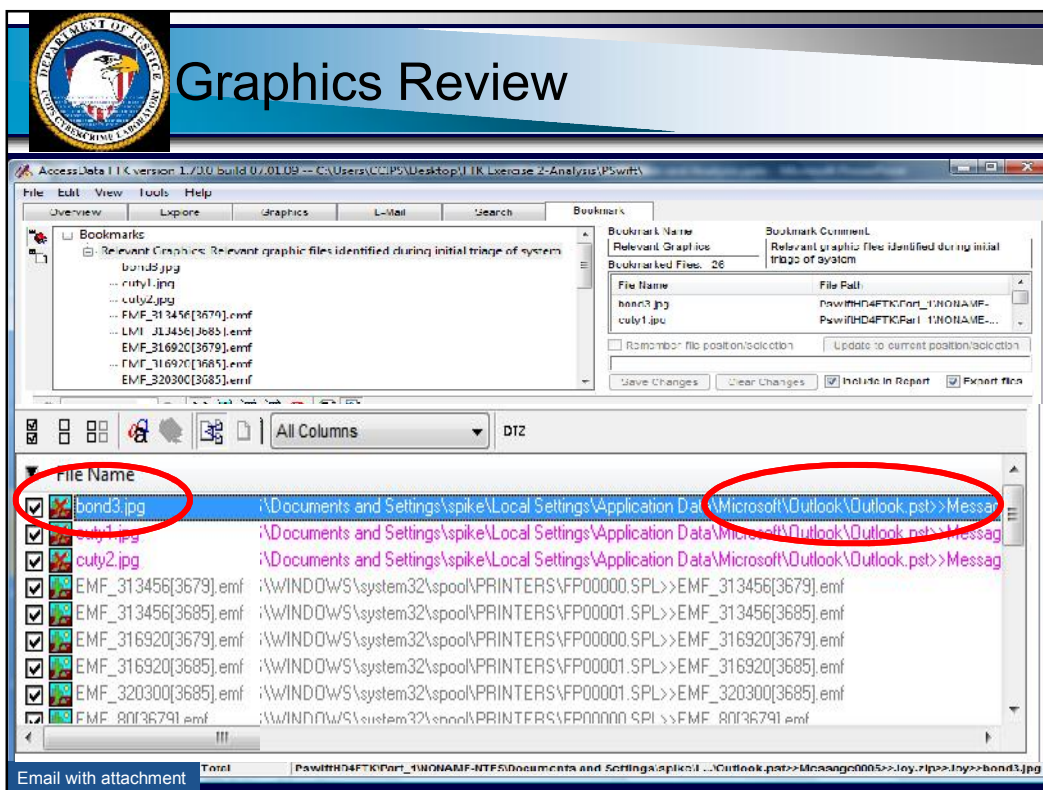
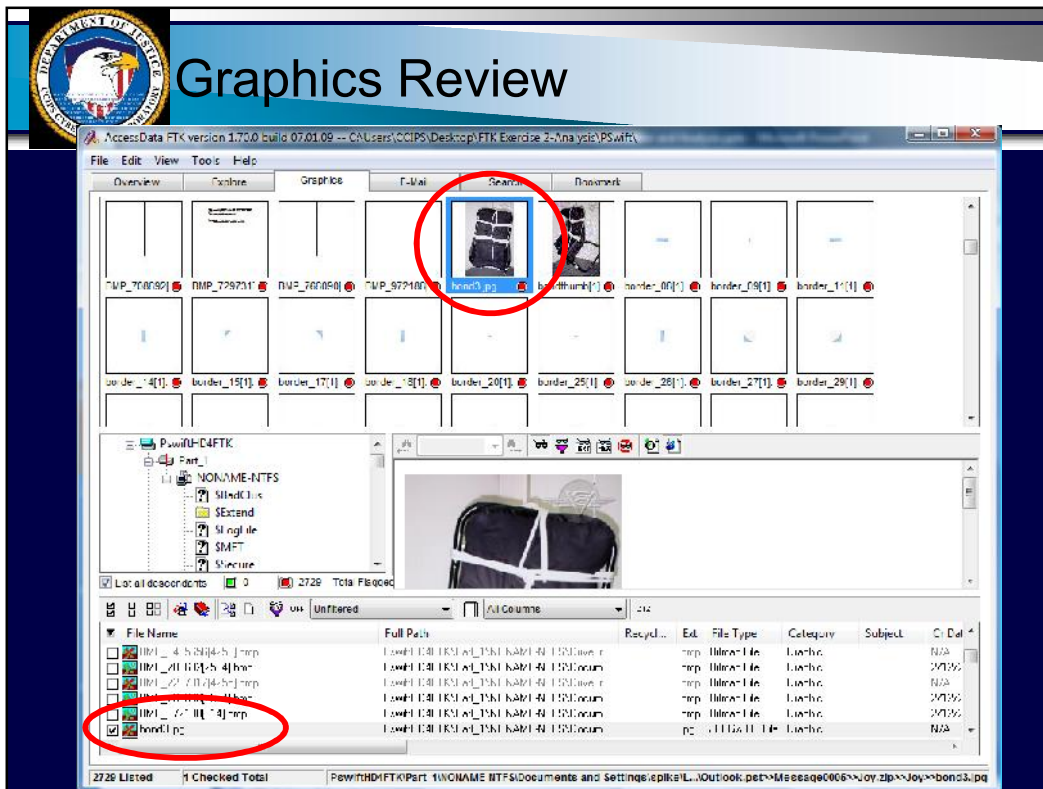
Victim Name



