



STROZ FRIEDBERG

# Computer Forensics in Investigations and in Court

Presented to: The Center for Cybercrime Studies and The  
Center for Modern Forensic Practice, John Jay College of  
Criminal Justice (CUNY)

by Edward M. Stroz, Co-President, Stroz Friedberg

November 11, 2009

## WHAT WE DO

# Consulting and Technical Services Specializing In:



**DIGITAL  
FORENSICS**



**ELECTRONIC  
DISCOVERY**



**DATA BREACH  
RESPONSE**



**RESPONSE TO  
ONLINE FRAUD  
AND ABUSE**



**INVESTIGATIONS**

## OUR CLIENTS

- 8 of the Fortune 10 Companies
- 72 of the Top 100 US Law Firms (AmLaw 100)
- 16 of the Top 20 UK Law Firms

## LEADING U.S. WORK

MARTHA STEWART  
SECURITIES FRAUD CASE



FTC BOGUS ANTI-SPYWARE  
CASES



ENRON  
BARGE TRIAL



AMD v. INTEL



ATTY GEN'L TASK FORCE  
TJX DATA BREACH

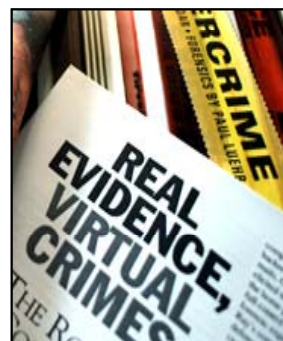
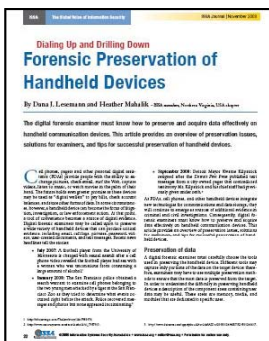


MADOFF MONITOR



# INDUSTRY LEADERSHIP

- Sedona Conference, Working Group1: Electronic Discovery
- New York State Bar Association: Electronic Discovery Committee
- Minnesota Bar Association: Computer Law Section
- American Bar Association Cybercrime Law Committee
- Digital Forensics and Cybercrime Textbook Writers
- Widely Published in Digital Forensics, E-Discovery, and Cybercrime journals
- Speaking Engagements: Sedona, ABA, IQPC, PLI, ISC2, IAPP, FTC, et al.



## DIGITAL FORENSICS - CASES

- **Theft of trade secrets**
- **Other job disputes (threats, discrimination)**
- **Data breaches**
- **Fraud investigations (SEC, FCPA)**
- **Patent infringement**
- **Trademark infringement**
- **E-discovery (spoliation claims, preservation)**

# Forensic Targets

- **Workplace Computers**
- **Home Computers**
- **Storage Devices**
  - (DVDs, CDs, flash drives)
- **Blackberries, PDA's,**
- **Cell Phones**
- **Digital Cameras**
- **Printers and Digital Faxes**
- **Servers (FTP, Web, E-mail, File)**
- **Web pages**



