SHERLOCK HOLMES GOES DIGITAL:

Computer Forensics for Lawyers

PRESENTERS:
Sharon D. Nelson, Esq. & John W. Simek
Sensei Enterprises, Inc.

University of Virginia
Law School

October 14, 2009 | Charlottesville, Virginia
The CSI effect
Resources from Sensei

The Electronic Evidence and Discovery Handbook
Forms, Checklists, and Guidelines
by Sharon D. Nelson, Bruce A. Chren, and John W. Statak

{ride the lightning}
Electronic Evidence Blog
by Sharon D. Nelson, Esq., President of Sensei Enterprises, Inc.

www.senseient.com

SHERLOCK HOLMES GOES DIGITAL: COMPUTER FORENSICS FOR LAWYERS

SENSEI ENTERPRISES
Computer Forensics | Information Technology
www.senseient.com
Craig Ball is a board certified trial lawyer and certified computer forensic examiner

Mr. Ball limits his practice to service as: Court-Appointed Special Master, Electronic Discovery Consultant
Computer Forensics Expert, Forensic Technology Speaker

Craig Ball's column, “Ball in Your Court,” won 2007 and 2008 Gold Medal recognition from the Trade Association Business Publications International as the “Best Regular Column” and 2006 and 2007 Silver Medal recognition from the American Society of Business Publication Editors as “Best Contributed Column”

Recent Publications
- Ball in your Court (through 10/08)
- E-Mail in Civil Discovery 2009 NEW
- E-Discovery: Right from the Start NEW
- Pacing Together the E-Discovery Plan
- What Judges Should Know: Forensics
- Eight on Electronic Data Discovery
- Four on Forensics
- Three for the Court: FJC Training
- What Judges Should Know: EU Tape
- Musings on Meet and Confer
- The Perfect Preservation Letter
- Exemplar Preservation Letter
- The Path to Production of E-Mail
- Metadata: Beyond “Data About Data”
- Plaintiff’s Guide to E-Discovery

Upcoming Presentations
- Austin, TX - 12/03/08
- Austin, TX - 12/03/08
- Washington DC - 12/10/08
- Austin, TX - 12/12/08
- Austin, TX - 12/15/08
- Austin, TX - 12/17/08
- Austin, TX - 01/22/09
- Austin, TX - 01/28/09
- New York, NY - 02/2-4/08
- Austin, TX - 02/06/08
- Cabo S. Lucas - 02/16/09

Resources
- PowerPersuasion Material
- Powering PowerPoint
- Google to the Rescue
- First 180 Days of New EDD Rules
- EDDUpdate

WEBCASTS
- Webcast: Defensible Doc Review
- Webcast: Forms of Production
- Socha Survey "Big Picture"
- Webcast: Search Technology
- Webcast: Ten E-Discovery Blunders
- Webcast: Beyond Data about Data
- Webcast: Paper or Plastic?

Click to read New York Times feature re: Craig Ball 10/15/07 "On the Trail of Digital Secrets"
The attorney’s lament: I’m sorry

I’m a technophobe
techno-illiterate
techno-challenged

My kids run the DVD controller
Courts are saying

- No more excuses
  - attorneys have clear duties
- Learn your client’s technology at the outset
  - keep your experts close at hand if needed
- Issue a litigation hold
- Monitor the hold
- Document, document, document
- Clients need to understand the importance of this process
2008 Report from the American College of Trial Lawyers

- “Civil litigation has priced itself out of the market”
- “E-discovery is crushing the system”
- Are the rules the problem or the application of the rules?
- Failure to understand the rules is costly
- In 2008, 25% of all reported e-discovery cases involved sanctions
Computer Forensics Cases

- Theft of proprietary information
- Contract disputes
- Divorce
- Embezzlement
- Fraud
- Child pornography
- Breach of fiduciary duty
Computer Forensics Cases

- Identity theft
- Libel
- Copyright and patent infringement
- Deceptive advertising
- Discrimination
- Harassment
- Murder
Electronic Discovery Reference Model

- Information management
- Identification
- Preservation
- Collection
- Processing and Review
Where is the relevant data?
Where’s the Data is Like “Where’s Waldo?”