## Getting Started

- Right now we have the Victim's name "Heather Miller" and we know what she looks like. What do you want to do first?
- Key word search for victim's name reveals no relevant Information.
- Next: review graphics

Graphic Review



**DEPARTMENT OF JUSTICE**

# Email Review

AccessData FTK 1.70.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\F... pswift

Overview Explore Graphics E-Mail Bookmark

File Edit View Tools Help

Personal Folders

- Cutlook.pst
  - Personal Folders
    - Calendar
    - Contacts
    - Deleted Items

Message List

Name	Path
Message000	...Documents and Settings\pik\Local Settings\Application Data\Microsoft\Cutlook\Cutlook.pst
Message003	...Documents and Settings\pik\Local Settings\Application Data\Microsoft\Cutlook\Cutlook.pst
Message004	...Documents and Settings\pik\Local Settings\Application Data\Microsoft\Cutlook\Cutlook.pst
Message005	PswiHD4FTK\PswiHD4FTK\pik\Local Settings\Application Data\Microsoft\Cutlook\Cutlook.pst
Message006	...Documents and Settings\pik\Local Settings\Application Data\Microsoft\Cutlook\Cutlook.pst
Message007	...Documents and Settings\pik\Local Settings\Application Data\Microsoft\Cutlook\Cutlook.pst

Message:005

**Subject:** pics from last weekend  
**From:** Maryland Dirtbag  
**Date:** 2/20/2007 1:22:41 PM  
**To:** pswift2007@gmail.com

**Message Body**

Buddy, here is the pics from last weekend. i fiet like a king on presidents holiday.

>From: "Peter Swift" <pswift2007@gmail.com>  
 >To: <mdhosebag@hotmail.com>  
 >Subject: last one  
 >Date: Thu, 15 Feb 2007 14:53:26 -0500  
 >

>this is the last one for a bit, you should be able to get you jolkes from

Attachments: joy.zip, joy, hon-1.jpg, curs1.jpg, curs2.jpg, chn-1.jpg, chn-2.jpg, pto-c.jpg

Headers

**DEPARTMENT OF JUSTICE**

# Email Headers

Standard Header Information

Delivered-To: pswift2007@gmail.com  
 Received: by 10.64.153.3 with SMTP id a3cs152336qbc;  
 Tue, 20 Feb 2007 10:22:41 -0800 (PST)  
 Received: by 10.114.126.1 with SMTP id y1nr3442785war:1171995758192;  
 Tue, 20 Feb 2007 10:22:38 -0800 (PST)

Tue, 20 Feb 2007 10:21:38 -0800  
 Message-ID: <BAY115-F286B576945D5DB4E9F0288B3890@phx.gbl>  
 Received: from 65.54.250.200 by by115fd.bay115.hotmail.msn.com with HTTP;  
 Tue, 20 Feb 2007 18:21:36 GMT  
 X-Originating-IP: [66.166.254.82]  
 X-Originating-Email: [mdhosebag@hotmail.com]  
 X-Sender: mdhosebag@hotmail.com  
 From: "Maryland Dirtbag" <mdhosebag@hotmail.com>  
 To: pswift2007@gmail.com  
 Bcc:  
 Subject: pics from last weekend  
 Date: Tue, 20 Feb 2007 13:21:36 -0500  
 Mime-Version: 1.0  
 Content-Type: multipart/mixed; boundary="====\_NextPart\_000\_1290\_1f21\_3b10"  
 X-OriginalArrivalTime: 20 Feb 2007 18:21:38.0744 (UTC) FILETIME=[F6436B80:01C7551B]  
 Return-Path: mdhosebag@hotmail.com

Time Analysis

Content-Type: multipart/mixed; boundary="====\_NextPart\_000\_1290\_1f21\_3b10"  
 X-OriginalArrivalTime: 20 Feb 2007 18:21:38.0744 (UTC)