## Other Digital Sources



Video surveillance



Key cards

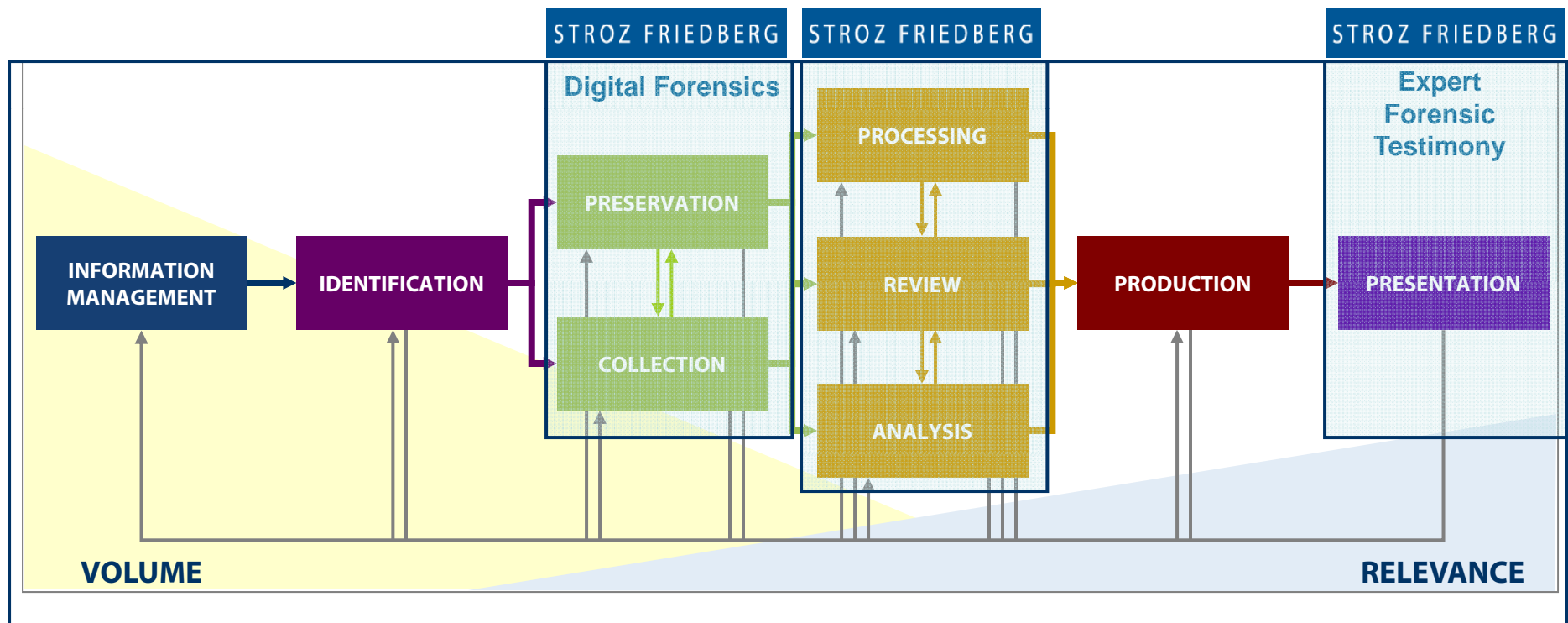


Key loggers

52	54.234482	34.851848	192.168.0.2
53	54.235272	0.000790	192.168.0.10
54	58.137063	3.901791	192.168.0.10
55	58.137176	0.000113	192.168.0.2

Packet Sniffers

# FORENSICS IN E-DISCOVERY



STROZ FRIEDBERG

Consulting, Strategic Planning and Comprehensive Project Management

## MAIN DISPLAY SCREEN Guided Search

The screenshot shows the Stroz Review software interface with the following callouts:

- Bring selected document(s) to the Document Review Screen.** (Callout to the 'View Original Document' button)
- Open the selected document using its native application.** (Callout to the 'Open' button)
- Open query building form to build complex queries.** (Callout to the 'Advanced Search' tab)
- Specify which part of the document to query against.** (Callout to the 'Body and/Attachments' dropdown)
- Search documents for matches within their addressee fields.** (Callout to the 'Address' field)
- Search Action Buttons.** (Callout to the 'Search', 'Save', 'Load', 'Clear' buttons)
- Specify sort criteria for search results.** (Callout to the 'Order By' dropdown)
- Restrict search results to those matching certain Document Review criteria.** (Callout to the 'Exclude Reviewed' and 'Combine/Reset Sets' buttons)
- Exclude previously reviewed documents from search results and folder views.** (Callout to the 'Exclude Reviewed' button)
- Access tools for managing multiple sets of documents.** (Callout to the 'Combine/Reset Sets' button)
- Document Grid - Each row represents a single document, and each column represents a specific piece of metadata. Distinct document sets are organized by tabs.** (Callout to the document grid)
- View an HTML representation of the selected document.** (Callout to the 'What is Text Mining?' HTML view)
- View document metadata, organized by type.** (Callout to the 'Document Metadata' pane)
- Folder Navigation Tree - displays folders and subfolders.** (Callout to the left-hand navigation tree)
- Narrow search results to Outlook/Lotus Notes items, docs created within a specified time period, and/or doc sets.** (Callout to the 'Document Date' and 'From' fields)
- Search for documents that match words and phrases entered into this field.** (Callout to the 'Find documents' search box)
- Search for documents that match key metadata terms.** (Callout to the 'Advanced Search' fields)

The complete Stroz Review Manual provides greater detail than this Quick Reference Guide. Access the Manual by clicking on Help on the Menu Bar and choose *Launch Stroz Review Manual* from the menu.

## REVIEW SCREEN

**Document Navigation Tree** - View a list of documents you have selected for review. Document sets can be grouped by *Document Set*, *Document Families*, *Exact Duplicates*, or *Email Threads*.

Indicates which document is currently selected.

Highlight search terms within the body of the document.

Select HTML, Text, or Image-based representations of the selected document.

Browse documents in the navigation tree.

Open the selected document using its native application.

**Image Manipulation Buttons** - Rotate, zoom in/out, save, or print the current page.

**Document Information Panel** - View data about the selected document in three tabs: Metadata, Doc Family, and Email Thread.

Page Navigation Buttons.

Indicates whether or not the selected document has been reviewed and/or produced.

Highlight, obscure, or otherwise call attention to selected sections of a page.

**Document Viewing Panel** - View an Image, HTML, or Plain Text representation of the selected document.

**Tagging Panel** - Contains issue and characteristic tags used to review your documents.

**Document Commenting Panel** - Contains additional document review tools, including document blog, review comments, and escalation to 2nd level review.

Allows you to save your document tag selections.

### How to Tag Your Documents in the Document Review Screen

- 1) To add tags to your documents, you must first select one or more documents in the **Document Navigation Tree** by clicking on the boxes adjacent to the documents you wish to select.
- 2) Select one or more issue tags from the **Tagging Panel** by clicking on the boxes adjacent to the desired tags.
- 3) Tag selections will be applied to your document(s) when you click one of the Save buttons.



