



Accretive Solutions <sup>as</sup>

as promised

as expected

as delivered

# Digital Forensics

## Friend and Foe

October 8, 2009

## Background – A few Definitions: Digital Forensics

- Wikipedia – a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums.
- Wiktionary – the analysis of digital media to detect forgery or manipulation.
- NetworkDictionary – a field of science of applying digital technologies to legal questions arising from criminal investigations.
- TelecomDictionary – the ability to identify and/or measure information related to the use, operation or actions of a digital media object or service by a company, system, or person.

**It serves more than just Legal / Criminal purposes**

# Background – Application of Digital Forensics

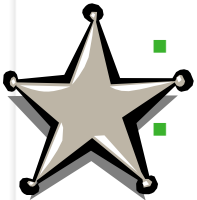
- **Legal**

- eDiscovery
- Litigation Support



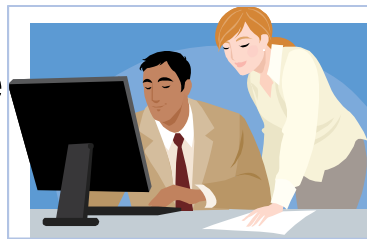
- **Criminal** (FBI, USSS, PD)

- Hacking
- Child Pornography
- Cyber Bullying
- Terrorism
- Homicide



- **Corporate**

- Acceptable Use
- Data Recovery



- **Research & Development**

- Troubleshooting
- Modeling
- Reverse Engineering



- **Personal**

- Activity Monitoring
- Data Recovery
- Anti-Virus / Spyware



***It's ALL about the DATA!***

## Background – Mike-a-pedia Definition ...and a quandary.

- Digital Forensics – Tools and techniques to acquire, preserve, and examine data on or transmitted by digital devices.



- What would Digital Forensics be... without appealing data, the smoking gun, or verifiable results?
- What types of data are appealing? Where is it found?



# Technology Enablers

Enabling us & Giving “them” appealing data

## Personal

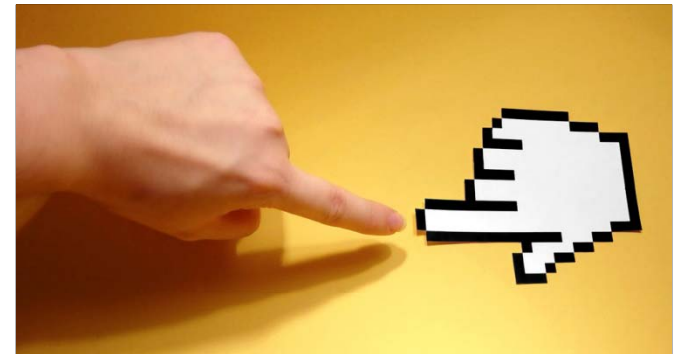
- Cell Phones
- VoIP Phone
- DVR, Cable, SAT
- Computers
- iPhones / iPod
- Traffic Camera
- Toll Tag
- Smart Cards
- Digital Camera
- Digital Video

## Corporate

- Camera Systems
- Laptops / PDA
- Backup Tapes
- Print Servers
- Systems (ERP)
- Badge Access
- BlackBerry
- VoIP Phone
- File Servers

## National

- SCADA
- Computers
- Laptops
- BlackBerrys



Accretive Solutions <sup>as</sup>

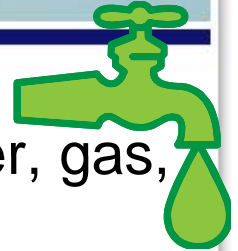
# Technology Enablers

Using stored data to make life “better” for us

- Caller ID & Redial
- Call Detail Records
- Internet Bookmarks
- Saved passwords
- Scheduled recordings
- Digitized photos & video
- No slowing down for Tolls
- Better timing at Lights
- Less information to remember
- GPS and Remembered Addresses
- Email and Internet in our palm
- Easy facility access without keys
- Mass storage of data
- Shared computing and printing



