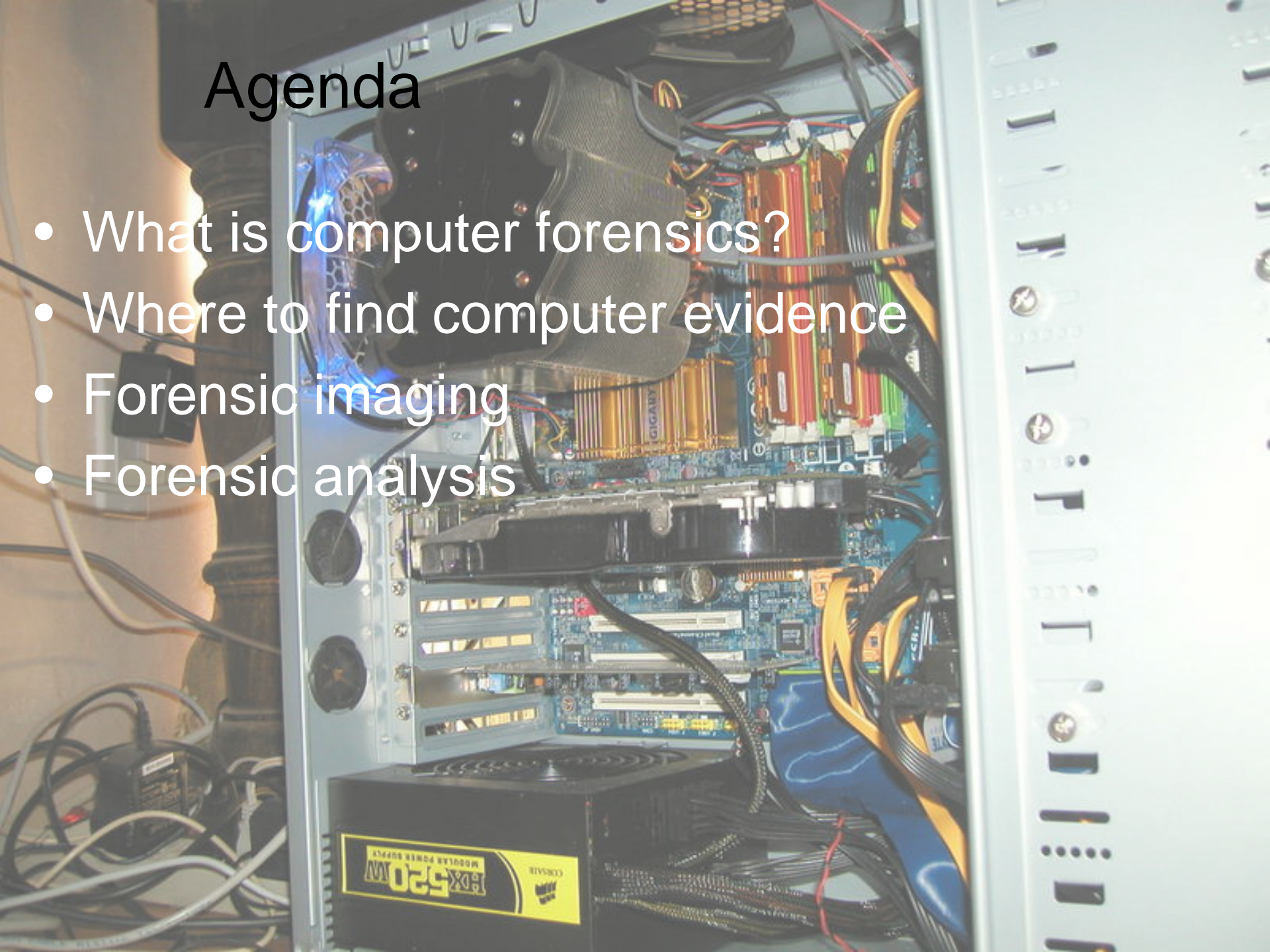


Computer Forensic Capabilities



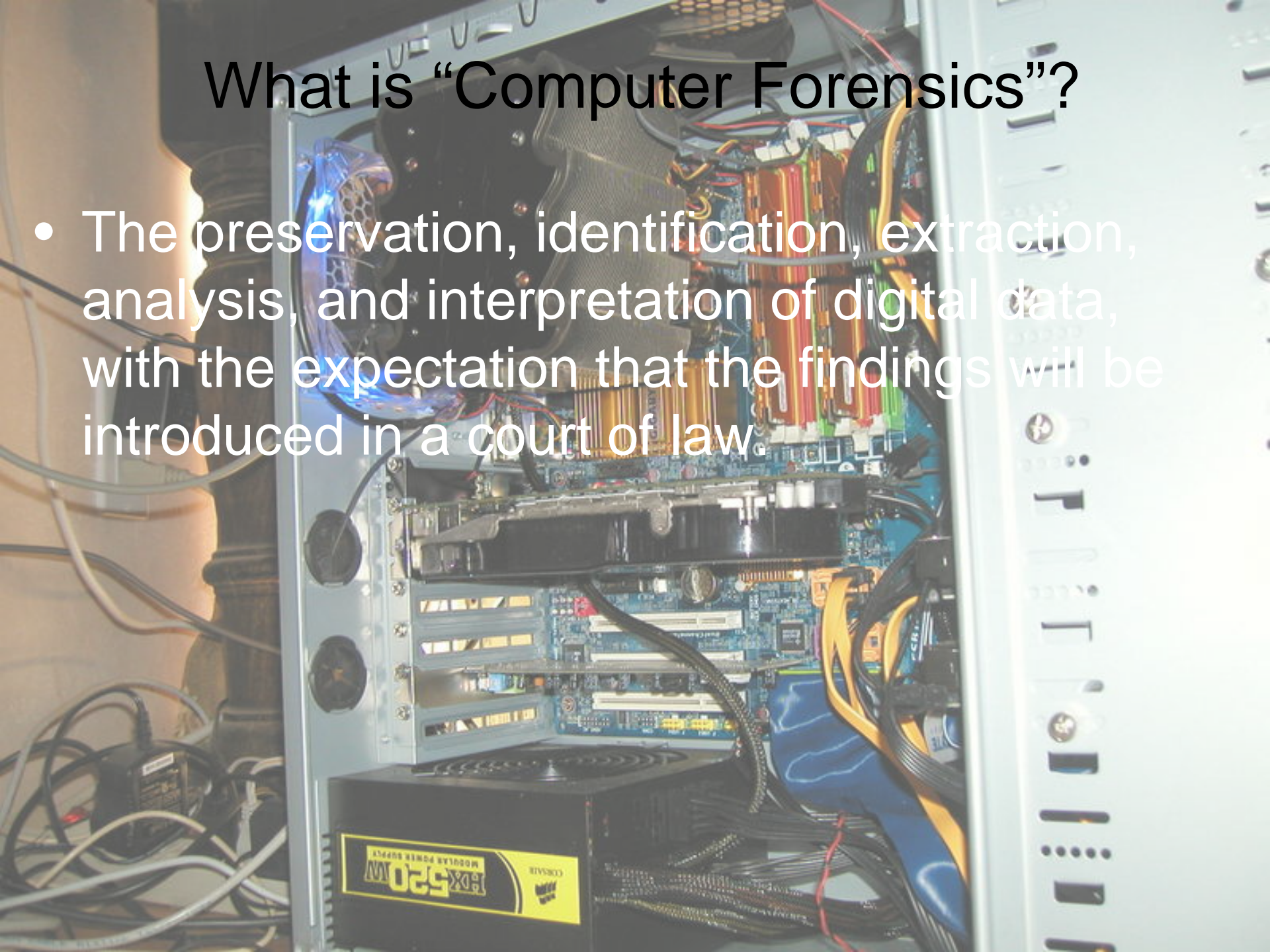
Agenda

- What is computer forensics?
- Where to find computer evidence
- Forensic imaging
- Forensic analysis