SHERLOCK HOLMES GOES DIGITAL: COMPUTER FORENSICS FOR LAWYERS

SENSEI ENTERPRISES
COMPUTER FORENSICS | INFORMATION TECHNOLOGY
www.senseielt.com
Yes, it’s on computers and laptops
But cell phones are increasingly powerful evidence
What Do Young People Do?

- Talk incessantly on their cell phones
- Text incessantly on their cell phones
- Take non-stop photos
- When something amazing is happening, they both text and take photos
Cell Phone Challenges

- Most but not all cell phones are supported by forensic software
- Sometimes, dates and times are not associated with the raw data
- If phone is unsupported, can take photos of the text messages, call log, etc. to create a record (no deleted entries however)
Cell Phone Challenges

- Keep cell phones charged
- Memory varies with phone
- Send the power cord
- A totally discharged phone may erase all data, returning the phone to factory defaults!
More Great Evidence: Digital Cameras
Video cameras

Watch "FREE" Satellite TV Channels on your computer

Go To: www.SatelliteTV.we.bs
Don’t Forget iPods
They don’t need to carry the computer off – they just need an iPod
or thumb drives, back up media, CDs, DVDs, etc.
Digital copiers
Computerized swipe cards

- Death of Yale graduate student – Annie Le
- Raymond Clark swiped card after Le
- Clark card swiped in area where Le’s body found
- Fire alarm tripped – possibly with swipe card
- Over 700 hours of surveillance video
SOCIAL NETWORKING SITES: GOLD MINES OR SAND TRAPS FOR LAWYERS?
E-Mail Environments

- Microsoft Exchange
- Lotus Notes
- Novell GroupWise
- Web-based
- ISP Hosted
Protocols

- POP (Post Office Protocol)
- IMAP (Internet Message Access Protocol)
- MAPI (Message Application Program Interface)
- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
E-Mail Files

- EDB
- NSF
- PST
- OST
- HTM
- DBX
- MBX
- EML
- MSG
- OLK
E-Mail Structure

- Headers
- Content Type
- Boundaries
- Attachments
Can you subpoena an ISP for e-mail?

- Maybe only in criminal cases
- ECPA is now being asserted by ISPs and cell phone providers
- If the e-mail is less than 30 days old
- Great for hot cases – stalking, harassment, missing children etc.
- ISPs hate subpoenas and hose data quickly
- But remember that there may be at least two sources of data – the sender and the recipient
What can you subpoena a cell phone provider for?

- Call logs, date and time, cell phone towers – retention period varies
- Text messages – retention period varies, but 2-4 weeks is usually the outside
- Policies re: retention are changing constantly
Cell phone carriers

- The cell towers that were involved can be critical
- Murderers have been convicted partly on the information gleaned from cell towers

Paul Cortez
March 21, 2007
25-life sentence
GPS devices and EZ-Pass Records
Voice communications

- Most voicemail is hosed in 30 days or less
- But this varies by company, so check
- Unified messaging
- Is there a separate server?
- Is it housed on the e-mail server?
What’s on the server?

- Documents
- E-mail
- Presentations
- Spreadsheets
- Financial data
- Databases
- Access logs
What’s on the local hard drive?

- Anything might be – if they choose to save it there
- Commonly, people with “bad intent” will save to the local drive
- Likewise, they’ll use web-based e-mail rather than business e-mail
What’s on the home machine?

- Who knows? But you have to check
- Did they use the home computer for business use?
- If home machines are to be imaged, must be careful to produce only data related to the case
Recoverable (if not overwritten!)

- Deleted files – documents, spreadsheets, etc.
- Internet history – what sites they visited/when and searches conducted
- E-mail, including web-based e-mail
- Installed applications and data
- Unified messaging
Recoverable
(If not overwritten!)