- Automated delivery / management of water, gas, power
- Remote surveillance
- Force Multiplier
- Telecommuting
- Parking with TollTag
- Portability
- Social iNetworking
- On-board Car Computer



Accretive Solutions <sup>as</sup>

# Friend or Foe

## Using stored data for us & against us

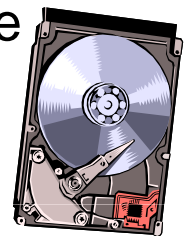
- Lost Laptop or Tape = Stolen ID, IP, CC, NS
- Speeding Ticket
- Red light Ticket
- Facial Recognition
- Internet History
- File Copies / IP Theft
- Developing a Personal Profile
- Transaction Records
- Successful Phishing
- Social Engineering
- Printer Logs



http://



- Deleting files doesn't mean they're deleted
- Knowing where I've been (gps, iphone, car)
- Knowing who I called / texted
- Finding the pictures / video I deleted
- Cached Web camera data
- External HDD use
- Pirated software
- Stenography
- Fraud detection



AS  
Accretive Solutions

# Friend or Foe

## Hypothetical Examples

- Example 1
  - The virus originated within our network. Using digital forensics, we assessed suspect workstations and found the initially infected computer and determined that the virus was created by a contractor.
- Example 2
  - Terrorist planning to meet a hostile arms dealer on a certain date, at a certain time. OIW officers forensically acquire said data from the terrorist's smartphone and subsequently modify the planned exchange time from 1pm to 2pm. As a result, the arms dealer doesn't get paid and the terrorist becomes a worriest.
- Example 3
  - The CEO's laptop falls from the Ivory Tower and breaks, physical devices no longer function. Digital forensic techniques are employed to recover the CEO's all important Solitaire High Score from the now dormant HDD
- Example 4
  - Test aircraft crashes into 100 million pieces. Digital forensics techniques are used to recreate the magnetic residue of the memory within the black box to obtain flight data and research root cause.

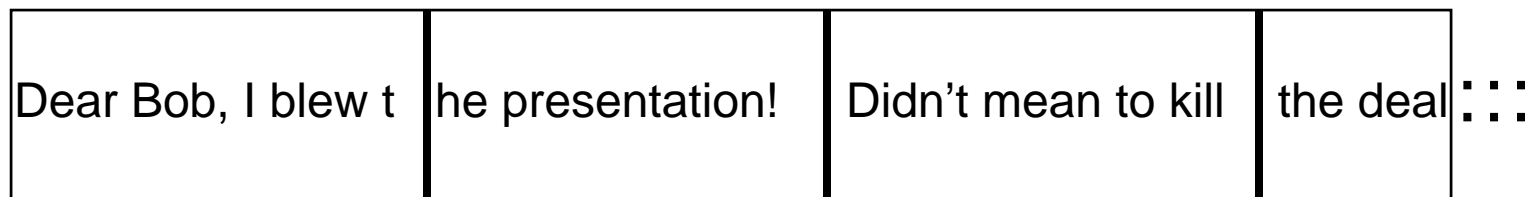
# Deleting does not mean Deleted !

- “Deleted” information, on almost any kind of digital storage media, is almost never completely gone...
- Simply deleting files doesn't securely delete them
  - Deleted files & deletion date/time can be recovered
- Renaming files to avoid detection doesn't work
- Formatting disks doesn't delete much data
- Web-based email can be (partially) recovered directly from a computer
- Files transferred over a network can be reassembled and used as evidence