## Types of Email Metadata

- What types of Metadata are available
  - When Created
  - How Created
  - When Sent
  - When Received
  - Who Sent/Received
  - Route
  - Time Analysis
  - Graphic Analysis
    - Origination
    - Who Created it
    - When Created
  - Application Logs

Time analysis




## Time Analysis

Infiltered [icon] Default File List Column Se [icon] DTZ

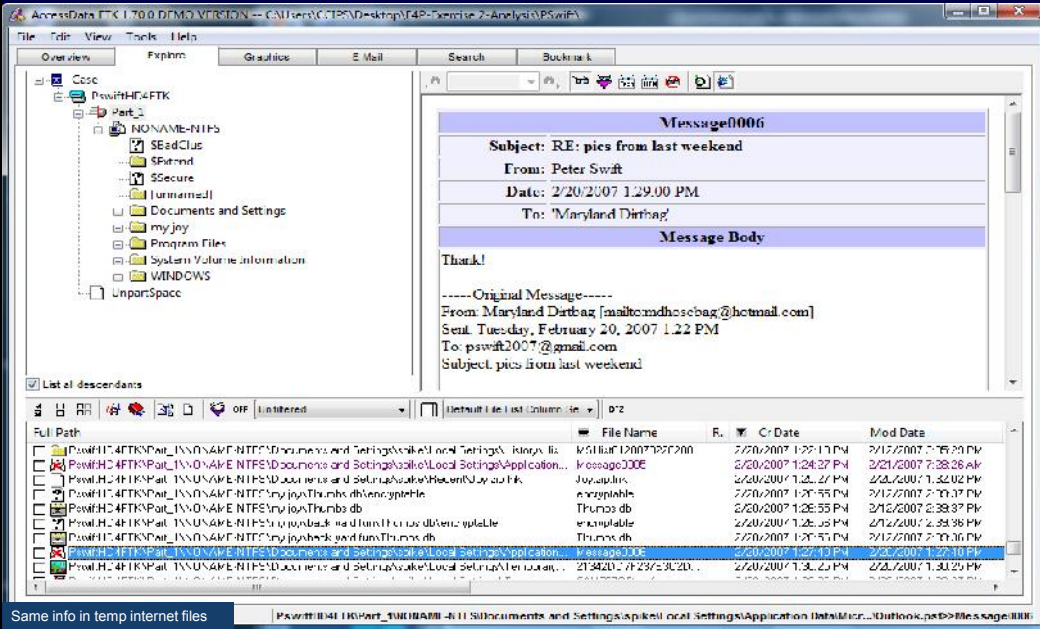
	File Name	R.	Cr Date
%Documents and Settings\spike\Local Settings\History\His...	MSHist0120070220200...		2/20/2007 1:22:10 PM
%Documents and Settings\spike\Local Settings\Application...	Message0005		2/20/2007 1:24:27 PM
%Documents and Settings\spike\Recent\Joy.zip.lnk	Joy.zip.lnk		2/20/2007 1:25:27 PM
%my joy\Thumbs.db\encryptable	encryptable		2/20/2007 1:26:55 PM
%my joy\Thumbs.db	Thumbs.db		2/20/2007 1:26:55 PM
%my joy\back yard fun\Thumbs.db\encryptable	encryptable		2/20/2007 1:26:56 PM
%my joy\back yard fun\Thumbs.db	Thumbs.db		2/20/2007 1:26:56 PM
%Documents and Settings\spike\Local Settings\Application...	Message0006		2/20/2007 1:27:40 PM
%Documents and Settings\spike\Local Settings\Temporary...	21342DD7F237E3C2D...		2/20/2007 1:30:25 PM
%Documents and Settings\spike\Local Settings\Temporary...	CA15C70D...		2/20/2007 1:30:25 PM