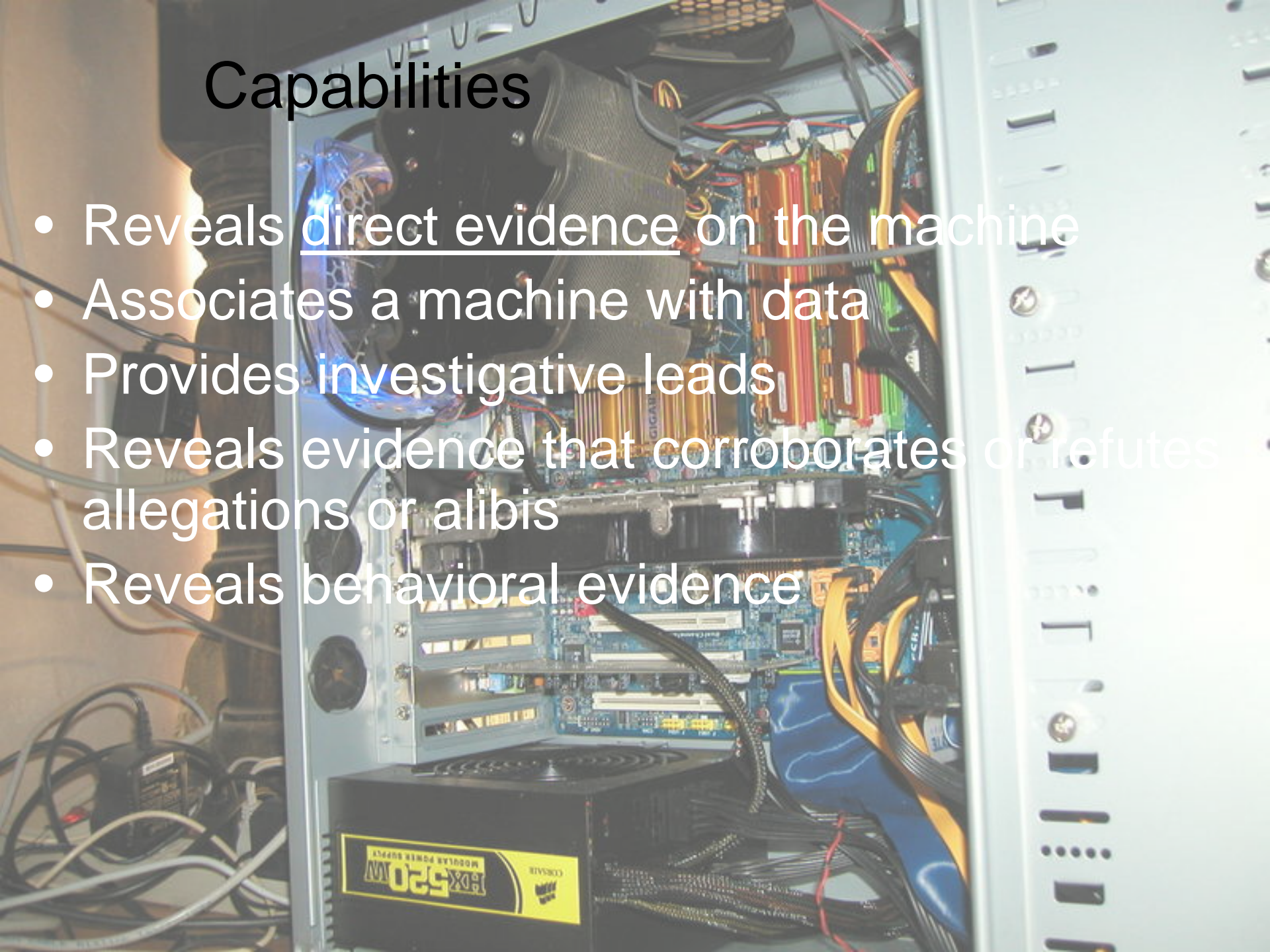
What is “Computer Forensics”?

- The preservation, identification, extraction, analysis, and interpretation of digital data, with the expectation that the findings will be introduced in a court of law.



Capabilities

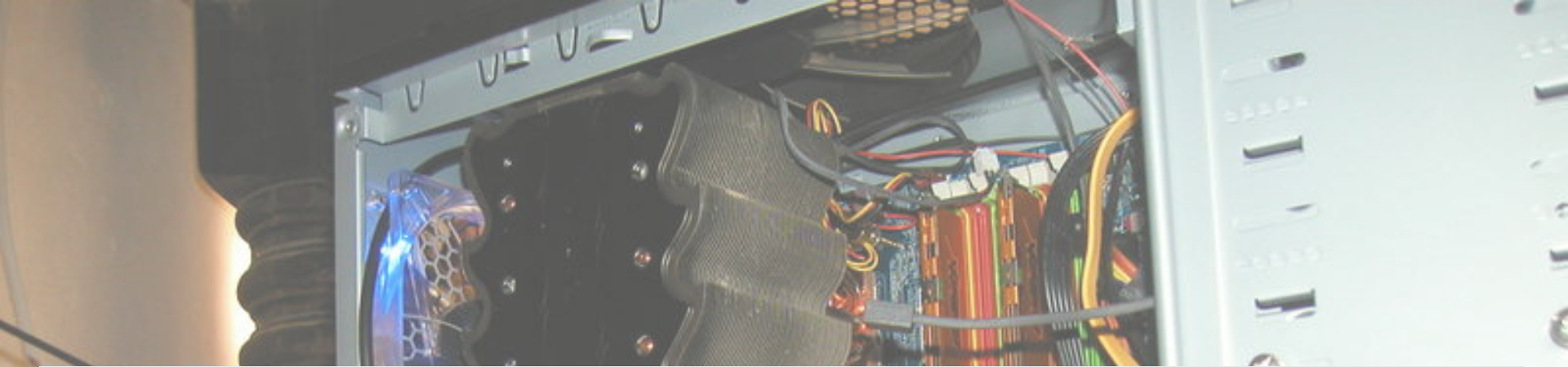
- Reveals direct evidence on the machine
- Associates a machine with data
- Provides investigative leads
- Reveals evidence that corroborates or refutes allegations or alibis
- Reveals behavioral evidence



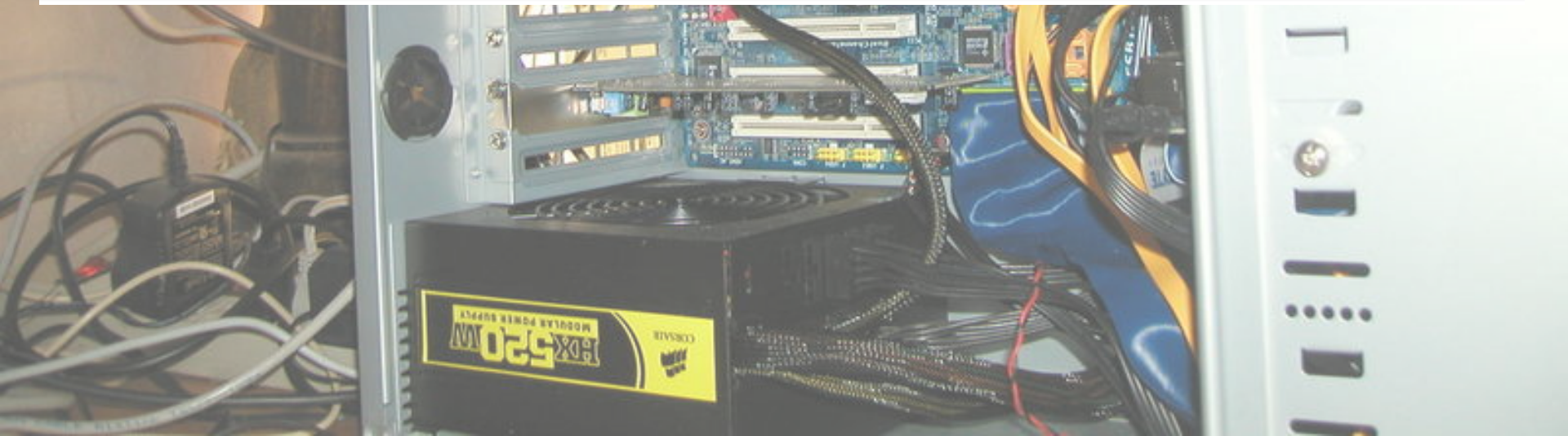
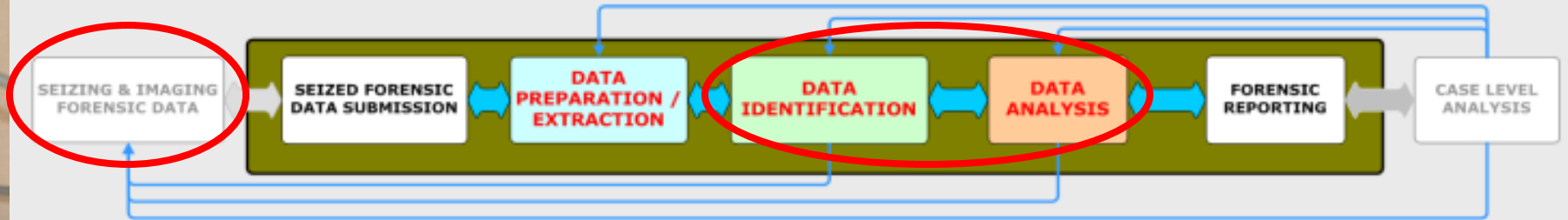
Case Agent-Examiner Relationship



- The case agent and forensic examiner must work as a team
- Case agent
 - Involves examiner early
 - Explains case
 - Provides focused requests
- Forensic examiner
 - Educates and advises investigator
 - Explains results and limitations