- Computer activity timeline
- Files where extensions are intentionally modified
- PDA data
- Digital media cards
- Text messaging
Metadata – The Invisible Man in Evidence

- Data about data – hidden from public view
- Shows date/time of
  - Creation
  - Access
  - Modification
  - Last printing
- Shows
  - Author
  - Number of revisions
SHERLOCK HOLMES GOES DIGITAL: COMPUTER FORENSICS FOR LAWYERS

Metadata

- Word
- WordPerfect
- Excel
- PowerPoint
- Scrubbers
  - Metadata Assistant
  - PDF
  - RTF

**Task List Current Properties**

- **Type:** Microsoft Word Document
- **Location:** I:\Task List
- **Size:** 25.5KB (26,112 bytes)

- **MS-DOS name:** TASKLI-3.DOC
- **Created:** Wednesday, July 02, 2003 2:19:24 PM
- **Modified:** Thursday, March 04, 2004 6:31:23 PM
- **Accessed:** Friday, March 05, 2004 8:05:58 AM

- **Attributes:**
  - [ ] Read only
  - [ ] Hidden
  - [x] Archive
  - [ ] System

[OK] [Cancel]
Metadata Assistant

Metadata Assistant for Word Results - Analyzing K:\Sent\Articles\LEGAL~1\SHACKLE~1.DOC

Document Name: SHACKLE~1.DOC
Path: K:\Sent\Articles\LEGAL~1
Document Format: Word Document
Compatibility Options: Microsoft Word 2000

Built-in document properties:
- Built-in Properties Containing Metadata: 3
- Title: SHACKLE TO MICROSOFT
- Author: Sharon Nelson
- Company: Sensei Enterprises, Inc.

Document Statistics:
- Document Statistics Containing Metadata: 6
- Creation Date: 10/7/2002 3:12:00 AM
- Last Save Time: 1/22/2003 3:07:00 PM
- Time Last Printed: [Blank]
- Time Saved By: Anthony Stefano
- Revision Number: 6
- Total Edit Time (Minutes): 27 Minutes

Custom document properties:
- No Custom Document Properties

Last 10 authors:
- Has Last 10 Data
- Author: Sharon Nelson
- Path: K:\Sent\Articles\Legal technology\SHACKLE TO MICROSOFT.doc
- Author: Sharon Nelson
- Path: C:\Documents and Settings\Sharon Nelson\Application Data\Microsoft\Word\AutoRecovery\save of SHACKLE TO MICROSOFT and
- Author: Sharon Nelson
- Path: C:\Documents and Settings\Sharon Nelson\Application Data\Microsoft\Word\AutoRecovery\save of SHACKLE TO MICROSOFT and
- Author: Sharon Nelson
- Path: C:\Documents and Settings\Sharon Nelson\Application Data\Microsoft\Word\AutoRecovery\save of SHACKLE TO MICROSOFT and
- Author: Anthony Stefano
- Path: K:\Sent\Articles\Legal technology\SHACKLE TO MICROSOFT.doc
- Author: jjwood
- Path: K:\Sent\Articles\Legal technology\SHACKLE TO MICROSOFT.doc
Smooth talking lawyer takes money from nursing home resident then failed to file six figure medmal claim. Statute of limitations expires in 2005.
August 1, 2005

Mrs. Sarah Brown
Community Nursing Home
Room 404
101 Lee St.
Fairfax, Virginia 22030

Re: Claim against Dr. Bruce White

Dear Mrs. Brown:

I understand from our phone conversation this morning that you have decided that you do not want to proceed with the lawsuit against Dr. White, even though it is clearly meritorious. I know you feel that it would cause too great an impact on your health. I certainly understand your concerns. In light of our conversation, I will take no further action on this case and will close my file.