7 Highlighted


Reply email



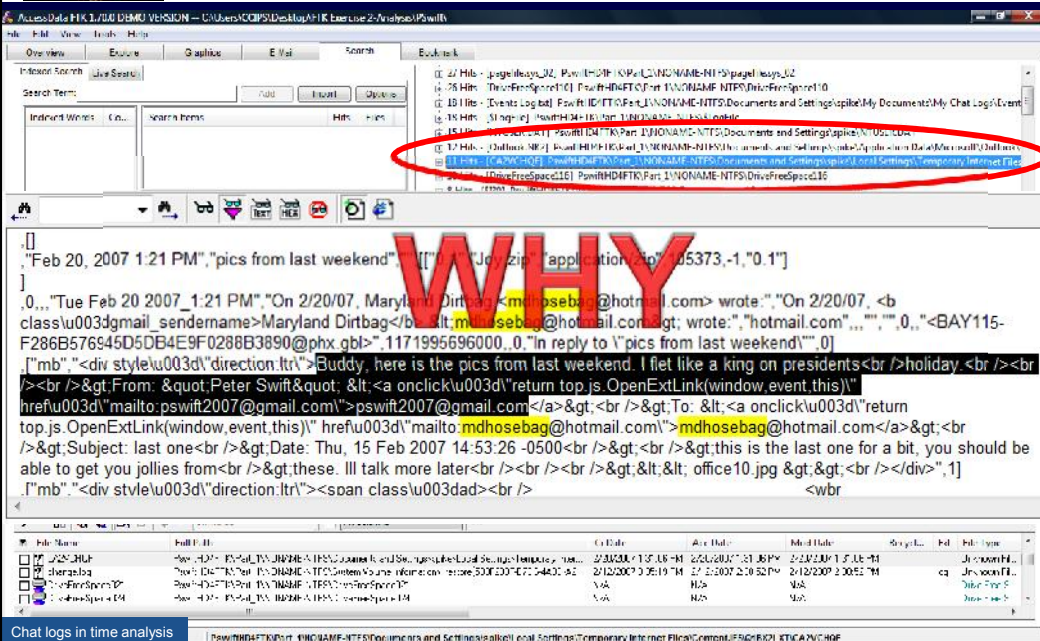
# Reply Email



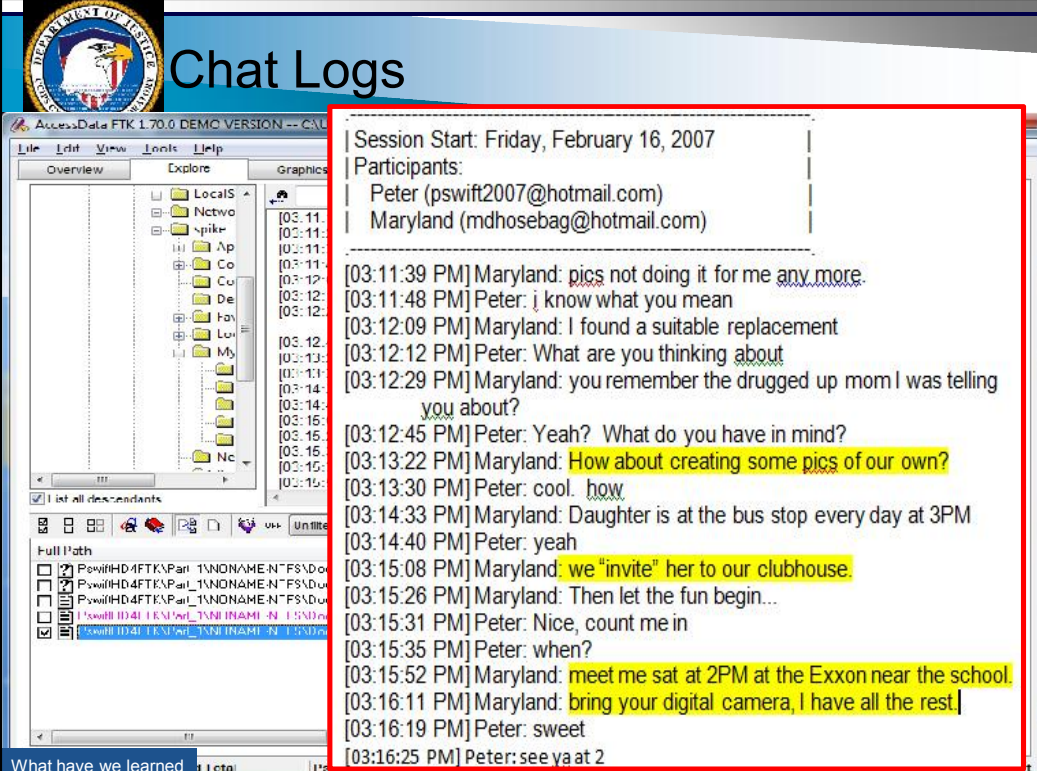
Same info in temp internet files



# Internet Cache-Copy of "Message005"



Chat logs in time analysis

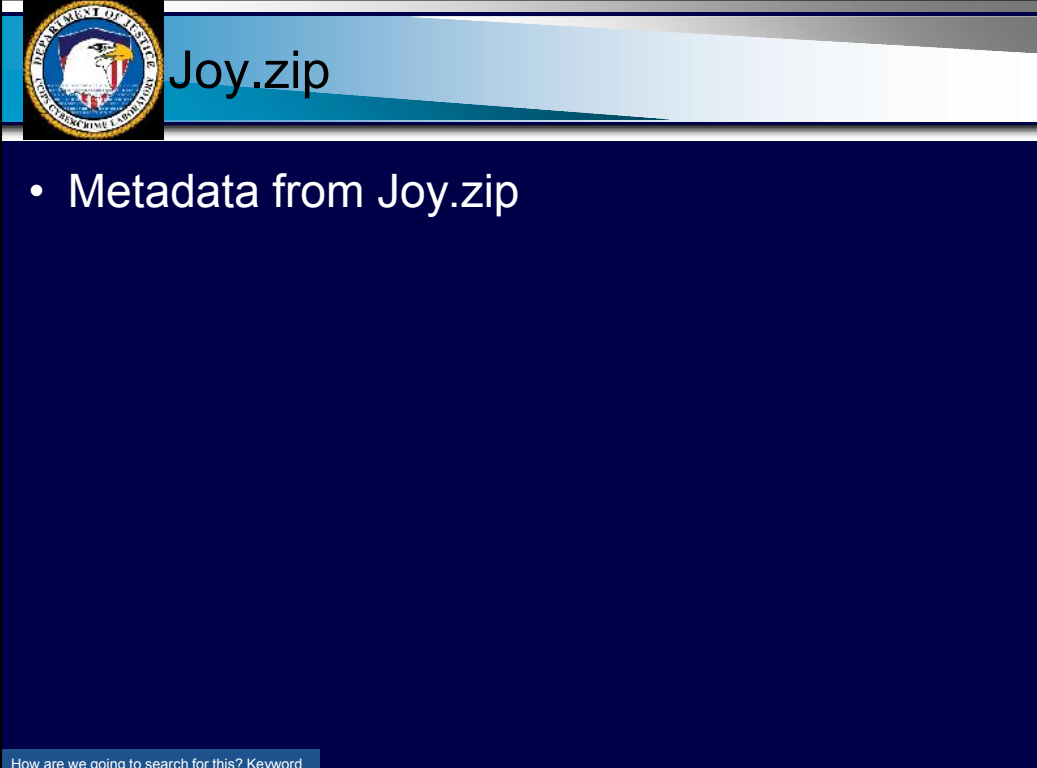


**Chat Logs**

Session Start: Friday, February 16, 2007  
 Participants:  
 Peter (pswift2007@hotmail.com)  
 Maryland (mdhosebag@hotmail.com)

[03:11:39 PM] Maryland: pics not doing it for me any more.  
 [03:11:48 PM] Peter: i know what you mean  
 [03:12:09 PM] Maryland: I found a suitable replacement  
 [03:12:12 PM] Peter: What are you thinking about  
 [03:12:29 PM] Maryland: you remember the drugged up mom I was telling you about?  
 [03:12:45 PM] Peter: Yeah? What do you have in mind?  
 [03:13:22 PM] Maryland: How about creating some pics of our own?  
 [03:13:30 PM] Peter: cool. how  
 [03:14:33 PM] Maryland: Daughter is at the bus stop every day at 3PM  
 [03:14:40 PM] Peter: yeah  
 [03:15:08 PM] Maryland: we "invite" her to our clubhouse.  
