An Introduction to Digital Forensics: The Seventh Circuit E-Discovery Pilot Program

August 30, 2013

Richard D. Lutkus, Seyfarth Shaw LLP

Matthew C. Christoff, Seyfarth Shaw LLP

What is Digital Forensics

- Digital forensics involves the preservation and analysis of digital devices to determine various *events or data characteristics* present on a device.

  - ►Examples:
    - Did an employee take data prior to departing employment
    - Who deleted data from a server and when
    - Recovery of inappropriate text messages
    - Investigate employee Internet activity
    - Determine employee computer use patterns
    - Did a document ever exist on a computer

Devices Implicated in Digital Forensics?

- Digital forensics implicates all devices that could potentially store data:
  - ►Computers (laptops, desktops, servers)
  - ►Smartphones (iPhone, Android, Windows Phone, BlackBerry)
  - ►Tablets (iPad, Galaxy Tab, Nook, Kindle)
  - ►Network Storage Devices (NAS, SAN, etc)
  - ►Gaming consoles (Xbox, PlayStation, Nintendo)
  - ►Printers, scanners, and copiers
  - ►Digital cameras and memory cards
  - ►Network infrastructure such as routers, switches
- Computers are the most common
- Enterprise devices rise to the top

Digital Forensics versus eDiscovery

- There are key differences:
  - ►Forensics involves deleted items, artifacts, parts of files, and other ephemera from one or a few *specific people’s data sources.*
  - ►eDiscovery is more focused on finding data that is responsive to discovery requests. Typically you do *not* undertake forensic analysis to populate document productions.
- Both can exist in a case, but have different approaches
  - ►eDiscovery can be limited in scope to only non-deleted data, for example.
  - ►Forensics oftentimes involves deleted items or reconstructing user actions, thoughts, intent, and planning.
  - ►Forensic analysis is often used prior to the onset of litigation to determine whether or not to sue

Knowing Your Case/Investigation

- Typical cases that involve forensics
  - ▶Trade secret/IP misappropriation
    - Taking client lists
    - Leaving with past employer data
    - Selling secrets
  - ▶Breach of Fiduciary Duty
    - Double-dealing or running sub-business
  - ▶Data breach
  - ▶Certain bankruptcy cases
- Typical eDiscovery-only cases: everything else
  - ▶Wage/Hour (though sometimes forensics)
  - ▶Class action (employment, benefits, retirement, etc.)
  - ▶Breach of contract
  - ▶Subpoena responses

Forensic Collection Methods

- Physical Collection
  - ►A “physical” collection will create an identical copy of the device that you are collecting, including deleted items, file fragments, and empty space.
  - ►A physical collection takes the most time and storage space, but will allow you to “go back to the well” in situations where you need to perform additional data exports or analysis.
  - ►This method is advised when there is the possibility that the owner of the device may have attempted to delete or wipe potentially relevant information.
    - Or when they are a key custodian

Forensic Collection Methods (cont.)

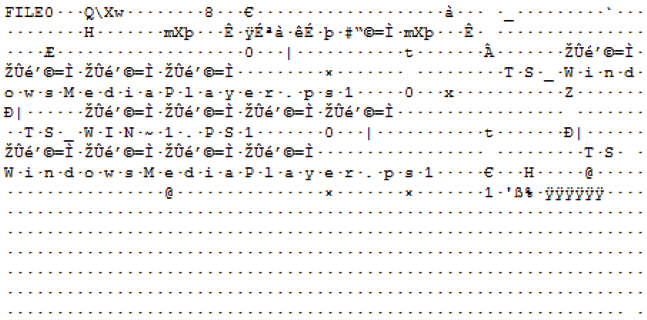
- Logical Collection
  - ►A “logical” collection will create a copy of all “active” or “live” data on a device, but will not capture certain deleted items, file fragments, or empty space.
  - ►Logical collections are more common than physical collections, as they are typically used in the majority of cases when no evidence of foul play exists.
  - ►Most forensic collection devices allow the forensic examiner to configure exactly what type of information is collected:
    - Specific data locations on a device
    - Include or exclude file types
    - Limit by date range

Forensic Collection Methods (cont.)

- Portable Collection Devices
  - ►Many forensic software vendors offer portable collection devices that can be configured by a forensic examiner to perform a physical or logical collection.
  - ►These devices can then be sent directly to a client with instructions on how to run the forensic software contained on the portable collection device.
  - ►Benefits include:
    - Reduction in cost through the use of internal resources and IT.
    - Collections can be based upon the schedule of the device owner, including those that are constantly traveling.
    - Less impact on employee computer use