Regards,

Peter T. Quinn, Esq.
Unrecoverable

- Wiped drive areas
- Instant Messaging (sometimes)
- Overwritten files (maybe)
- Frequently, segments of files
- Encrypted files
Optical Media Fragments

- CD-RW
- DVD-RW
- DVD+RW
- Multi-session
Your Nemesis: Wiping and Scrubbing

- Evidence Eliminator
- Secure Clean
- Evidence Scrubber
- Window Washer
- Disk Wiper
- All leave traces
- Spoliation is both damning and expensive
Spoliation

- Destruction or significant alteration of evidence or failure to preserve evidence
- Where litigation is pending or reasonably anticipated
- Or where data must be retained under a statutory or regulatory mandate
Computer Forensics vs. EDD

- CF – Identifying, preserving, acquiring, analyzing, extracting and presenting the evidence
- EDD – Managing the evidence
- Many do EDD, wild disparity in quality
- Few do CF and fewer do it well
- Prices for both are all over the map
- Beware of “lower” hourly rates
Choosing Your Forensic Technologist

- Technical Certifications
- Forensic Certifications
- Courts Qualified
- Professional Experience
- Referrals From Clients and Colleagues
Choosing Your Forensic Technologist

- CV – Get and Ask Questions
- Seminars & Publications
- Speaks English
- Knowledge of the Law
- Beware of “Point and Click” Forensics
- Does Geography Matter? Sometimes
What Your Expert Will Do

- Assist in identifying evidence
- Label evidence at it comes in, by sequential numbering, name of computer owner
- Photograph the computers/media
- Document system date and time/MD5 Hash
- Scan all evidence for viruses
- Scan all evidence for child porn
- Maintain chain of custody, recording each device, manufacturer, model, serial #
- Secure the evidence under lock and key
The Steps in Your Case

- Preserve the evidence
- Have your forensics expert make a forensic image
- Expert analysis
- Review by phone
- Do you need/want a report?
- Do you need/want testimony?
- Do you want the expert present as a non-testifying witness to assist you?
What happens in a computer forensics lab?

- How are deleted files recovered?
- Indexing
- Data carving
- Culling the data
- De-NIST
- Internet history recovery
- Virtual mounting
- Registry analysis
  - Programs
  - USB stores
  - GUID
Common forensics tools/methodologies

- EnCase
- Forensic Toolkit (FTK)
- X-Ways Forensic
- NetAnalysis
- Nuix
- Paraben Suite
- Cellebrite
- Mount Image Pro
- VMware

- Data Carving
- Searching
- De-Duplication
- Hashing
Litigation hold

- When you know or reasonably should have known
- That a regulatory or legal action is in place
- Or likely to take place
- Document, document, document
Things you need to know soon

- Where is the data?
- What operating system is used on the servers?
- Is any relevant ESI encrypted?
- How is data backed up?
- What e-mail package is used?
- What third parties may have data?
- Who are the key players?
- Facts will determine other specifics
- Develop a checklist and survey sheets to use with clients
Things you need to know and do soon

- Identify subject matter
- Identify time frame at issue
- Preservation
- Communicate with opposing counsel
- Memos addressing need to preserve/spoliation:
  - Your clients
  - Opposing counsel
  - Third parties
- Monitor the hold
Meet early with clients

- Prepare them for CF and its costs
- Do a cost-benefit analysis
- Discuss spoliation and its consequences
- Go through the litigation hold duties
- Address preservation issues right away
Get a REAL network diagram from your client and opposing counsel
Working with IT staff

- It’s THEIR turf – they know where the data is and how it’s backed up
- They speak another language
- They don’t like lawyers (or paralegals)
- They often think they know better than you
- They are often sure they can do what forensics or EDD experts can do
- They can’t
- Diplomacy is critical
Data collection pitfalls

- People don’t remember where all the data is
- Third parties are forgotten
- Employees (even supervisors) try to hide the ball
- Poor searching
- Letting employees search themselves
- You have an ethical obligation – your client may have something to hide – this creates tension
How you can avoid pitfalls