 [03:15:26 PM] Maryland: Then let the fun begin...  
 [03:15:31 PM] Peter: Nice, count me in  
 [03:15:35 PM] Peter: when?  
 [03:15:52 PM] Maryland: meet me sat at 2PM at the Exxon near the school.  
 [03:16:11 PM] Maryland: bring your digital camera, I have all the rest  
 [03:16:19 PM] Peter: sweet  
 [03:16:25 PM] Peter: see ya at 2

What have we learned



**Joy.zip**

- Metadata from Joy.zip

How are we going to search for this? Keyword



**Time Analysis**

Unfiltered | Default File List Column Se | DTZ

File Name	R.	Cr Date
MSHist0120070220200...		2/20/2007 1:22:10 PM
Message0005		2/20/2007 1:24:27 PM
Joy.zip.lnk		2/20/2007 1:25:27 PM
encryptable		2/20/2007 1:26:55 PM
Thumbs.db		2/20/2007 1:26:55 PM
encryptable		2/20/2007 1:26:56 PM
Thumbs.db		2/20/2007 1:26:56 PM
Message0006		2/20/2007 1:27:40 PM
21342DD7F237E3C2D...		2/20/2007 1:30:25 PM

7 Highlighted

Link File w/Thumb drive

**Link File**

AccessData FTK 1.7.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\F4P-Exercise 2-Analyis\PSwin\