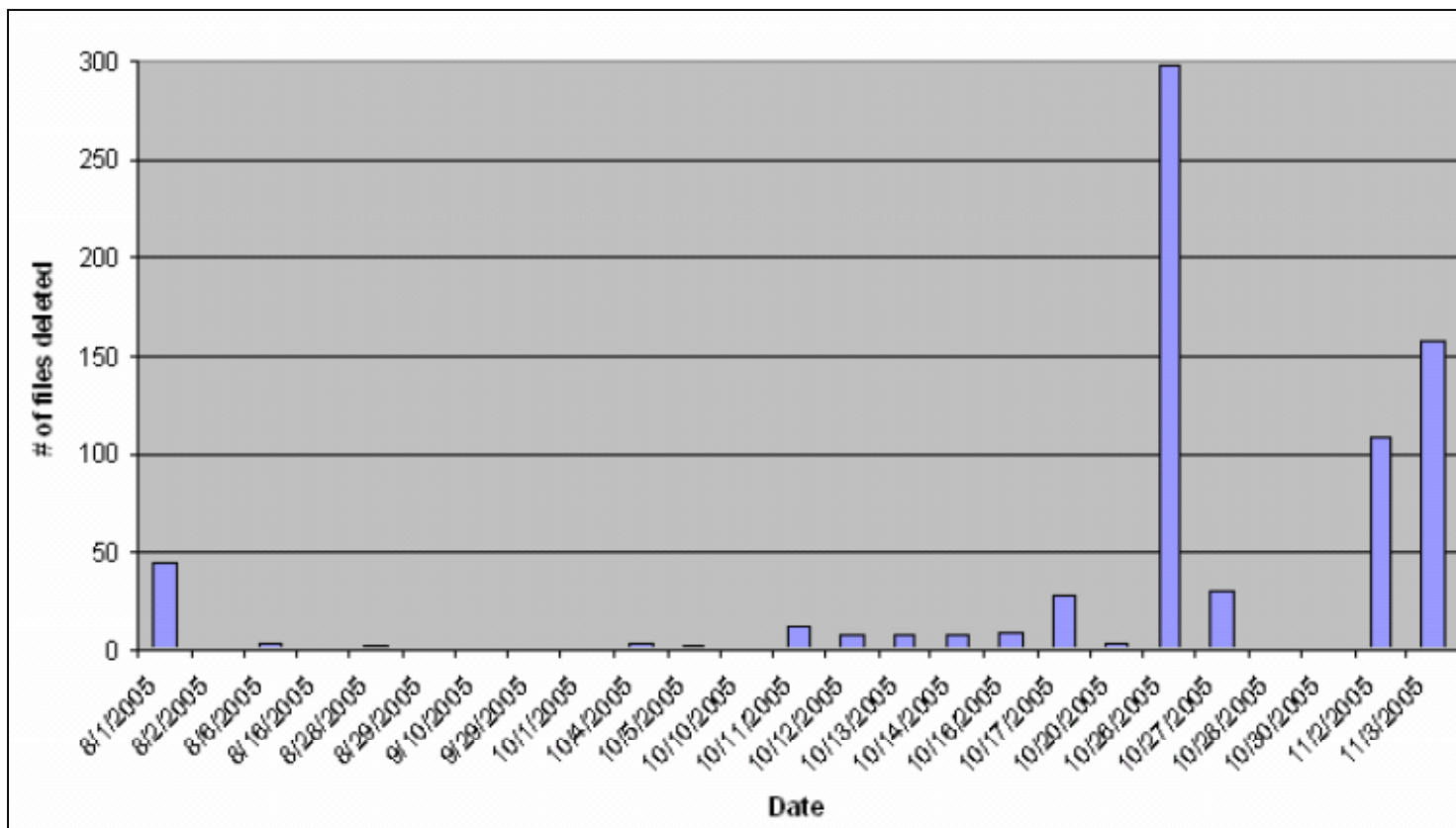
The complete Stroz Review Manual provides greater detail than this Quick Reference Guide. Access the Manual by clicking on Help on the Menu Bar and choose *Launch Stroz Review Manual* from the menu.

## AVAILABLE EVIDENCE

- **Hard Drives**
  - Deletion Activity (“deleted” or partial files, wiping activity)
  - Internet and Search History (surfing and webmail activity)
  - System Activity (logins, files printed, devices inserted)
  - Metadata (“modified” “created” “accessed” dates, “authors”)
  - Removable Devices (thumb drives, DVD’s)
  - Link Files (access to files on and off the hard drive)
  - Matching Files (exact copies and near-duplicates)
- **CDs and DVDs**
  - Burn programs and dates

- **Cell Phones**
  - Contacts and last numbers dialed
  - Saved files/photos
  - Email, text messages
- **Web Sites**
  - Offline, surfable copies of web site
  - Source code
  - Dynamic surfing or packet activity
- **Email**
  - Psycho-linguistic patterns

# DELETION ACTIVITY



# INTERNET HISTORY

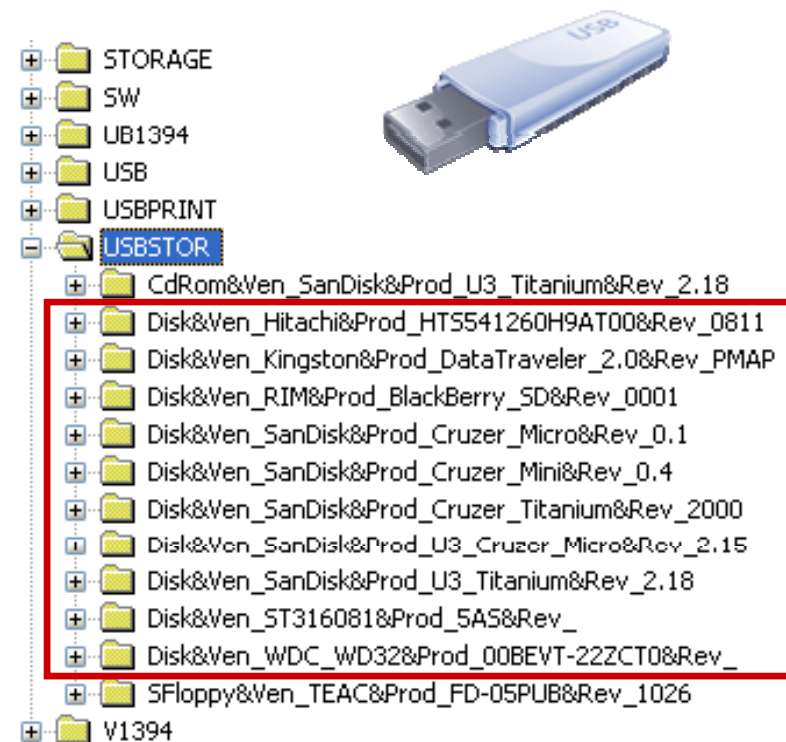
- Find webmail accounts such as Gmail or Hotmail
- Locate suspicious or inappropriate Internet activity (i.e. visiting competitors' websites, pornography, etc.)