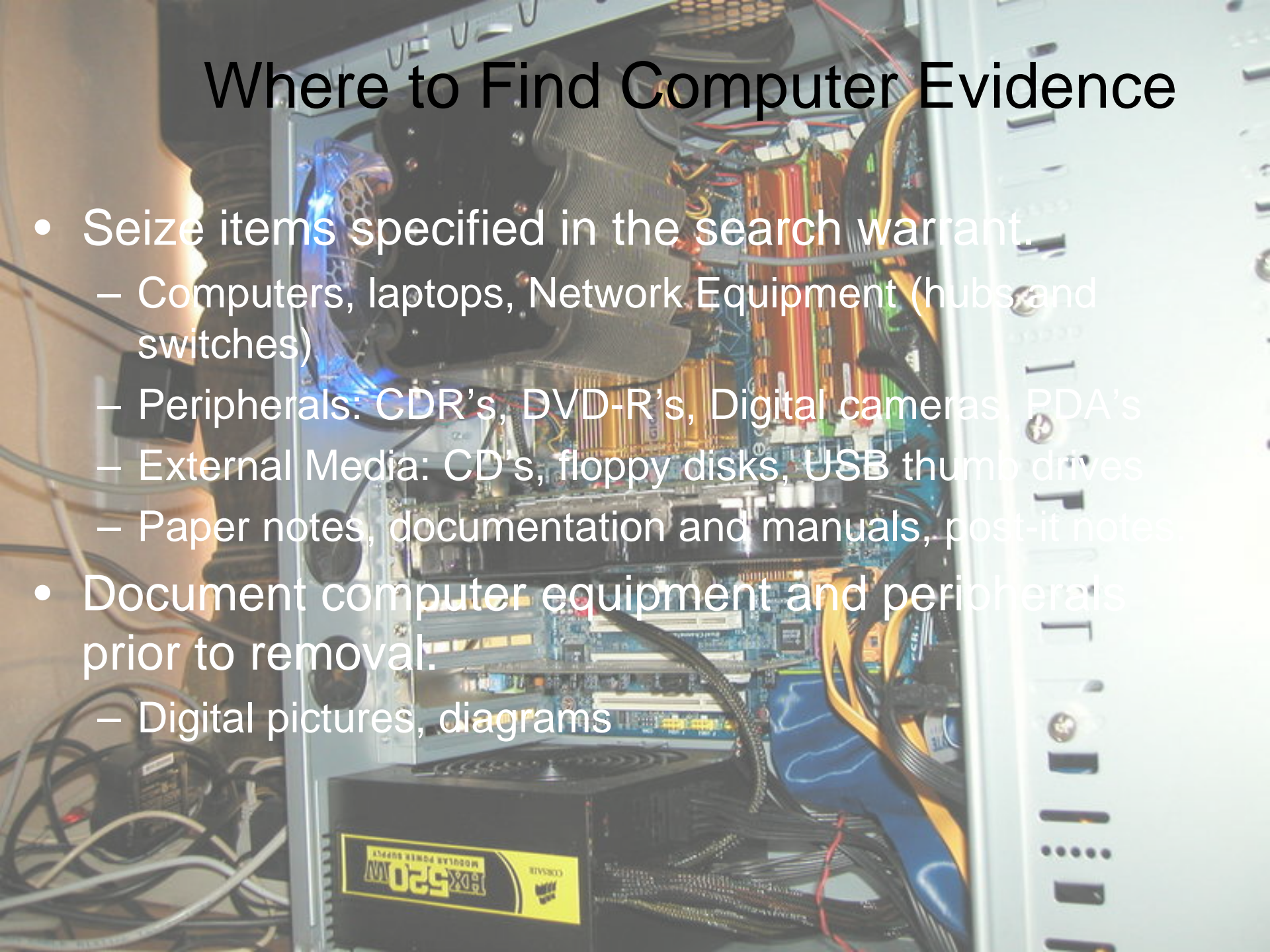


PROCESS OVERVIEW



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

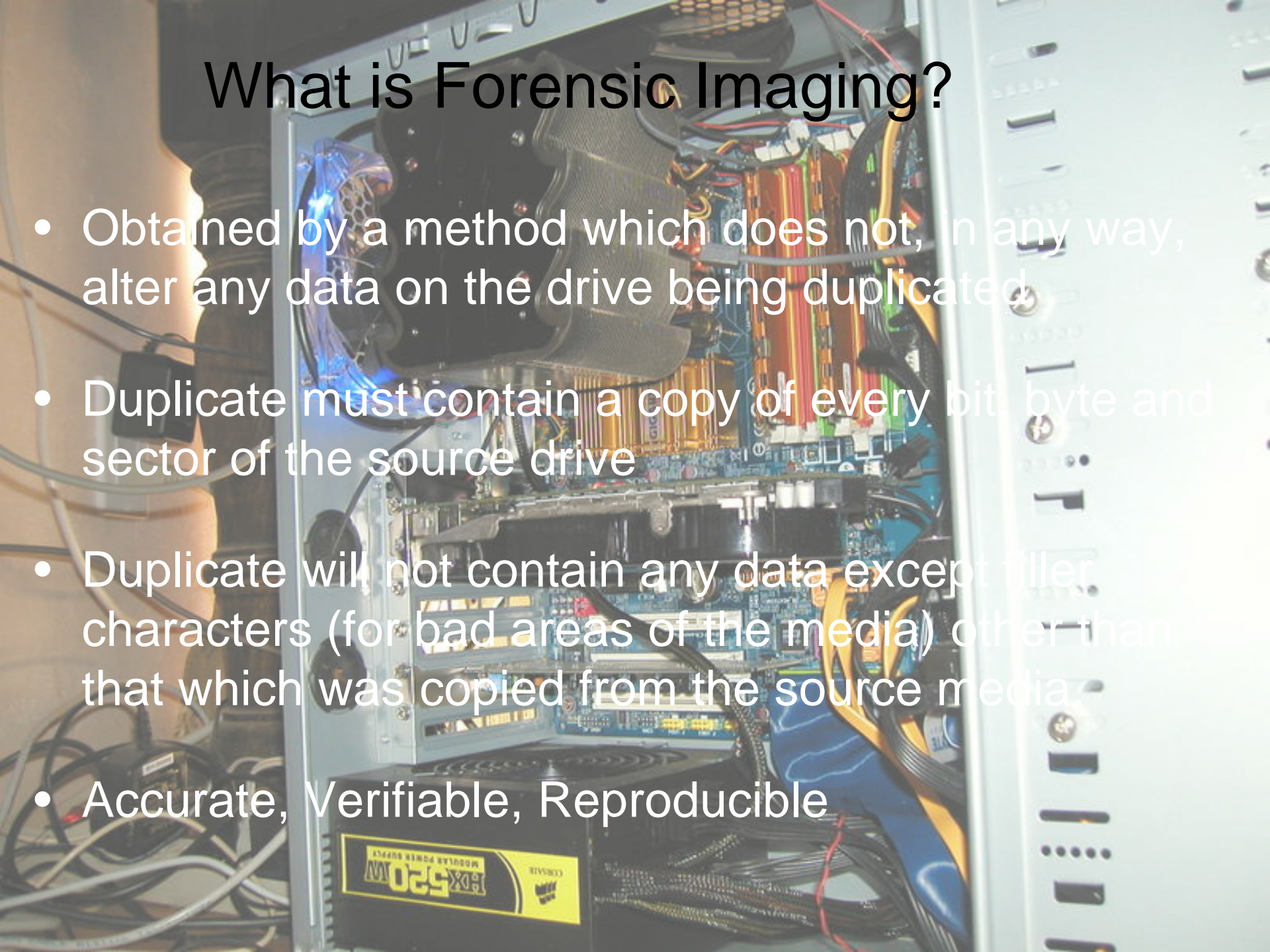


But Wait, There's More



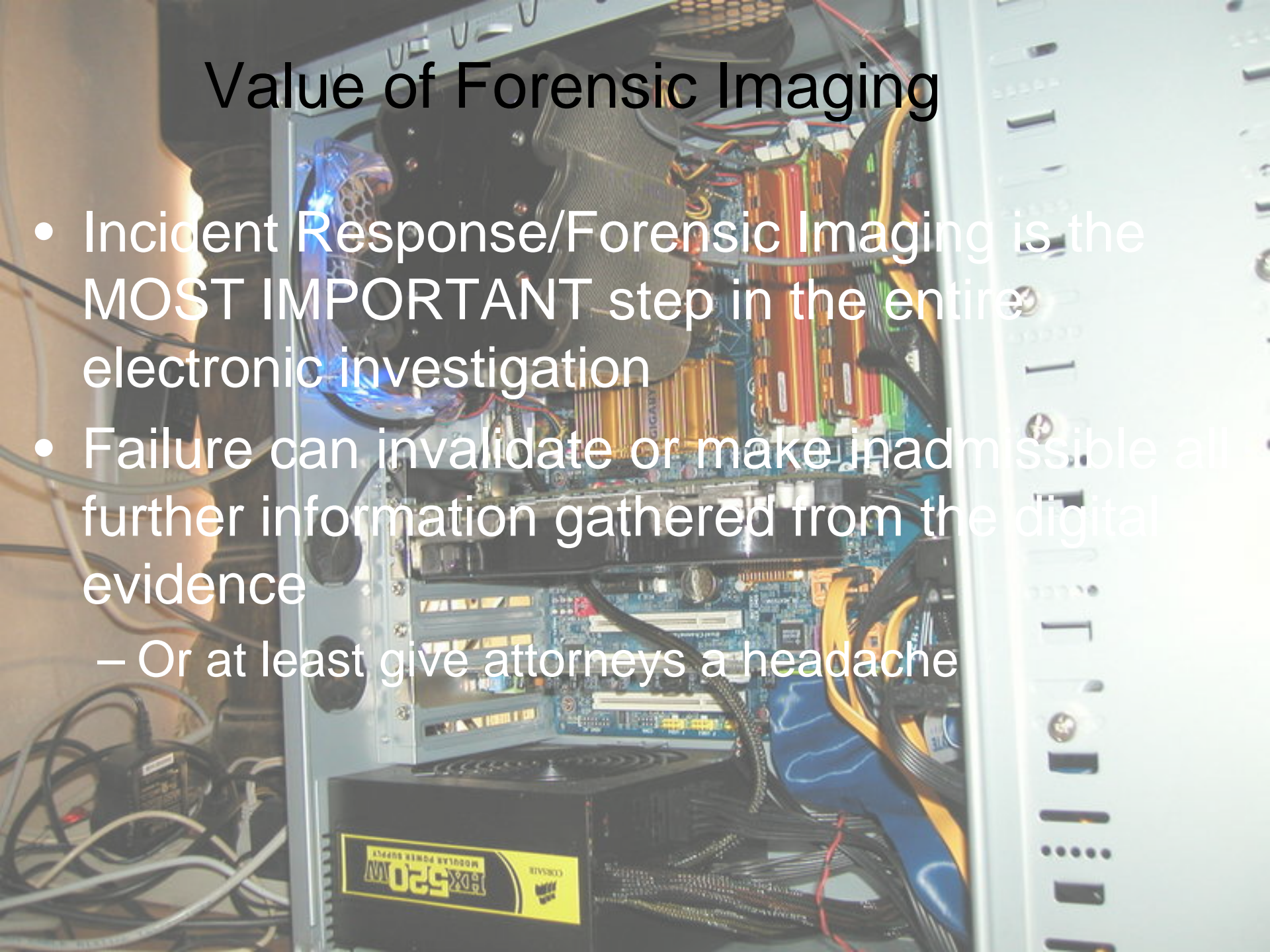
What is Forensic Imaging?