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Case

- PsWinH4-FTK
  - Part 1
    - NONAME-NTFS
      - SEcdClus
      - SEExtend
      - SSEcure
      - [unnamed]
      - Documents and Settings
      - myjoy
      - Program Files
      - System Volume Information
      - WINDOWS
      - unperfspace

List all descendants

Unfiltered | Default File List Column Se | DTZ

**Shortcut File**

Link target information

Local Path	E:\Joy.zip
Volume Type	Removable Disk
Volume Label	TRANSCLND
Volume Serial Number	0899-373D
File size	0
Creation time (UTC)	N/A

Full Path | File Name | R. | Cr Date | Mod Date

... \Documents and Settings\spike\Local Settings\History\His...	index.dct		2/20/2007 1:22:10 PM	2/20/2007 1:22:10 PM
... \Documents and Settings\spike\Local Settings\Application...	index.dct		2/20/2007 1:22:10 PM	2/15/2007 3:38:46 PM
... \Documents and Settings\spike\Recent\Joy.zip.lnk	k\$HstC120070212200...		2/20/2007 1:22:10 PM	2/12/2007 3:35:29 PM
... \myjoy\Thumbs.db\encryptable	k\$HstC12007022C200...		2/20/2007 1:22:10 PM	2/12/2007 3:35:29 PM
... \myjoy\Thumbs.db	Message0005		2/20/2007 1:24:27 PM	2/21/2007 7:28:26 AM
... \myjoy\back yard fun\Thumbs.db\encryptable	Joy.zip.lnk		2/20/2007 1:25:27 PM	2/21/2007 1:25:27 PM
... \myjoy\back yard fun\Thumbs.db	encryptable		2/20/2007 1:26:55 PM	2/20/2007 1:26:55 PM
... \Documents and Settings\spike\Local Settings\Application...	Thumbs.db		2/20/2007 1:26:55 PM	2/20/2007 1:26:55 PM
... \Documents and Settings\spike\Local Settings\Temporary...	encryptable		2/20/2007 1:26:56 PM	2/20/2007 1:26:56 PM
...	Thumbs.db		2/20/2007 1:26:56 PM	2/20/2007 1:26:56 PM
...	Message0006		2/20/2007 1:27:40 PM	2/20/2007 1:27:40 PM
...	21342DD7F237E3C2D...		2/20/2007 1:30:25 PM	2/20/2007 1:30:25 PM

Log file c:\myjoy\joy.zip | I\$wvH4-FTK\ort\_1\NONAME-NTFS\Documents and Settings\spike\Recent\Joy.zip.lnk

# What does this tell us?

AccessData FTK 1.7.0.0 DEMO VERSION - C:\Users\COPI\Desktop\FTK EserUse2-7\ntfs\PSwRt

151 file - [LogFile] PswRt DHTK Part UNONAME-NTFS logFile

TRANSCEND

TRANSCEND?

File Name	Full Path	Cr Date	Acc Date	Mod Date	Recy...	Ext	File Type
151 file	C:\Users\COPI\Desktop\FTK EserUse2-7\ntfs\PSwRt	2/12/2007 12:54:37	2/12/2007 12:54:37	2/12/2007 12:54:37			Journal File

What is TRANSCEND - Google

# What is "Transcend"?

Google Web Images Video News Maps more »

transcend e: Search Advanced Search Preferences

Web Results 1 - 10 of about 2,700,000 for **transcend e:** (0.54 seconds)

**Welcome to Transcend website**  
Yes, I want to receive Transcend's official site e-Newsletter (News, new product information.)  
Yes, I want to receive Transcend's E-Commerce site ...  
[www.transcendusa.com/TsClub/Signup.asp?LargNc=0&Func1No=7&Func2No=114-49k](http://www.transcendusa.com/TsClub/Signup.asp?LargNc=0&Func1No=7&Func2No=114-49k) - [Cached](#) - [Similar pages](#) - [Note this](#)

**Welcome to Transcend Website - Contact Us**  
Worldwide Offices, Contact Sales, Contact TechSupport, Global Partners, Send Resume, Where to buy.  
[www.transcendusa.com/Contact/index.asp?Func1No=6&LangNo=0](http://www.transcendusa.com/Contact/index.asp?Func1No=6&LangNo=0) - 62k - [Cached](#) - [Similar pages](#) - [Note this](#)

**MSBA Legal E-Mail**  
Transcend e-Discovery, LLC. P. O. Box 715 New Market, MD 21774 ... The staff of Transcend e-Discovery, LLC is comprised of former law enforcement officers ...  
[www.msba.org/links/email/showwemd.asp?ID=220](http://www.msba.org/links/email/showwemd.asp?ID=220) - 10k - [Cached](#) - [Similar pages](#) - [Note this](#)