http://lw15fd.law15.hotmail.msn.com/cgi-bin/premail/4173			
http://lw15fd.law15.hotmail.msn.com/cgi-bin/getmsg?curmbox=F0000000			
http://lw15fd.law15.hotmail.msn.com/cgi-bin/hmhome?curmbox=F0000000			
:Host: 64.4.22.23			
:Host: www.reliaquote.com			
http://lw15fd.law15.hotmail.msn.com/cgi-bin/HoTMaiL?curmbox=F0000000			
http://www.yahoo.com/r/mp			
http://64.4.22.23//redirlog/hmhinbox?url=http%3a%2f%2flw15fd%2elaw1			
http://maps.yahoo.com/py/maps.py?Pyt=Tmap&addr=3400+Internationa			
<u>http://maps.yahoo.com/py/maps.py?Pyt=Tmap&amp;addr=3400+Internationa</u>			



## REMOVABLE DEVICES

- **Traces of past devices can be uncovered with forensic analysis.**
- **The make and model of a thumb drive can often be found.**
- **The date and time when a device was first connected and last connected can be determined.**
- **Mass copying can often be determined by correlating the device connection with numerous files bearing the same last access times.**



## LINK FILES

- Provide data on files now missing or outside the hard drive.
- Proprietary tool created by Stroz Friedberg allows us to quickly and efficiently view the contents of link files

Name:	Burgundy PR UK 2006 v2.DOC.lnk
File Ext:	lnk
File Type:	Link
File Category:	Windows
Description:	File, Archive
Last Accessed:	05/03/07 09:11:14AM
File Created:	08/29/06 03:03:16PM
Last Written:	08/29/06 03:04:08PM
Entry Modified:	08/29/06 03:04:08PM
File Acquired:	05/21/07 06:38:35PM
Starting Extent:	0C-C1880790,448
File Extents:	1
Permissions:	•
References:	0
Physical Location:	7,703,748,544
Physical Sector:	15,046,383
Evidence File:	karachi_laptop
File Identifier:	17448
Full Path:	C:\Documents and Settings\hnaseem_olad\Recent\Burgundy PR UK 2006 v2.DOC.lnk
Short Name:	BURGUNDY_1.LNK

Link file shows this document was accessed...

On a particular date and time...

And where the file was located.

- [Exhaust](#)
- [Front](#)
- [Gas Turbine](#)
- [Heater](#)
- [Lighting](#)
- [Mirror](#)
- [Seats](#)
- [New Parts](#)
- [Information](#)
- [Material](#)
- [Data](#)
- [Products](#)
- [Customer](#)
- [Order](#)

```
Union City Stepvan Parts and Panels.htm - Notepad
File Edit Format View Help

src="Union City Stepvan Parts and Panels_files/home_button.gif" width=60
border=0></A><FONT color=#9999cc>..<A
onclick="Newwindow(this.href);return false;"
href="http://www.rustrepair.com/app2/onlinecat.htm?p=wi" target=_self><IMG
height=24 alt="stepvan store"
src="Union City Stepvan Parts and Panels_files/onlinestore_button.gif"
width=98 border=0></A>..<A
href="http://www.walkinvan.com/stepvan_index_p1.htm" target=_self><IMG
height=24 alt="stepvan index"
src="Union City Stepvan Parts and Panels_files/stepvan_index_p1.gif"
border=0></A></FONT></FONT>
<P align=center></FONT>
<FORM>
<DIV align=center></FORM>
<FORM><!--Label this button VALUE to f
type=button value="Read Disclaimer" name=But
</FORM>
<P align=left><FONT color=#ffffff3 size=
now, buy union city body stepvan parts
parts now.<BR>new union city body stepvan parts today, get union city body
stepvan parts now, buy union city body stepvan parts
today.</FONT></P><FONT color=#9999cc size=2>
<P align=left> </P></FONT></DIV></TD></TR>
<TR></TR></TBODY></TABLE>
<TABLE cellpadding=0 width="100%" border=0>
<TBODY>
<TR>
<TD bgcolor=#0066ff>
<DIV align=center><FONT size=2>©2001 Mill supply, Inc. (All Material on
this page is copyright by Mill Supply, Inc. 2001)
<TABLE cellpadding=0 width=772 border=0>
<TBODY>
<TR>
<TD width=265><A
href="http://www.walkinvan.com/grumman_stepvan_p1.htm"><B><FONT
size=1>Grumman Olson</FONT></B></A></TD>
<TD width=292><A
```