- 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



Value of Forensic Imaging

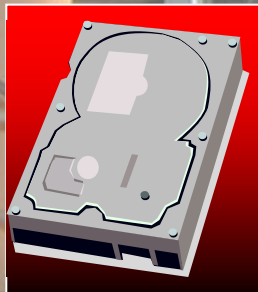
- Incident Response/Forensic Imaging is the **MOST IMPORTANT** step in the entire electronic investigation
- Failure can invalidate or make inadmissible all further information gathered from the digital evidence
 - Or at least give attorneys a headache



The Imaging Process

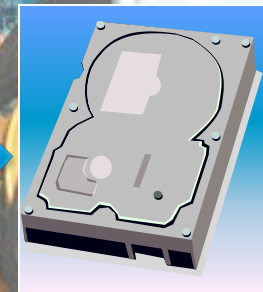
010011
010101
01

010011
010101
01



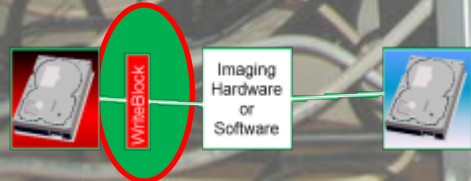
WriteBlock

Imaging
Hardware
or
Software



Physical Write Blocks

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



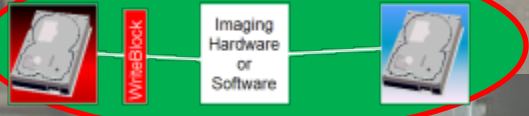
Attaching Write Block



Imaging Hardware or Software



Attaching Write Block



Hardware Imager

Suspect Drive



Forensic Drive



VOOM HardCopy II
Technologies Inc.

Imaging 2.398 MB/s
08/02/18 5:09:28

Cancel Menu Enter



WriteBlock

Imaging
Hardware
or
Software



Software Imaging

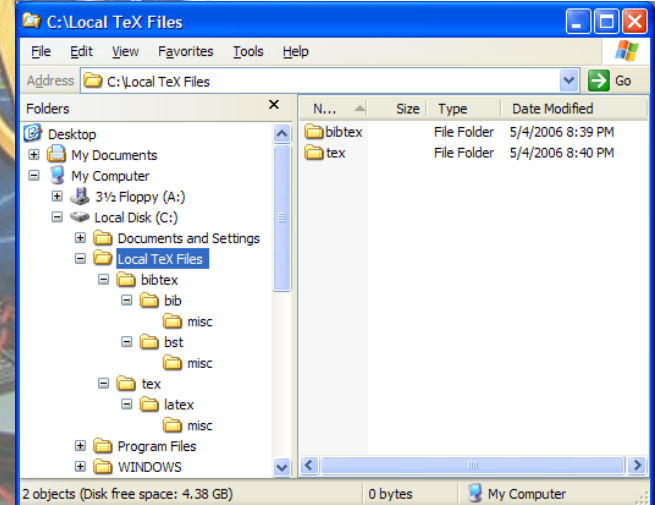
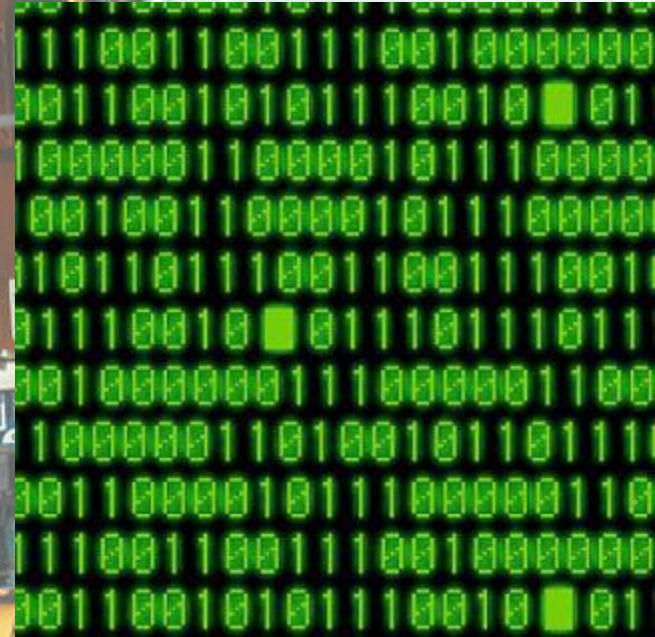
- Bootable CDs or floppies
- Control computer so it only issues read commands to the drive, never write
- Examples:
 - FTK Imager
 - EnCase
 - DD
 - Ghost
 - Others



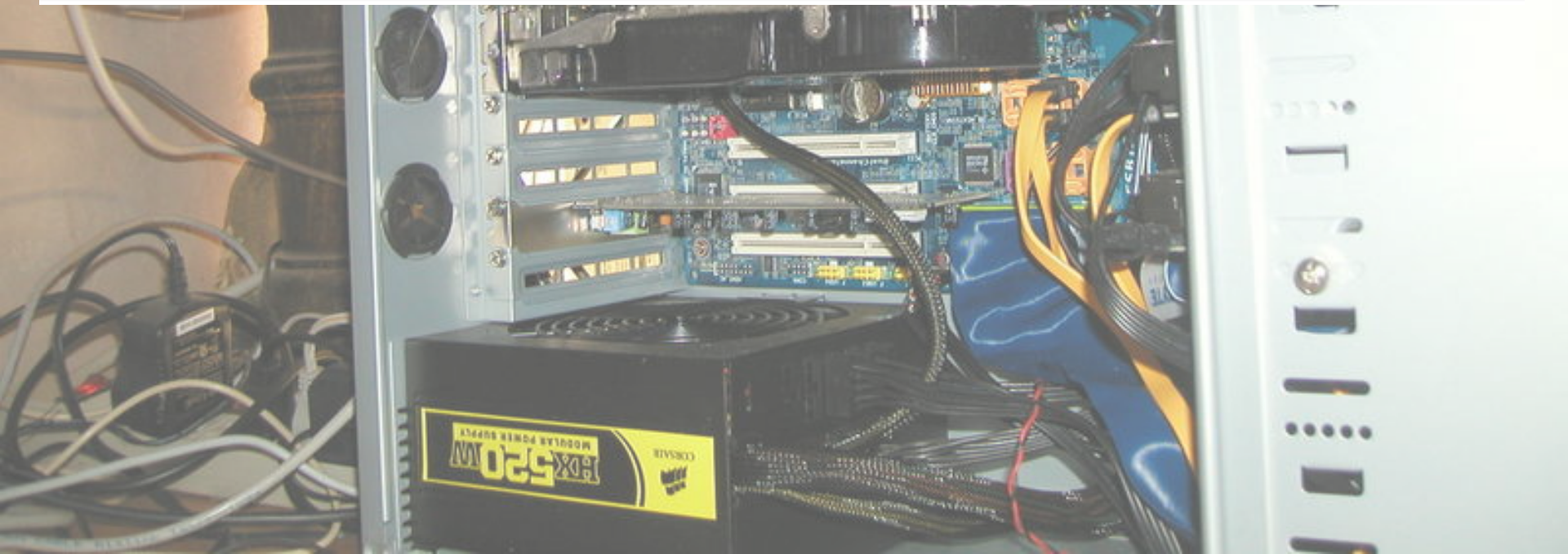
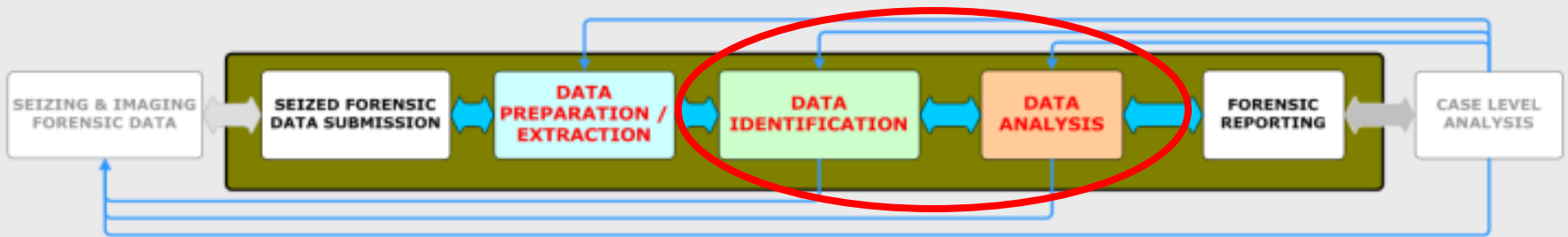
Physical vs. Logical

- 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.