# Deleting does not mean Deleted !

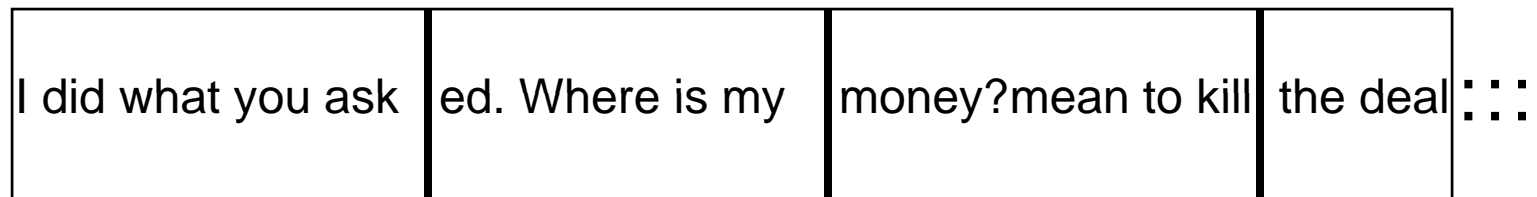
## A Disk Layer Example

BOSS.TXT: "Dear Bob, I blew the presentation! Didn't mean to kill the deal"



<< file is deleted and storage is reallocated >>

Espionage.TXT: "I did what you asked. Where is my money?"



# Finding Data with AccessData's Forensic Tool Kit! Screenshots from FTK

The screenshot displays the FTK software interface. At the top, there is a menu bar with options: File, Edit, View, Evidence, Filter, Tools, and Help. Below the menu bar, there is a filter dropdown set to '-unfiltered-' and a 'Define...' button. A toolbar contains several icons for navigation and search. Below the toolbar, there are tabs for 'Explore', 'Overview', 'Email', 'Graphics', 'Bookmarks', 'Live Search', 'Index Search', and 'Volatile'. The 'Index Search' tab is active, showing a window titled 'dtSearch@ Index'. The window is divided into two main sections: 'Terms' and 'Search Criteria'. The 'Terms' section contains a table of indexed words and their total hits. The 'Search Criteria' section shows the search operator set to 'And' and the search terms set to 'spencer'. The search results table shows 13545 hits for the term 'spencer'. On the right side of the search results, there are buttons for 'Clear', 'Export...', 'Export...', 'Options...', and 'Search Now'.

Indexed Words	Total Hits
spencble	67
spencbleq	1
spence	2610
spenceb	4
spencem	1
spencen	1
spenceq	10
spencer	13545

Search Terms	Total Hits
spencer	13545

Accretive Solutions

# Finding Data with AccessData's Forensic Tool Kit! Screenshots from FTK

The screenshot displays the 'File Content' window in FTK. The text is in 'Natural' view, showing a paragraph about a family's summer activities. The word 'Spencer' is highlighted in blue, and 'Spencer' is highlighted in yellow in the second paragraph. Below the text is a 'File List' window showing a table of files.

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
2006 Meldrum Review.doc		64977	doc	Jern02.E01\NONAME [...]	Microso...	32.00 KB	28.50 KB	ABE12...	00A7B...	2E7375...	2/25/2007 10:0...	10/1/2008 10:0...	2/25/2007 10:0...
2006 Meldrum Review.doc		617358	doc	Jern02.E01\NONAME [...]	Microso...	n/a	35.11 KB	02F20...	82A9D...	34FB13...	2/25/2007 10:0...	n/a	2/25/2007 10:0...
2007 Gators 4-001 (129...		825259	html	Jern02.E01\NONAME [...]	HTML	n/a	n/a				n/a	n/a	n/a
2007 Gators 4-001 (129...		383118	jpg	Jern02.E01\NONAME [...]	JPEG E...	n/a	2776 KB	FD10...	2E9526...	AF069...	n/a	n/a	n/a
2007 Meldrum family 2....		671233	snappf...	Jern02.E01\NONAME [...]	Unknown	n/a	19.16 KB	4B57E...	149389...	9EDFE...	2/4/2008 11:45...	n/a	2/5/2008 2:06...
2007 Meldrum Review.doc		64978	doc	Jern02.E01\NONAME [...]	Microso...	36.00 KB	35.00 KB	D3073...	ABF4A...	E926C...	2/1/2008 11:19...	10/22/2008 1:2...	2/5/2008 2:10...
2007 Meldrum Review.doc		671234	doc	Jern02.E01\NONAME [...]	Microso...	n/a	41.61 KB	8886F...	9EB714...	2EFD5...	2/1/2008 11:19...	n/a	2/5/2008 2:15...
2008 Meldrum family re...		64985	doc	Jern02.E01\NONAME [...]	Microso...	36.00 KB	35.50 KB	7908F...	23E041...	7AAC4...	3/10/2009 4:13...	3/10/2009 11:3...	3/10/2009 11:3...
2008 Meldrum family re...		389801	doc	Jern02.E01\NONAME [...]	Microso...	n/a	41.63 KB	2C52E...	E8518E...	488560...	3/10/2009 4:13...	n/a	3/10/2009 11:3...
2008 Meldrum family re...		398262	doc	Jern02.E01\NONAME [...]	Microso...	n/a	41.63 KB	2C52E...	E8518E...	488560...	3/10/2009 4:13...	n/a	3/10/2009 11:3...
200821026		158100		Jern02.E01\NONAME [...]	Unalloc	6794.0B	6794.0B				n/a	n/a	n/a