**"FONT color=#ffffff3" changes font color to white (on white)**

**"FONT color=#9999cc" changes font color back to light blue**

ne of our bigger lines. Be

es them all. We have [Hupp](#),  
ls and fan blades. Mill



©2001 Mill Supply, Inc. (All Material on this page is copyright by Mill Supply, Inc. 2001)

- [Grumman Olson](#)
- [Beverlyton Body](#)
- [Supreme Body](#)
- [Ultimaster](#)
- [Kason Hardware](#)
- [Vehac Mixers](#)
- [Truck Lite](#)
- [Tedco & Whitfire Roll-up Doors](#)
- [Auto-Body Part Net](#)
- [Side Door Hardware](#)
- [Exhaust Systems](#)
- [Front End Parts](#)

# FORENSICS IN E-DISCOVERY - Auto-Coding

**Extracts text from the face of the document and organizes the information**

**Folder Tree (Left):**

- BOXNAME
  - 007-DOJ-AG [Doc No in Box: 1 of 102]
- DOCTYPE INFO
  - DOCTYPE
    - EDOC
  - T\_DOCTYPE
    - email
- DOCDATE INFO
  - DOCDATE
    - 2005/02/18
- T\_DOCDATE
  - 2005/02/18
- TITLE
  - DOJDocsPt1070003...
- T\_TITLE
  - RE: 2 AGAC items
- AUTHORS
  - AUTHOR
    - RENATA
  - T\_AUTHORNAME
    - Sampson, Kyle
- RECIPIENTS
  - T\_RECIPNAME
    - Mercer, Bill
- NAME MENTIONS
  - T\_EMAILADDRESS
    - Judy.Beeman2@usdoj.gov
  - T\_ORGANIZATION
    - Legislative Committee
  - T\_PERSON
    - Beeman, Judy
    - Gonzales
    - Mercer, Bill
    - Sampson, Kyle
    - Ullyot, Ted
- OTHER DATES INFO
  - T\_OTHER\_DATES
    - 2005/02/17
    - 2005/02/18
    - 2005/03/02

**Email Body (Right):**

Sampson, Kyle

From: Sampson, Kyle  
Sent: Friday, February 18, 2005 8:23 AM  
To: Mercer, Bill  
Subject: RE: 2 AGAC items

ok, good  
will look for recommendations from you on subcommittees

-----Original Message-----  
From: Mercer, Bill  
Sent: Thursday, February 17, 2005 10:41 PM  
To: Sampson, Kyle  
Subject: Re: 2 AGAC items

... have a conversation about the subcommittees.

... are doing well. I would like to add a Legislative to interact w/OLA and OLP. I would recommend termination of ... I don't see this as a core function at this ... we don't have much of a budget. I can't see the value in this one.

... migration (Iglesias):  
These are a mixed bag. Some are the least active and should get new ... constituted.

... as these decisions are made, I will let people know that now is the time to add/leave subcommittees.

-----Original Message-----  
From: Sampson, Kyle <Kyle.Sampson@USDOJ.gov>  
Sent: Thu Feb 17 17:24:56 2005  
Subject: 2 AGAC items

A couple of AGAC items:

- The Attorney General would like to have dinner with the AGAC on the evening of **Wednesday, March 2, 2005** beginning at approximately 6pm (or 6:30pm)? Could you all **SELECT a RESTAURANT and make reservations and add to the AGAC schedule of events?** Participants would be USAs, AG (and perhaps Mrs. Gonzales), me, and Ted Ullyot.
- The Attorney General would like to make the following appointments to the AGAC:  
New appointments (for terms expiring **12/31/2007**)



**May 14, 2009**

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Dear** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Sincerely,**