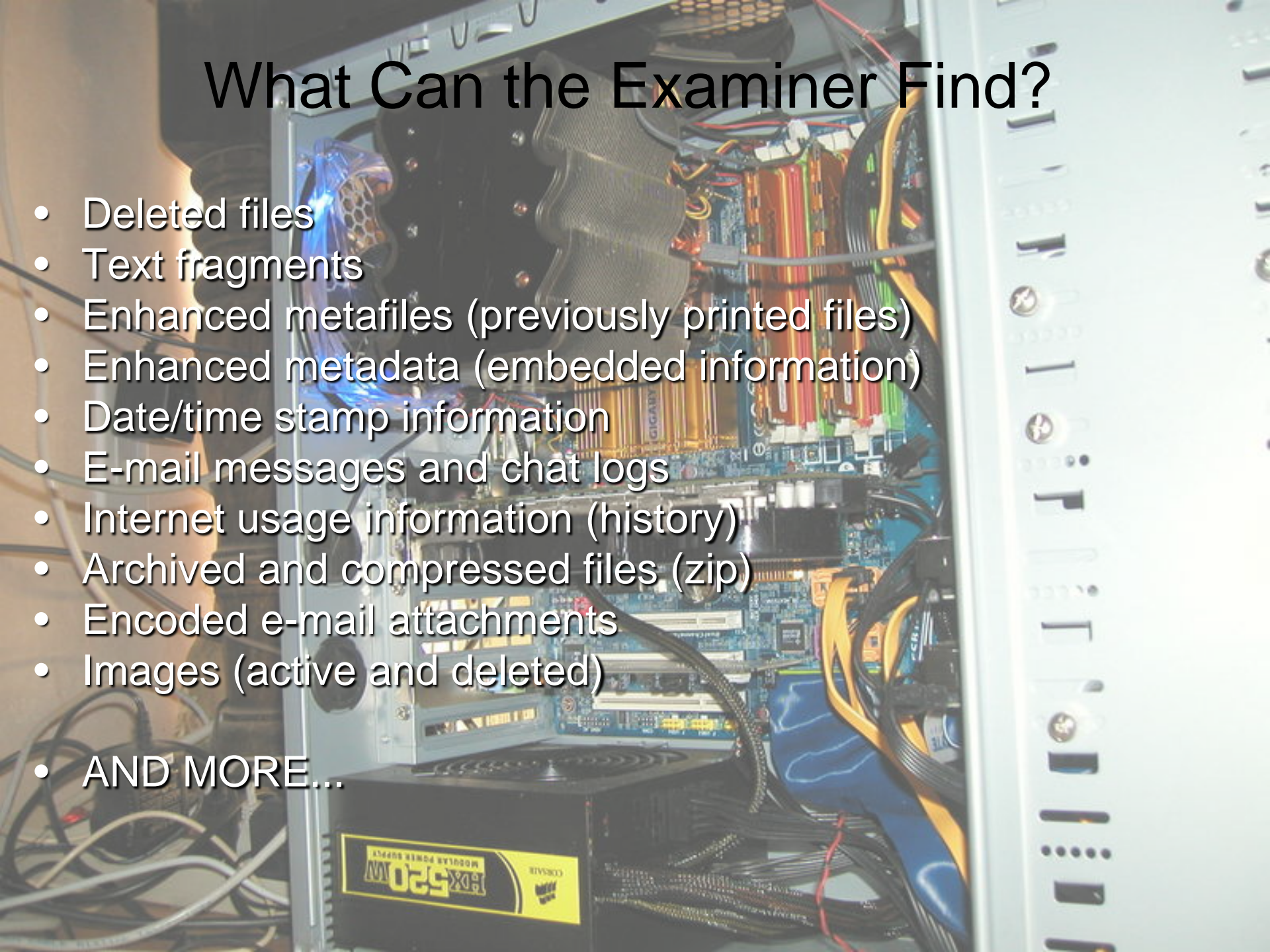


PROCESS OVERVIEW



What Can the Examiner Find?

- Deleted files
- Text fragments
- Enhanced metafiles (previously printed files)
- Enhanced metadata (embedded information)
- Date/time stamp information
- E-mail messages and chat logs
- Internet usage information (history)
- Archived and compressed files (zip)
- Encoded e-mail attachments
- Images (active and deleted)
- AND MORE...



Forensic Request from Case Agent

- EXAMPLE: Kidnapping assault of Heather Miller
 - 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

Getting Started

- Keyword Searches
- Drawbacks to key word searches
 - Adobe PDF documents
 - Faxes
 - Excel
 - Registry
 - Compound/Compressed Files
 - Several others

Getting Started

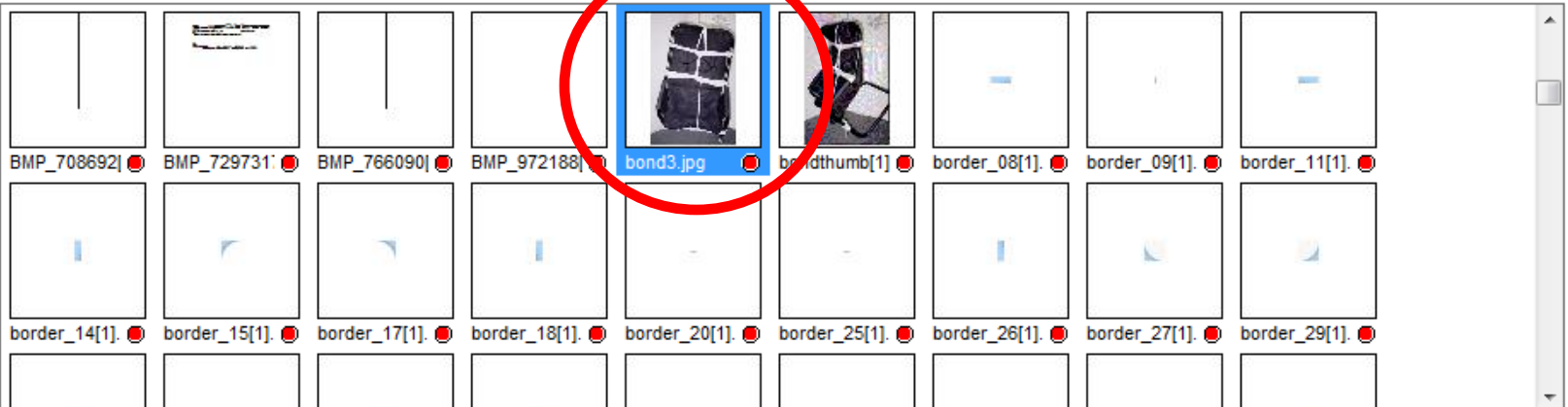
- Right now we have the Victim's name "Heather Miller" and we know what she looks like. What do you want to do first?
- Key word search for victim's name reveals no relevant Information.
- Next: review graphics

Graphics Review

AccessData FTK version 1.70.0 build 07.01.09 -- C:\Users\CCIPS\Desktop\FTK Exercise 2-Analysis\PSwift\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark




BMP_708692[1] BMP_729731[1] BMP_766090[1] BMP_972188[1] bond3.jpg bondthumb[1] border_08[1] border_09[1] border_11[1]

border_14[1] border_15[1] border_17[1] border_18[1] border_20[1] border_25[1] border_26[1] border_27[1] border_29[1]

PswiftHD4FTK

- Part_1
 - NONAME-NTFS
 - SBadClus
 - SExtend
 - SLogFile
 - SMFT
 - SSecure

List all descendants 0 2729 Total Flagged



Unfiltered All Columns DTZ

File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Dat
<input type="checkbox"/> BMP_6485656[4250].bmp	PswiftHD4FTK\Part_1\NONAME-NTFS\DriveFr...		bmp	Bitmap File	Graphic	N/A	
<input type="checkbox"/> BMP_708692[2584].bmp	PswiftHD4FTK\Part_1\NONAME-NTFS\Docum...		bmp	Bitmap File	Graphic	N/A	2/12/2
<input type="checkbox"/> BMP_7297317[4255].bmp	PswiftHD4FTK\Part_1\NONAME-NTFS\DriveFr...		bmp	Bitmap File	Graphic	N/A	
<input type="checkbox"/> BMP_766090[2591].bmp	PswiftHD4FTK\Part_1\NONAME-NTFS\Docum...		bmp	Bitmap File	Graphic	N/A	2/12/2
<input type="checkbox"/> BMP_972188[614].bmp	PswiftHD4FTK\Part_1\NONAME-NTFS\Docum...		bmp	Bitmap File	Graphic	N/A	2/12/2
<input checked="" type="checkbox"/> bond3.jpg	PswiftHD4FTK\Part_1\NONAME-NTFS\Docum...		jpg	JPEG/JFIF File	Graphic	N/A	

2729 Listed 1 Checked Total PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\L... Outlook.pst>>Message0005>>Joy.zip>>Joy>>bond3.jpg

Graphics Review

AccessData FTK version 1.70.0 build 07.01.09 -- C:\Users\CCIPS\Desktop\FTK Exercise 2-Analysis\PSwift\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Bookmarks

- Relevant Graphics: Relevant graphic files identified during initial triage of system
 - bond3.jpg
 - cuty1.jpg
 - cuty2.jpg
 - EMF_313456[3679].emf
 - EMF_313456[3685].emf
 - EMF_316920[3679].emf
 - EMF_316920[3685].emf
 - EMF_320300[3685].emf

Bookmark Name: Relevant Graphics
Bookmark Comment: Relevant graphic files identified during initial triage of system
Bookmarked Files: 26

File Name	File Path
bond3.jpg	PswifH4FTK\Part_1\NONAME-...
cuty1.jpg	PswifH4FTK\Part_1\NONAME-...