Summary: Loaded: 2,832 | Filtered: 2,832 | Total: 2,832 | Highlighted: 1 | Checked: 0

# Finding Data with AccessData's Forensic Tool Kit! Screenshots from FTK

The screenshot displays the AccessData's Forensic Tool Kit (FTK) interface. At the top, there are navigation tabs: Explore, Overview, Email, Graphics, Bookmarks, Live Search, Index Search, and Volatile. Below these is a 'Thumbnails' section showing a grid of image thumbnails. One thumbnail is highlighted with a yellow border. Below the thumbnails, there are statistics: Loaded: 44,259, Filtered: 44,259, Total: 131,106, Highlighted: 1, Checked: 0, and a 'Show Tooltip' checkbox.

The 'Evidence Items' section shows a tree view of the file system structure, including folders like @BadClus, @Extend, @LogFile, @MFT, @Secure, and various files. The 'File Content' section shows a preview of a selected image file, with tabs for Hex, Text, Filtered, and Natural. Below this is a 'File List' section with a table of files.

Name	Label	Item #	Extension	Path	Category	P-Size	L-S...	MDS	SHA1	SHA256	Created	Accessed	Modified
IMG_0586.jpg		392720	jpg	Jenn02.E01,NO NAME [...]	JPEG E...	5954 KB	591887...	C7C12...	74D98...	n/a	n/a	n/a	n/a
IMG_0586.JPG		384304	jpg	Jenn02.E01,NO NAME [...]	JPEG E...	5954 KB	591887...	C7C12...	74D98...	n/a	n/a	n/a	n/a
IMG_0586.JPG		389628	jpg	Jenn02.E01,NO NAME [...]	JPEG E...	5958 KB	591887...	C7C12...	74D98...	2/26/2009 3:32...	n/a	2/26/2009 3:32...	2/26/2009 3:32...
IMG_0586.jpg		389660	jpg	Jenn02.E01,NO NAME [...]	JPEG E...	5958 KB	591887...	C7C12...	74D98...	2/26/2009 11:5...	n/a	2/26/2009 11:5...	2/26/2009 11:5...
IMG_0586.JPG		398089	jpg	Jenn02.E01,NO NAME [...]	JPEG E...	5958 KB	591887...	C7C12...	74D98...	2/26/2009 3:32...	n/a	2/26/2009 3:32...	2/26/2009 3:32...
IMG_0586.jpg		398121	jpg	Jenn02.E01,NO NAME [...]	JPEG E...	5958 KB	591887...	C7C12...	74D98...	2/26/2009 11:5...	n/a	2/26/2009 11:5...	2/26/2009 11:5...
image001.png		382966	png	Jenn02.E01,NO NAME [...]	PNG	14.63 MB	9C023...	49C80...	6FE73...	n/a	n/a	n/a	n/a

Accretive Solutions

# Destroying (physically) doesn't always mean Destroyed But here are a few good ways.



degausser

or



or



# Destroying (physically) doesn't always mean Destroyed ...and here are a few bad ways.



# Questions



Please Give Us Your Feedback!

**Accretive Solutions**<sup>as</sup>

**as** promised   **as** expected   **as** delivered

**Accretive Solutions**<sup>as</sup>