\_\_\_\_\_  
\_\_\_\_\_

**To:** \_\_\_\_\_  
**Sent:** 05/14/2009 8:32am  
**From:** \_\_\_\_\_  
**Subject:** \_\_\_\_\_

Hi \_\_\_\_\_

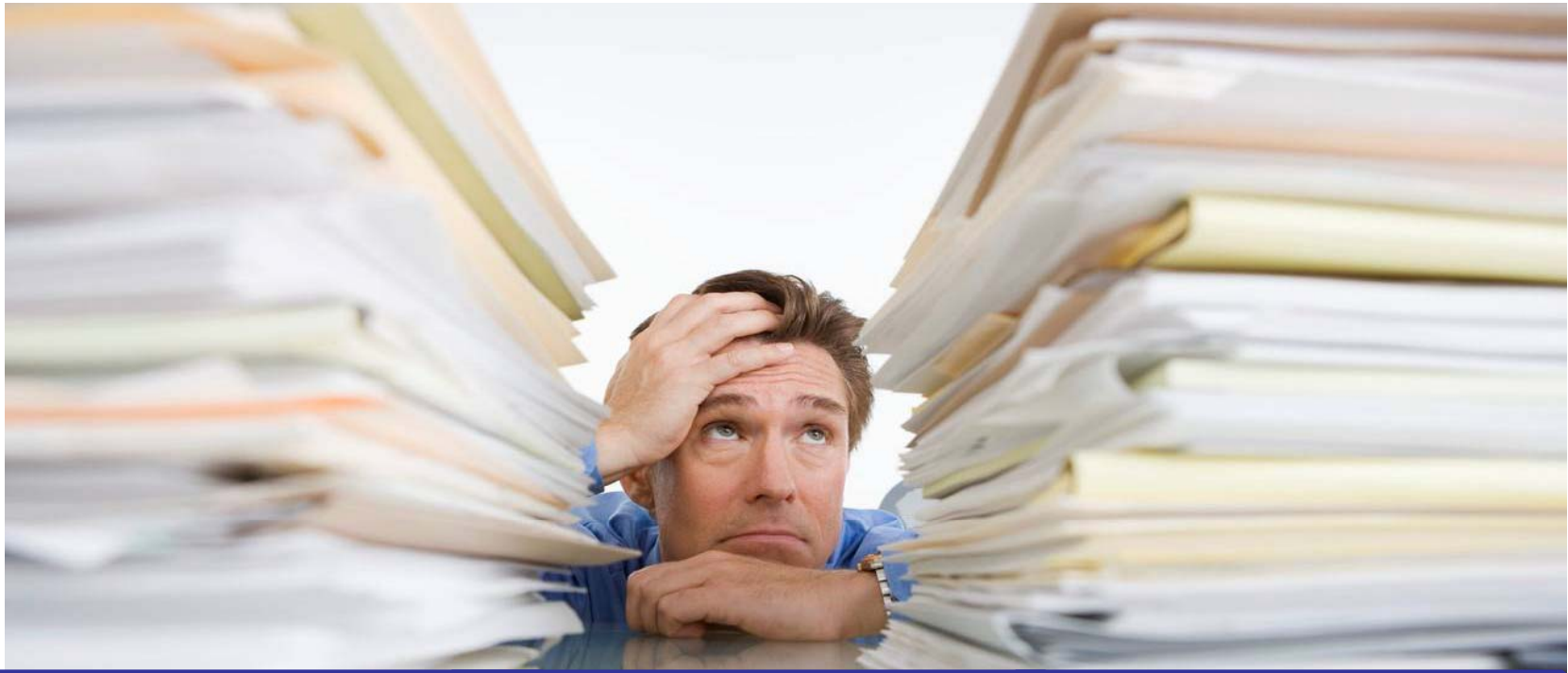
... original message ...

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Mapping data location within a particular document type shows real “author.”**