Allocated Space

- In general, all files on a computer are identified within a system file called the Master File Table (“MFT”)
  - ▶The MFT lists where the individuals fragments of a file exist across the hard drive. These fragments are located within “Allocated Space”
  - ▶Library Analogy: Think of the MFT as the card catalog, and files as books.
- Files that are viewable by a user are “allocated,” meaning they have dedicated space in which they exist



```
FILE0···Q\Xw·······8···€··················à···  ·_··········`···
········H·······mXþ···Ê·ÿÉªà·êÉ·þ·‡"©=Ì·mXþ···Ê· ················
····Æ··················0···|···········t·······Â·······ŽÛé'©=Ì·
ŽÛé'©=Ì·ŽÛé'©=Ì·ŽÛé'©=Ì·········x········ ··········T·S·_·W·i·n·d·
o·w·s·M·e·d·i·a·P·l·a·y·e·r·.·p·s·1·····0···x············Z·······
Ð|······ŽÛé'©=Ì·ŽÛé'©=Ì·ŽÛé'©=Ì·ŽÛé'©=Ì················· ·······
··T·S·_·W·I·N·~·1·.·P·S·1·······0···|···········t·······Ð|······
ŽÛé'©=Ì·ŽÛé'©=Ì·ŽÛé'©=Ì·ŽÛé'©=Ì················· ·········T·S· ·
W·i·n·d·o·w·s·M·e·d·i·a·P·l·a·y·e·r·.·p·s·1·····€···H·····@·····
················@················x·······x·······1·'ß%·ÿÿÿÿÿÿ····
················································································
················································································
················································································
················································································
················································································
··············································································· ·
```

Unallocated Space

- Unless a file is securely deleted using appropriate software, the operating system merely removes the files entry in the MFT, allowing new or existing files to use the space previously occupied by the “deleted” file.
  - ►The “deleted” file exists in “unallocated space”
  - ►Data located within unallocated space is typically not viewable by a user without specialized software.

- Fortunately, if a new or existing file has not overwritten the data of the “deleted” file, forensic software may be able to analyze the hard drive and recreate the file in part or in whole.

Unallocated Analysis

- Analysis of unallocated space can also reveal additional information:
  - ►Large patterns of repeating characters (or the absence of any data at all) may indicate that wiping software was used.
  - ►Such patterns are *highly unlikely* to exist through normal usage.

- Data carving can find files that are “lost” in unallocated space… meaning their MFT entry is missing.
- A wealth of historical data can be found here, however…
  - ►The older the data you are seeking, the less likely you will find it.
  - ►Continued computer use constantly writes data, thus overwriting files in unallocated space with new data. Permanent loss.

Digital Forensic Toolkit

- Forensic Collection and Analysis Software
  - ►EnCase (Guidance Software)
  - ►FTK (Access Data)
  - ►X-Ways, Helix, Raptor
- Chain of Custody Forms
- Camera
- Write-Blocking Hardware
- Imaging device with various connectors
- Media to store resulting forensic images

Defining Scope of Digital Forensic Investigations

- The specific facts and allegations of your case will directly impact the types of information that you are looking for.
    - ► Trade secret misappropriation
        - How did you learn about it?
        - Who found out?
        - When did they find out?
    - ► HR Investigation
        - Who reported wrongdoing?
        - What did the bad actor do?
- Client digital footprint drives the pool of potential sources
    - ► Corporate-issued computers, smartphones, etc.

Defining Scope of Digital Forensic Investigations

- There are MANY more sources of information than what you may need for any one investigation.
- Conducting a forensic collection and analysis in all situations will likely be a waste of time, money, and resources.

- **Remember:** <u>Not everything will be relevant.</u>

Common Client Pitfalls

- IT redeploys departed employee computer *immediately* or before any case/investigation is even ripe (IT is often under stress to constantly redeploy hardware)
- Client does self-help preservation and alters metadata on original evidence or fails to complete preservation efforts
- Client allows auto-deletion routines to execute without knowledge of matter
- Legal may be aware of holds or potential holds, but does not properly inform IT of their obligations
- No chain of custody
- Hiring incompetent vendors
- Impatience: forensic analysis can take time

Potential Attorney Mistakes

- Not issuing a litigation hold in a timely manner
- Not ensuring compliance with issued holds
- Not sending follow-up litigation hold reminders
- Not giving clear direction on how to handle electronic sources of evidence
- Not engaging internal or external resources to scope potential data sources early enough
- Not giving adequate consideration to how forensic analysis can be employed on both an offensive and defensive basis

Electronic Evidence Handling

- In the forensic investigation (as opposed to standard eDiscovery) context, DO NOT:
  - ►Access or allow the client to access potential sources of electronic evidence
    - Do not even turn the device on. Leave it! If it’s on, pull the plug, pull the battery, or call in an expert.
  - ►Ask for a “copy” of the original device
    - Not only is a “copy” insufficient, but it could actually destroy artifacts that may help your case
  - ►Allow IT to redeploy a machine that is potentially at issue
    - If they really must, have them pull the hard drive and preserve at least that, documenting the original computer information
  - ►Plug in any device a client sends you
    - Curiosity can be a case-killer
    - Antivirus and indexing software can change access dates, etc.

Electronic Evidence Handling (cont.)