Remember file position/selection

Include in Report Export files

All Columns DTZ

File Name	File Path
bond3.jpg	:\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst>>Message0005>>Joy.zip>>Joy>>bond3.jpg
cuty1.jpg	:\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst>>Message0005>>Joy.zip>>Joy>>cuty1.jpg
cuty2.jpg	:\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst>>Message0005>>Joy.zip>>Joy>>cuty2.jpg
EMF_313456[3679].emf	:\WINDOWS\system32\spool\PRINTERS\FP00000.SPL>>EMF_313456[3679].emf
EMF_313456[3685].emf	:\WINDOWS\system32\spool\PRINTERS\FP00001.SPL>>EMF_313456[3685].emf
EMF_316920[3679].emf	:\WINDOWS\system32\spool\PRINTERS\FP00000.SPL>>EMF_316920[3679].emf
EMF_316920[3685].emf	:\WINDOWS\system32\spool\PRINTERS\FP00001.SPL>>EMF_316920[3685].emf
EMF_320300[3685].emf	:\WINDOWS\system32\spool\PRINTERS\FP00001.SPL>>EMF_320300[3685].emf
EMF_80136791.emf	:\WINDOWS\system32\spool\PRINTERS\FP00000.SPL>>EMF_80136791.emf

Total | PswifH4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\L... Outlook.pst>>Message0005>>Joy.zip>>Joy>>bond3.jpg

Email with attachment

Email Review

Deleted Email

AccessData FTK 1.70.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\F4... Swift\

File Edit View Tools Help

Overview Explore Graphics E-Mail Bookmark

File Name

- Message0002 ... Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst
- Message0003 ... Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst
- Message0004 ... Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst
- Message0005 PswifHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst
- Message0006 ... Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst
- Personal Folders PswifHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst

List all descendants

Message0005

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 flet 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 jollies from

Message0005

- Joy.zip
- Joy
 - bond3.jpg
 - cuty1.jpg
 - cuty2.jpg
 - struggle.jpg
 - struggle2.jpg
 - tiptoe.jpg

TO / FROM / SUBJECT / DATE

Email Headers

Standard Header Information

Delivered-To: pswift2007@gmail.com
Received: by 10.64.153.3 with SMTP id a3cs152336qbe;
Tue, 20 Feb 2007 10:22:41 -0800 (PST)
Received: by 10.114.126.1 with SMTP id y1mr3442785wac.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

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

	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

7 Highlighted



Reply Email

AccessData FTK 1.70.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\F4P-Exercise 2-Analysis\PSwift\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Case

- Case
 - PSwiftHD4FTK
 - Part_1
 - NONAME-NTFS
 - SBadClus
 - SExtend
 - S\$ecure
 - [unnamed]
 - Documents and Settings
 - my joy
 - Program Files
 - System Volume Information
 - WINDOWS
 - UnpartSpace

List all descendants

Unfiltered

Default File List Column Se DTZ

Full Path	File Name	R.	Cr Date	Mod Date
PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\History\His...	MSHist0120070220200...		2/20/2007 1:22:10 PM	2/12/2007 3:35:29 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application...	Message0005		2/20/2007 1:24:27 PM	2/21/2007 7:28:26 AM
PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Recent\Joy.zip.lnk	Joy.zip.lnk		2/20/2007 1:25:27 PM	2/20/2007 1:32:02 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\my joy\Thumbs.db\encryptable	encryptable		2/20/2007 1:26:55 PM	2/12/2007 2:39:37 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\my joy\Thumbs.db	Thumbs.db		2/20/2007 1:26:55 PM	2/12/2007 2:39:37 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\my joy\back yard fun\Thumbs.db\encryptable	encryptable		2/20/2007 1:26:56 PM	2/12/2007 2:39:36 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\my joy\back yard fun\Thumbs.db	Thumbs.db		2/20/2007 1:26:56 PM	2/12/2007 2:39:36 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application...	Message0006		2/20/2007 1:27:40 PM	2/20/2007 1:27:40 PM
PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Temporary...	21342DD7F237E3C2D...		2/20/2007 1:30:25 PM	2/20/2007 1:30:25 PM

Message0006

Subject: RE: pics from last weekend

From: Peter Swift

Date: 2/20/2007 1:29:00 PM

To: 'Maryland Dirtbag'

Message Body

Thank!

-----Original Message-----

From: Maryland Dirtbag [mailto:mdhosebag@hotmail.com]

Sent: Tuesday, February 20, 2007 1:22 PM

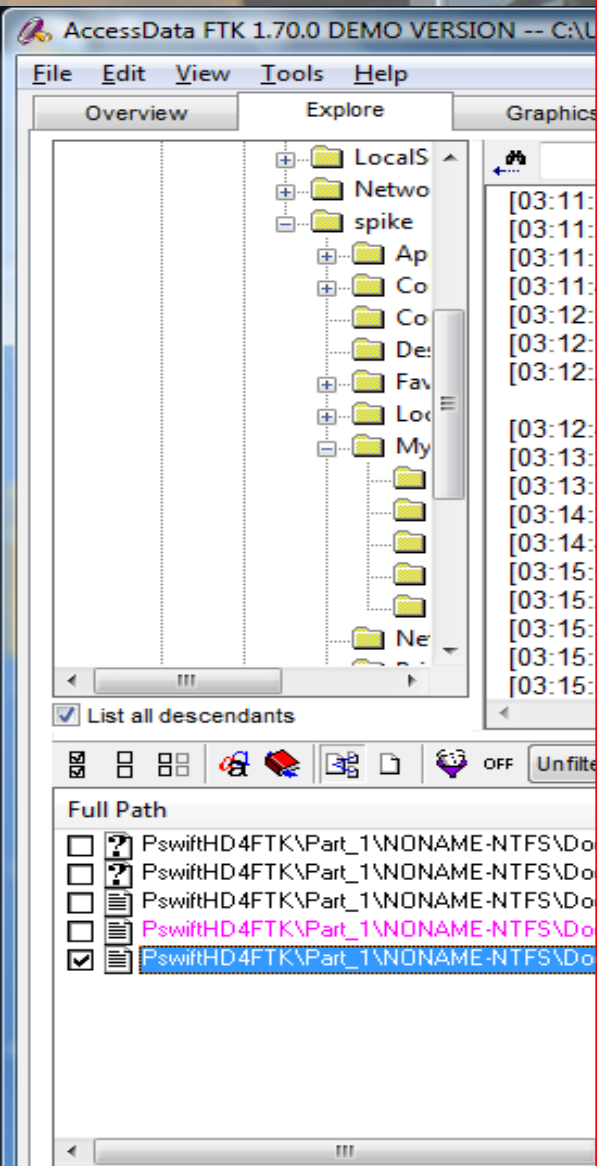
To: pswift2007@gmail.com

Subject: pics from last weekend

Same info in temp internet files

PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application Data\Micr... Outlook.pst>>Message0006

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.

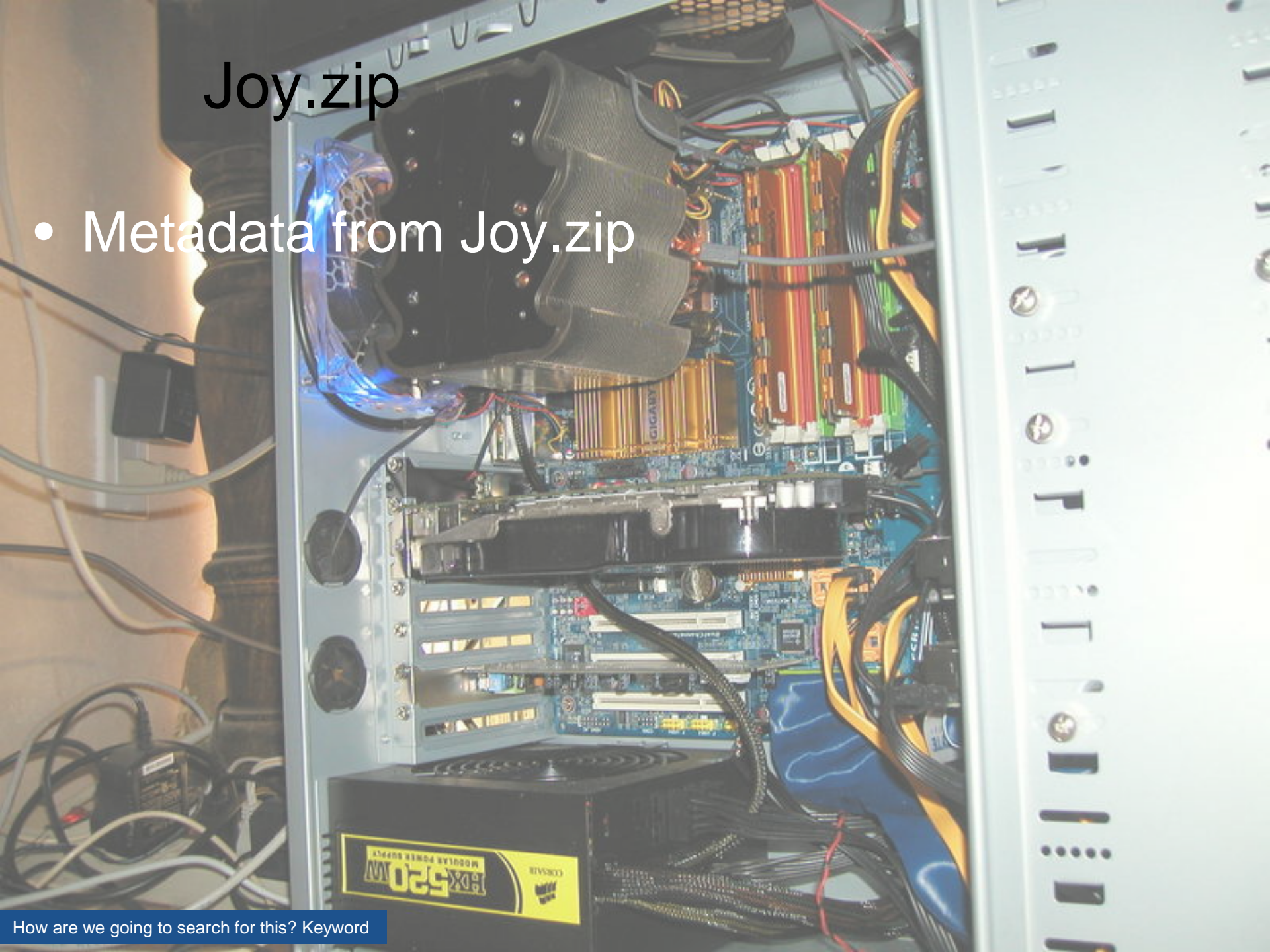
[03:16:11 PM] Maryland: bring your digital camera, I have all the rest.