STROZ FRIEDBERG

## WORKS ON PAPER

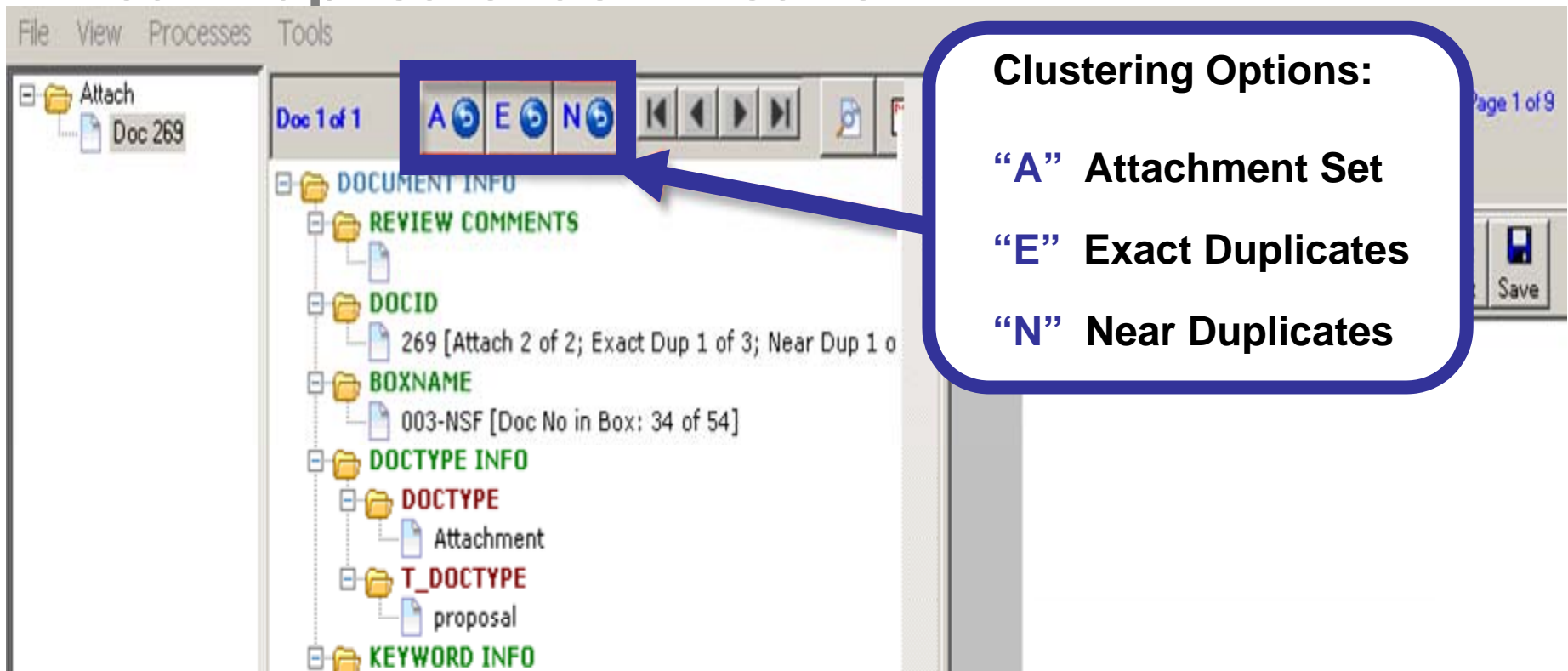


**PHASE I**  
**Enhanced OCR**

**PHASE II**  
**Intelligence**

**PHASE III**  
**Extract Results**

# FORENSICS IN E-DISCOVERY – Near Duplicate Identification

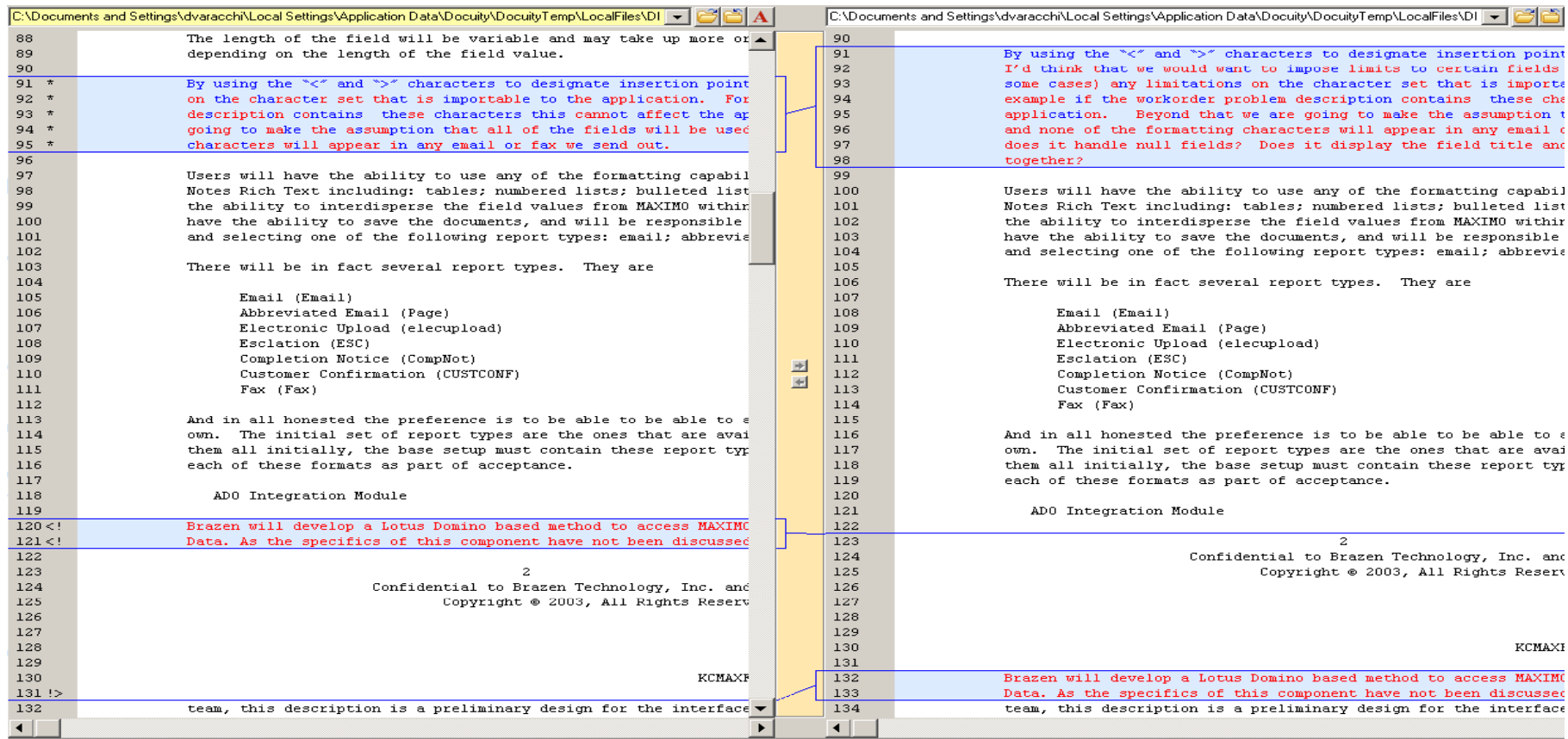


The screenshot shows a software interface with a menu bar (File, View, Processes, Tools) and a document list. The document list includes folders like DOCUMENT INFO, REVIEW COMMENTS, DOCID, BOXNAME, DOCTYPE INFO, and KEYWORD INFO. A blue box highlights the clustering options 'A', 'E', and 'N' in the toolbar. A blue arrow points from this box to a callout box on the right.