**Privacy Policy**  
When you visit Transcend's Online Store or send e-mails to us, you are communicating with us electronically. By doing so you consent to receive ...  
[ec.transcendusa.com/term.asp?TID=8](http://ec.transcendusa.com/term.asp?TID=8) - 132k - [Cached](#) - [Similar pages](#) - [Note this](#)

[Transcend Online Store USA](#)

Sponsored Links  
**Transcend - Official Site**  
Memory Supplier for Desktops, Laptops & Servers Lifetime Warranty  
[www.TranscendUSA.com](http://www.TranscendUSA.com)

Internet | Protected Mode: On 100%

# Google is Your Friend

Welcome to Transcend Website - JetFlash™ M,etFlash™ MP3,JetFlash™ DSC ,JetFlash™ WL ,Hi Speed Windows Internet Explorer

http://www.transcendusa.com/Products/CatList.asp?CategoryId=3&LangNo=0&Fl... Live Search

Transcend

Products | Support | Online Store | Press Center | About Transcend | Contact Us | OEM | Site Map | Advanced Search

Standard Memory  
Proprietary Memory  
JetRam Module  
Flash Cards  
USB Flash Drive  
T.sonic MP3 Series  
Portable H.U  
Multimedia Products  
Accessories  
IDE Flash Disk  
Certifications  
Portable HDD  
Multimedia Products  
Accessories  
IDE Flash Disk

Home>Products>USB Flash Drive>USB Flash Drive

USB Drive

JetFlash™ T2K

Hi-Speed Series V Series T Series JetFlash™ elite

Hi Speed Series Perfect design for performance demanding users.  
V series Perfect design for va ue-driven users.  
T series Perfect replacement for floppy disk/CD/DVD.  
JetFlash™ elite

Click on Images Tab

# Google is Your Friend (Images)

Google Images

Transcend Search Advanced Image Search Preferences

Moderate SafeSearch is on

Images Showing: All image sizes Results 1 - 20 of about 119,000 for Transcend [definition]. (0.09 seconds)

transcend :: mp3 rctation GIVE...  
750 x 600 - 95k - jpg  
music.trabia-garden.net

transcend  
600 x 458 - 85k - jpg  
www.ueberfaachen.de

TRANSCEND  
About Transcend:  
406 x 616 - 176k - gif  
www.transcend.us

TRAVEL & CHANGE  
500 x 320 - 32k - jpg  
www.transcend.us  
[ Move from www.transcend.us ]

transcend.jpg  
500 x 600 - 02k - jpg  
jeltowns.com

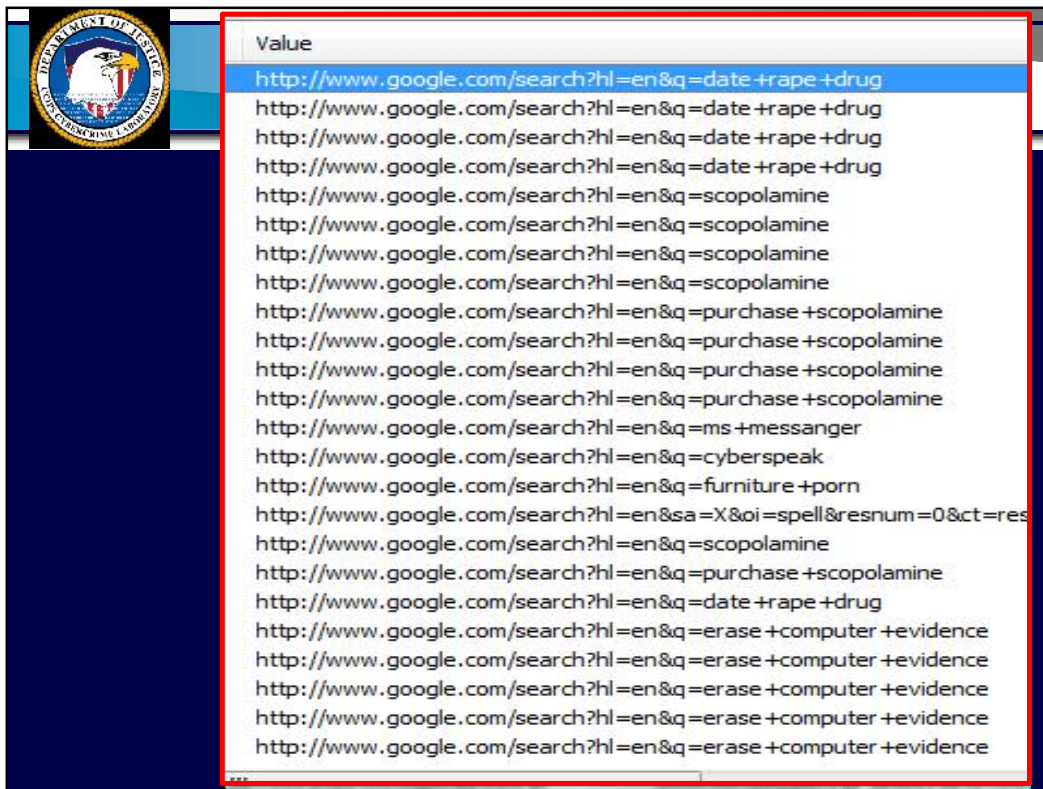
big-Transcend I.Sonic 610  
512Mb - jpg ...  
200 x 223 - 11k - jpg