[03:16:19 PM] Peter: sweet

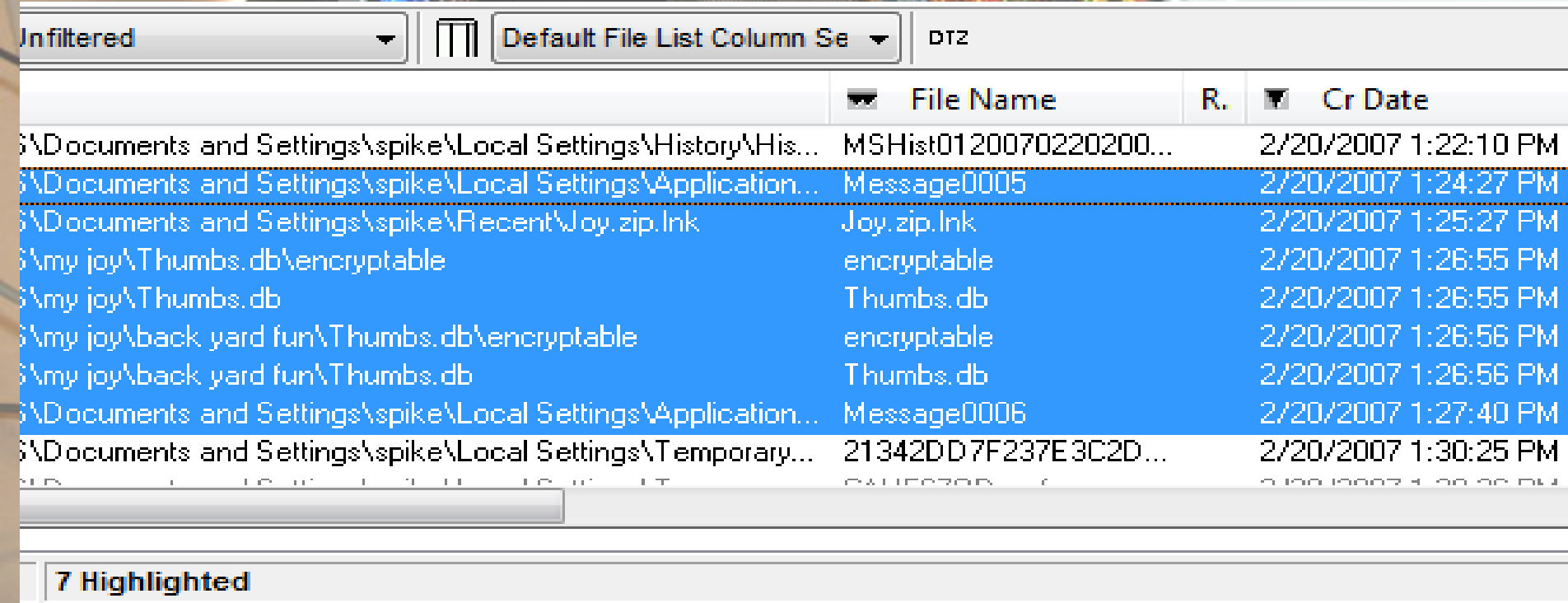
[03:16:25 PM] Peter: see ya at 2

Joy.zip

- Metadata from Joy.zip



Time Analysis



	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...	CA15670D...		2/20/2007 1:30:25 PM

7 Highlighted



Link File w/Thumb drive

Link File

AccessData FTK 1.70.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\F4P-Exercise 2-Analysis\PSwift\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Case

- PSwiftHD4FTK
 - Part_1
 - NONAME-NTFS
 - SBadClus
 - SExtend
 - S\$Secure
 - [unnamed]
 - Documents and Settings
 - my joy
 - Program Files
 - System Volume Information
 - WINDOWS
 - UnpartSpace

List all descendants

Shortcut File

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

Unfiltered Default File List Column Se DTZ

Full Path	File Name	R.	Cr Date	Mod Date
PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\History\His...	index.dat		2/20/2007 1:22:10 PM	2/20/2007 1:22:10 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\History\His...	index.dat		2/20/2007 1:22:10 PM	2/15/2007 3:09:46 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\History\His...	MSHist0120070212200...		2/20/2007 1:22:10 PM	2/12/2007 3:35:29 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\History\His...	MSHist0120070220200...		2/20/2007 1:22:10 PM	2/12/2007 3:35:29 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Local Settings\Application...	Message0005		2/20/2007 1:24:27 PM	2/21/2007 7:28:26 AM
PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Recent\Joy.zip.lnk	Joy.zip.lnk		2/20/2007 1:25:27 PM	2/20/2007 1:32:02 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\my joy\Thumbs.db\encryptable	encryptable		2/20/2007 1:26:55 PM	2/12/2007 2:39:37 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\my joy\Thumbs.db	Thumbs.db		2/20/2007 1:26:55 PM	2/12/2007 2:39:37 PM
PSwiftHD4FTK\Part_1\NONAME-NTFS\my joy\back yard fun\Thumbs.db\encryptable	encryptable		2/20/2007 1:26:56 PM	2/12/2007 2:39:36 PM

Log file c:\my joy\joy.zip

PSwiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\Recent\Joy.zip.lnk

What does this tell us?

AccessData FTK 1.70.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\FTK Exercise 2-Analysis\PSwift\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search Live Search

Search Term: Add Import Options


Indexed Words	Co...	Search Items	Hits	Files

Edit Item Remove Item Remove All View Item Results >

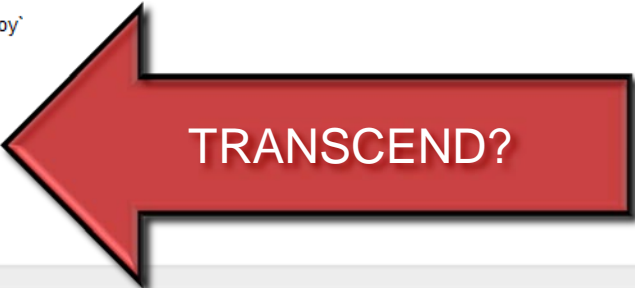
Cumulative operator: View Cumulative Results >

16 Hits - [LogFile] PswiftHD4FTK\Part_1\NONAME-NTFS\LogFile

```
></a><td width\u003d7><td><b><<Joy>>.zip</b><br>103K <a href \u003d\"/mail/?attid\u003d0.1&disp\u003datted&view\u003d
><td width\u003d7><td><b>Joy.<<zip>></b><br>103K <a href \u003d\"/mail/?attid\u003d0.1&disp\u003datted&view\u003d
Joy.Ink *RCRD( FILE0 Joy.Ink <<Joy>>.zip.Ink JOYZIP~1.LNK FILE0 Joy.zip.Ink0 JOYZIP~1.L *RCRD( LARams-LetsRamIt.Ink LARAMS
Ink *RCRD( FILE0 Joy.Ink Joy.<<zip>>.Ink JOYZIP~1.LNK FILE0 Joy.zip.Ink0 JOYZIP~1.L *RCRD( LARams-LetsRamIt.Ink LARAMS~1.L
y.zip.Ink JOYZIP~1.LNK FILE0 <<Joy>>.zip.Ink0 JOYZIP~1.L *RCRD( LARams-LetsRamIt.Ink LARAMS~1.LNK FILE0 LARAMS~1.LNK;
p.Ink JOYZIP~1.LNK FILE0 Joy.<<zip>>.Ink0 JOYZIP~1.L *RCRD( LARams-LetsRamIt.Ink LARAMS~1.LNK FILE0 LARAMS~1.LNKamI
Ink *RCRD( my joy.InkN INDX( <<Joy>>.zip.Ink JOYZIP~1.LNK LARams-LetsRamIt.Ink LARAMS~1.LNK mdhosebag@hotmail.com
*RCRD( my joy.InkN INDX( Joy.<<zip>>.Ink JOYZIP~1.LNK LARams-LetsRamIt.Ink LARAMS~1.LNK mdhosebag@hotmail.com.bt
oy.InkN MYCHAT~1.LNK Joy.Ink <<Joy>>.zip.Ink JOYZIP~1.LNK LARams-LetsRamIt.Ink LARAMS~1.LNK mdhosebag@hotmail.co
nkN MYCHAT~1.LNK Joy.Ink <<zip>>.Ink JOYZIP~1.LNK LARams-LetsRamIt.Ink LARAMS~1.LNK mdhosebag@hotmail.com.t
joy.InkN MYCHAT~1.LNK Joy.Ink <<zip>>.zip Joy.zip TRANSCEND E:\Joy.zip LGFM<Q spike MYCHAT~1 z06p My Chat Logs C:\Do
Joy spanky-home *RCRD( Joy.<<zip>> Joy.zip TRANSCEND E:\Joy.zip LGFM<Q spike MYCHAT~1 z06p My Chat Logs C:\Docurr
spanky-home *RCRD( Joy.zip <<Joy>>.zip TRANSCEND E:\Joy.zip LGFM<Q spike MYCHAT~1 z06p My Chat Logs C:\Document:
anky-home *RCRD( Joy.zip Joy.<<zip>> TRANSCEND E:\Joy.zip LGFM<Q spike MYCHAT~1 z06p My Chat Logs C:\Documents an
Joy.zip Joy.zip TRANSCEND E:\<<Joy>>.zip LGFM<Q spike MYCHAT~1 z06p My Chat Logs C:\Documents and Settings\spike\My
```