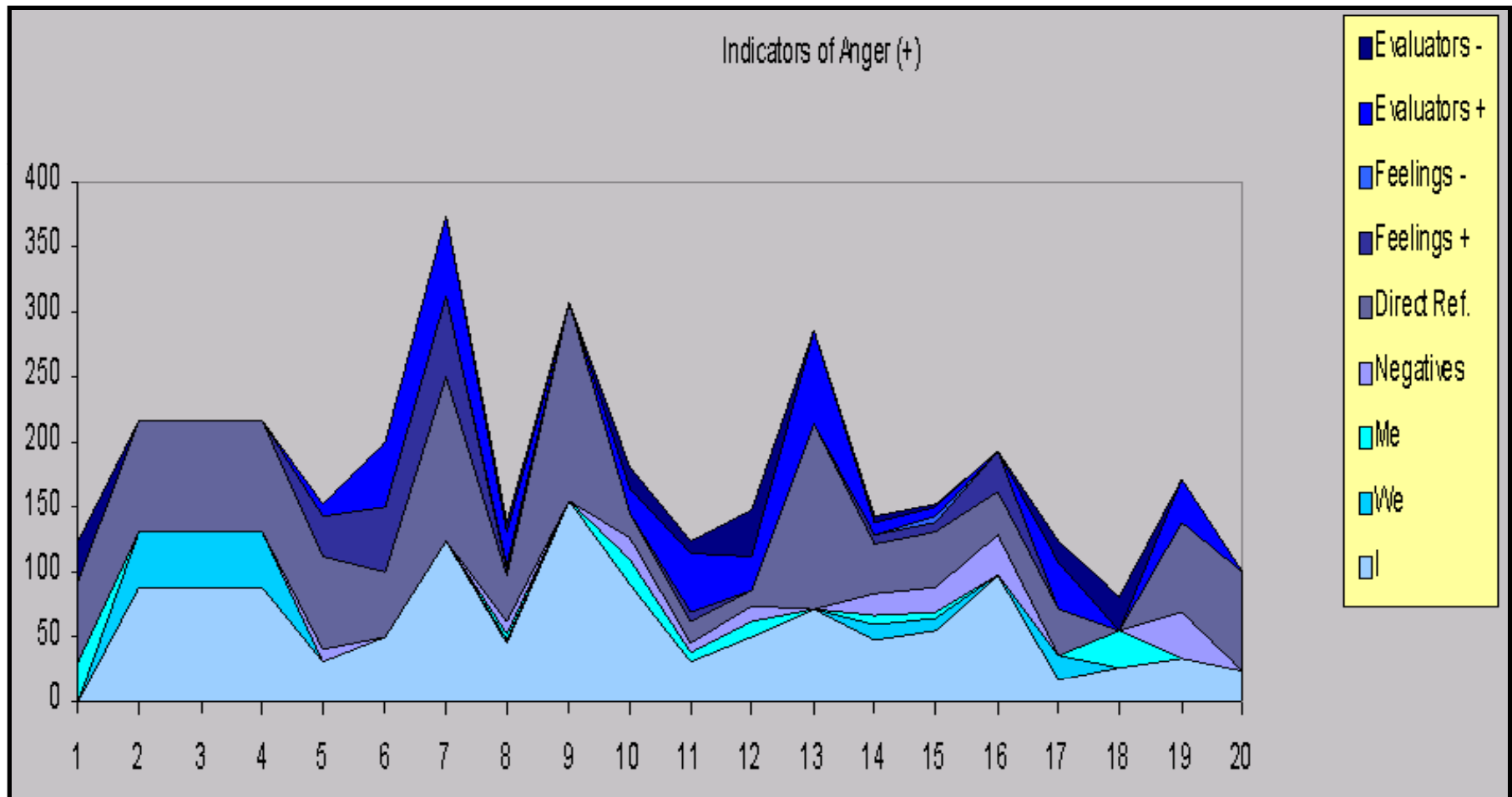
**Clustering Options:**

- “A” Attachment Set
- “E” Exact Duplicates
- “N” Near Duplicates

# FORENSICS IN E-DISCOVERY – Near Duplicate Comparison



# PSYCHO-LINGUISTIC PROFILING



# PSYCHO-LINGUISTIC PROFILING

- (Asked to train his back-up, subject refuses)

“His experience was **ZERO**. He does **not** know **ANYTHING** about ...our reporting tools.”

Until you **fire me** or I **quit** I have to take orders from you...Until he is a trained expert, I **won't** give him access...If you order **me** to give him root access, then you have to **permanently relieve me** of my duties on that machine. I **can't** be a **garbage cleaner** if someone **screws up**....I **won't** compromise on that.”

- Content Analysis Cues
  - **Negatives/anger**
  - **Me/victimization**
  - **Key word/risk behavior**

## The Digital Thugs

- Ex-CIA profiler estimated that suspect was extremely angry and technologically sophisticated, had a history of work problems, and possibly owned weapons.
- Suspect sent multi-million extortion demand and threatened to unleash a DOS attack using MicroPatent's name
- Suspect revealed he had been "dumpster diving," prompting physical surveillance.
- Suspect was arrested at local college and his residence was searched . . .





When the defendant's house in Maryland was searched, the FBI found numerous firearms, explosives and chemicals, as well as a recipe for the production of a deadly toxin.



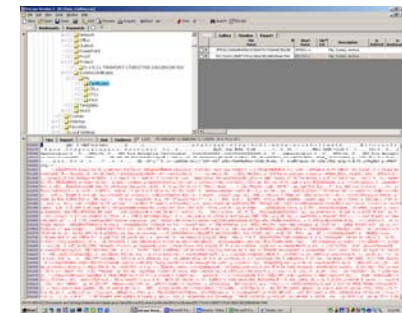
***Ricin***  
Made from castor beans  
6,000 times more powerful than cyanide  
Initial flu-like symptoms, followed by  
death within three to five days

## Summary - When Forensics Make “Cents”



- **Need Verified Preservation?**

- Of key employee data
- By trusted third party
- Using scientific process



- **Authenticity at Issue?**

- Timing (hour/minute/sec)
- Authorship
- Data integrity



- **Latent Data Needed?**

- Full Metadata
- Historic/deleted data
- System logs
- Source code

The banner features a dark blue background on the left with the text 'STROZ FRIEDBERG' in white. On the right, there is a collage of images including a person's profile, a globe, a microscope, and a key.

STROZ FRIEDBERG

## Questions and Discussion

**Edward M. Stroz**  
**Co-President**  
**Stroz Friedberg, New York**  
**[www.strozfriedberg.com](http://www.strozfriedberg.com)**