big-Transcend I.Sonic 610 256  
Mb ...  
260 x 130 - 11k - jpg

Nov 14: Transcend USB Disk  
Drive  
251 x 189 - 4k - jpg

Next we find a LINK file







## Web History

- Identify web surfing session
  - Where/when did they open browser?
  - How did they get to the significant finding?
  - Web mail
  - Other Activities?
- All goes toward user attribution



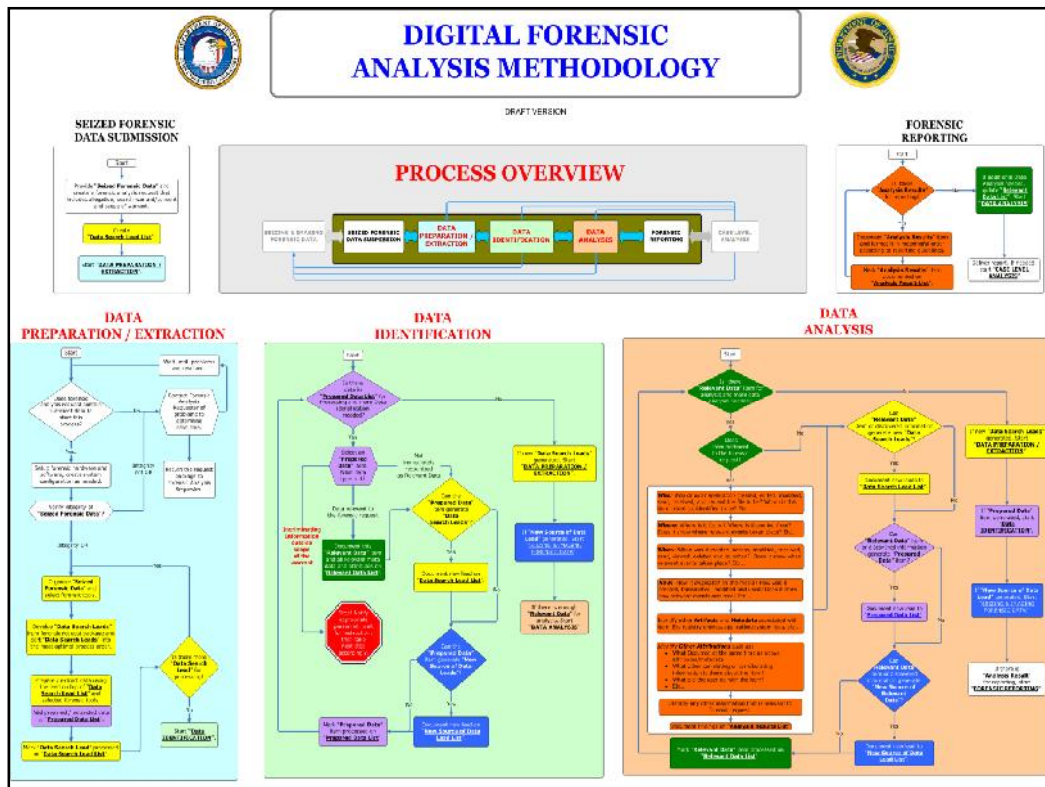
## Summary

- Electronic evidence is everywhere
- Forensic examiners must look beyond the “Single File”
- Metadata can be critical to establishing user attribution
- Even if evidence itself has been deleted/destroyed, there are numerous artifacts that can still be found



# Other Training Tools

- Digital Forensic Analysis Methodology flowchart
  - aid to explaining and discussing the process of computer forensics
  - available at: [http://www.cybercrime.gov/forensics\\_chart.pdf](http://www.cybercrime.gov/forensics_chart.pdf)





## Contact

James Silver  
Computer Crime and  
Intellectual Property Section  
United States Department of Justice

- Phone:202-514-1026
- Web:[www.cybercrime.gov](http://www.cybercrime.gov)