U63cU63c
C:\my joy\Joy
..\..\my joy\Joy
spanky-home
*RCRD(
Joy.zip
Joy.zip
TRANSCEND
E:\Joy.zip
LGFM<Q
spike
MYCHAT~1



TRANSCEND?

File Name	Full Path	Cr Date	Acc Date	Mod Date	Recycl...	Ext	File Type
LogFile	PswiftHD4FTK\Part_1\NONAME-NTFS\LogFile	2/12/2007 12:54:37 ...	2/12/2007 12:54:37 ...	2/12/2007 12:54:37 ...			Unknown Fil...
MFT	PswiftHD4FTK\Part_1\NONAME-NTFS\MFT	2/12/2007 12:54:37 ...	2/12/2007 12:54:37 ...	2/12/2007 12:54:37 ...			Unknown Fil...

20 Listed 1 Checked Total PswiftHD4FTK\Part_1\NONAME-NTFS\LogFile

What is TRANSCEND - Google

What is "Transcend"?



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?LangNo=0&Func1No=7&Func2No=114 - 49k -

[Cached](#) - [Similar pages](#) - [Note this](#)

[Welcome to Transcend Website - Contact Us](#)

Worldwide Office, Contact Sales, Contact TechSupport, Global Partners, Send Resume, Where to buy.

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/showvend.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 - 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

Google is Your Friend

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

http://www.transcendusa.com/Products/CatList.asp?FldNo=3&LangNo=0&Fu

File Edit View Favorites Tools Help

Welcome to Transcend Website - JetFlash™ M,Jet...


Transcend Search

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 HDD
Multimedia Products
Accessories
IDE Flash Disk
Certifications

Home>Products>USB Flash Drive>USB Flash Drive

USB Drive



JetFlash™ T2K

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

Click on Images Tab

Internet | Protected Mode: On 100%

Google is Your Friend (Images)



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

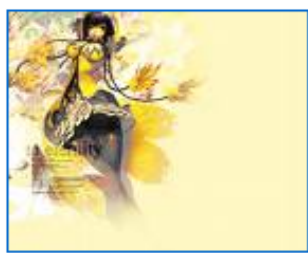
Transcend

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 rotation
GIVE ...
750 x 600 - 95k - jpg
[music.trabia-garden.net](#)



transcend
600 x 458 - 85k - jpg
[www.ueberflaechen.de](#)



About Transcend:
406 x 616 - 176k - gif
[www.transcend.ws](#)



TRAVEL & CHANGE
500 x 320 - 32k - jpg
[www.transcend.ws](#)
[\[More from www.transcend.ws \]](#)



transcend.jpg
600 x 900 - 82k - jpg
[jeltowns.com](#)



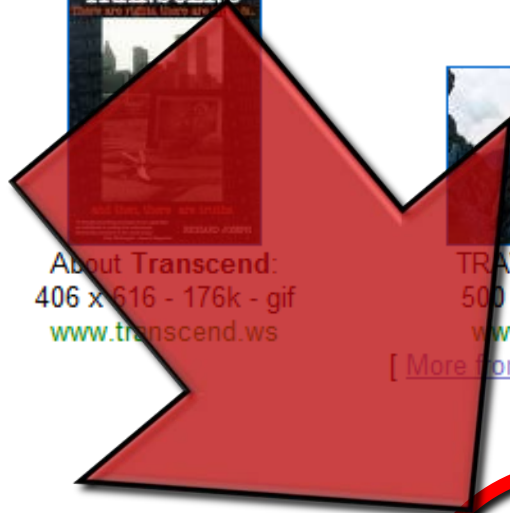
big-Transcend T.Sonic 610
512Mb .jpg ...
200 x 223 - 11k - jpg



big-Transcend T.Sonic 610 256
Mb ...
260 x 180 - 11k - jpg



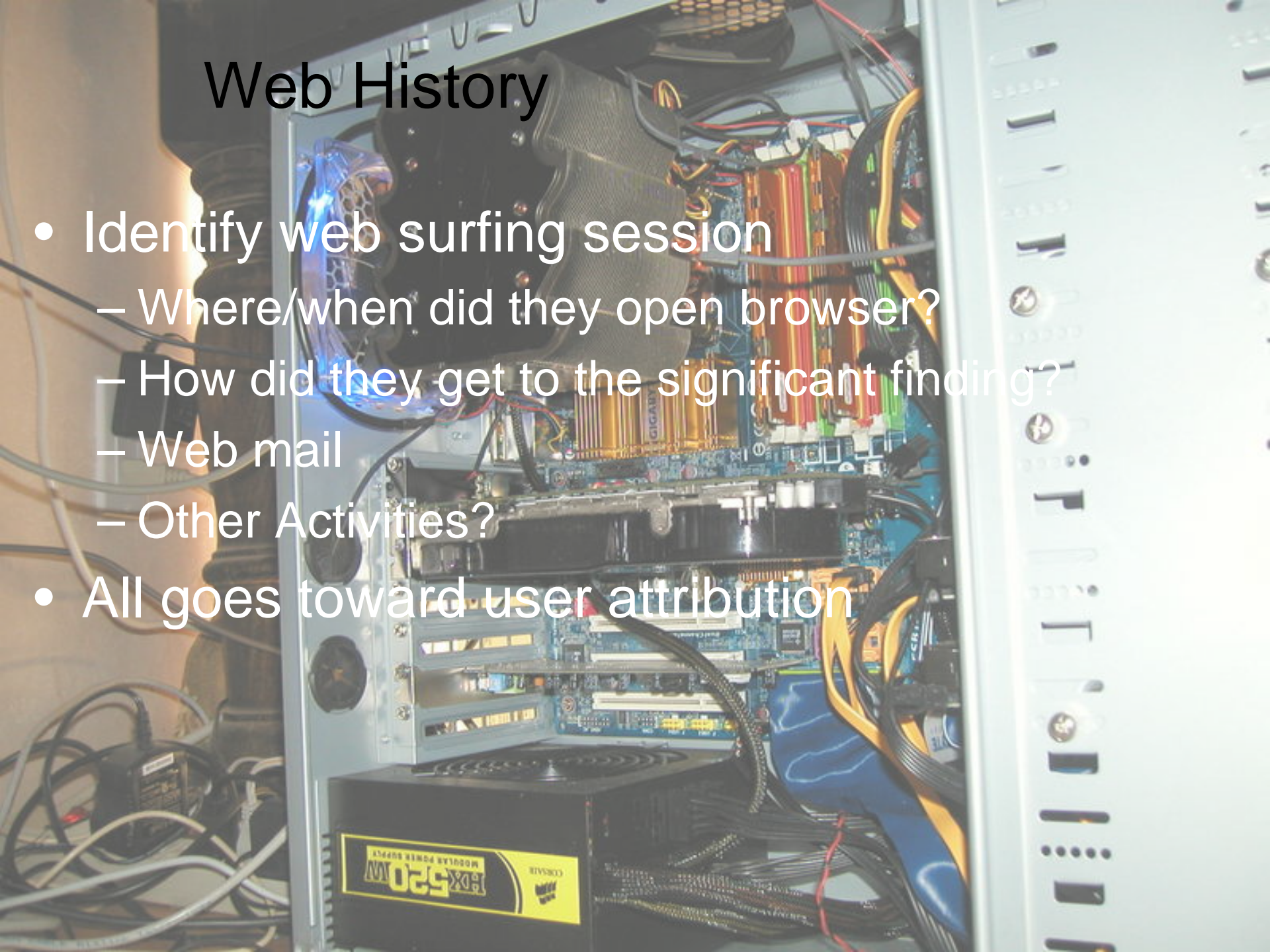
Nov 24: Transcend USB Disk
Drive
251 x 189 - 4k - jpg



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
- Case agents must work closely with examiners
- Forensic examiners must look beyond the “Single File”
- Metadata can be critical to establishing user attribution
- Even if evidence itself has been deleted/destroyed, numerous artifacts can be found