- Get that network diagram
- Make friends with IT
- Involve the client’s legal staff, records managers and management
- Stress the importance of EDD legal and technical experts
- Ask about 3rd parties – give them examples
- Stress importance of preservation and consequences of spoliation or hiding data
- Make sure the entire process is transparent and defensible
Early case assessment: work with opposing counsel on scope and methodology

- Meet and confer responsibilities
- Preservation and production issues
  - Active data only?
  - Locations of data? Third parties?
  - What format?
  - What ESI needs to be preserved?
  - Is metadata important here?
- Avoid conflicts – judges are impatient with them
Search smart

- "System" is a dumb search term
- "pot" will get you "spot" and "potential" unless constructed properly
- Search syntax is its own science
- Narrow your terms
- The greater the volume of data, the greater the cost of production and review
Kinds of searches

- **Keywords**
  - Still the most common (Boolean, GREP etc.)
  - Can be very over-inclusive or under-inclusive

- **Conceptual**
  - “Car” will return “auto” and “vehicle”
  - More expensive
  - A better way, and probably will become standard at some point
Attorneys are not generally equipped to construct search terms

Normally, paralegals are not either

Client employees definitely are not

Generally, an expert is required

Search construction is part art, part science

Your searching methodology must be three things:
  – Defensible
  – Transparent
  – Tested for reliability

Preservation

- Can keep data onsite
- Should be backed up
  - Windows Backup
  - Reflect
  - SyncBack
  - Second Backup
  - Truesafe
- Onsite preservation helps prevent over-collection, reduce costs and delays
- Document, document, document
Manual preservation

- Custodian finds data and copies it
- Not a good idea if metadata is in issue
- Or if custodian doesn’t have time/brains
Collection

- E-mail tips
- Document tips
- Maintain chain of custody
- Get hash signatures
  - VisualHash
  - Pinpoint Hash
  - Pinpoint MetaViewer
  - Faststream MD5/SHA1 Hash Extractor
  - Easy Hash
  - Iside
  - Karen’s PowerTools (Hasher)
- Robocopy
- XXCopy
- Don’t forget paper! OCR it.
  - FreeOCR
  - GOCR
  - SimpleOCR
  - Tesseract
- Code scanned documents
Processing

- DiscoveryForce.com
- Document conversion
  - Omniformat
  - VeryPDF
- Foreign language – unicode compliance
- Indexing
- De-duping
- Near-duplicates
- Metadata culling
In small cases, you can often do it yourself

Acrobat Pro
- Have an index
- Run searches
- Redact
- Bates stamp

Don’t delete relevant documents, dupes or near dupes – suppress them instead.
Quick peeks – a valuable tool

- Take a “quick peek”
- Use MD5 hashes from your client’s database to run against the opposing party
- One such peek turned up 900 matching files
What should you expect to pay?

- One computer case – under $10,000
- A dozen computers – under $25,000
- Remember, after imaging, you are searching ONE body of evidence all at once
- Look for low hanging fruit first
- Do you just need a letter or an informal report?
- Or have your expert on the phone with the other side?
Why Not Look at Evidence Yourself or with Your Client’s IT Staff to Save $$$$?

- Just booting a computer changes hundreds of file access times
- Potential compromise of timeline by changing date
- Shutdown and startup process vary by system configuration
- Overwrite swap file area
- Evidence may become suspect or rendered inadmissible
Coming soon - proportionality

- From across the “pond”
- Mentioned more and often in U.S. cases
- D.C. Appeals Court Affirms Order Requiring a Non-Party to Spend $6 Million, 9% of its Total Annual Budget, to Comply with an e-Discovery Subpoena
  - the Fannie Mae case, involving the Office of Federal Housing Enterprise Oversight
Vendor tips for small cases

- Don’t need a large vendor
- Get an estimate
- Recognize that estimates have limitations
- Place cap, not to exceed without written authorization
Cost estimates

- Judges are extremely skeptical
- Often comes down to a dual of the experts
- Make sure your estimate is defensible!