- Instead, be sure to DO the following:
  - ►Create a clear chain of custody that starts at the custodian and stays current
    - This form should stay WITH the ORIGINAL EVIDENCE at all times, and be updated whenever it changes hands or location
  - ►Contact internal or external resources to assist in proper handling of electronic evidence
    - Specialized training, even with minimal efforts, can save critical data
    - Avoids spoliation arguments later on
  - ►Inform the client of the necessity to carefully handle evidence
  - ►Suggest client utilize internal procedures that are clearly documented or third party resources to ensure preservation

Forensic Analysis

- What can you expect?
  - ▶Deleted files and “orphaned” or lost files
  - ▶Internet History
  - ▶Recently accessed files
  - ▶Email (sometimes deleted)
  - ▶Chat sessions (on occasion)
  - ▶Logs
    - CD burning, login information, VPN usage, virus scans, etc
  - ▶Device usage (iPhone, iPad, Android, USB device, etc)
    - Call history, SMS/MMS history, pictures/videos, etc.
  - ▶Computer usage trends
  - ▶Timeline analysis (complex)

Social Media

- An increasing target for preservation, collection, and review is information stored on social media sites.
  - ►A forensic analysis of data captured from a user’s hard drive may reveal relevant social media artifacts, including images from the user’s profile or from profiles that they had viewed.
- Other alternatives do exist for getting at this data:
  - ►Many social media sites are beginning to offer the option of downloading a self-contained archive of a user’s profile for backup purposes, including Facebook and Twitter.
  - ►Recently, a number of third party software developers have released software designed to analyze, review, and archive information posted to social media sites that meet specific criteria.

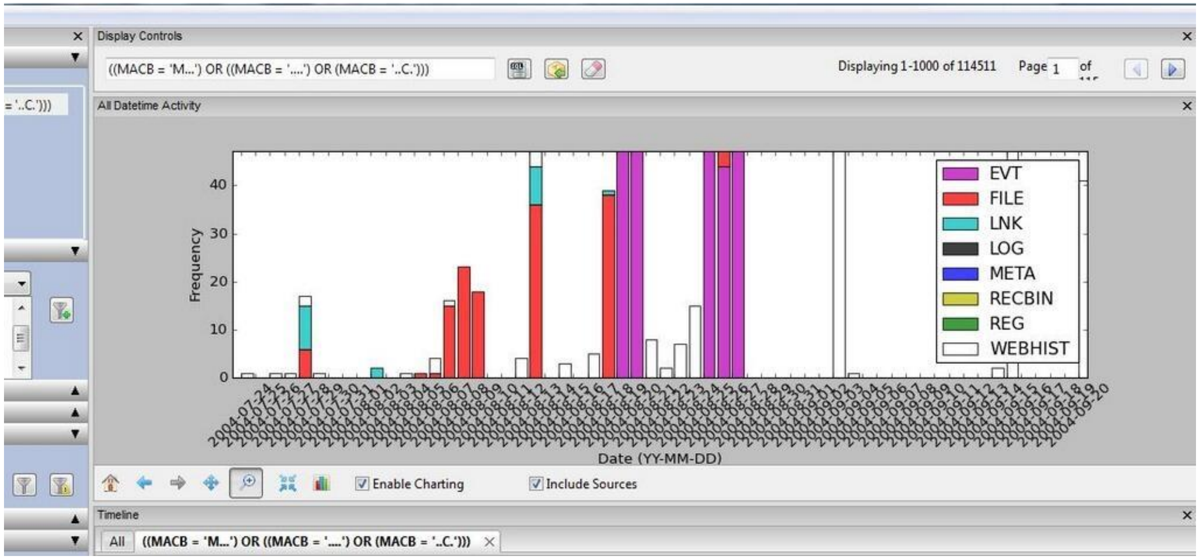
Timeline Analysis

- A subset of forensic analysis that seeks to build a chronological timeline of gathered artifacts
  - ►Takes many sources of artifacts into account:
    - Internet use, file activity, USB usage, logon events, software launching, etc.

- Helps give context to event-based investigations

- Shows user activity in relative, visual sense that can reveal patterns

Timeline Analysis (cont.)


Display Controls

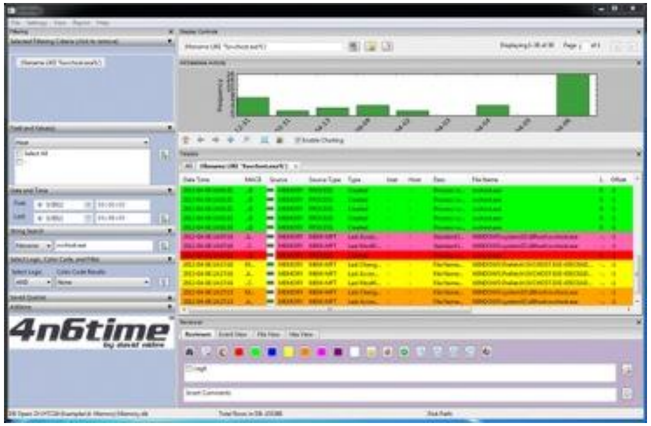
((MACB = 'M...') OR ((MACB = '....') OR (MACB = '..C.')))

Displaying 1-1000 of 114511 Page 1 of

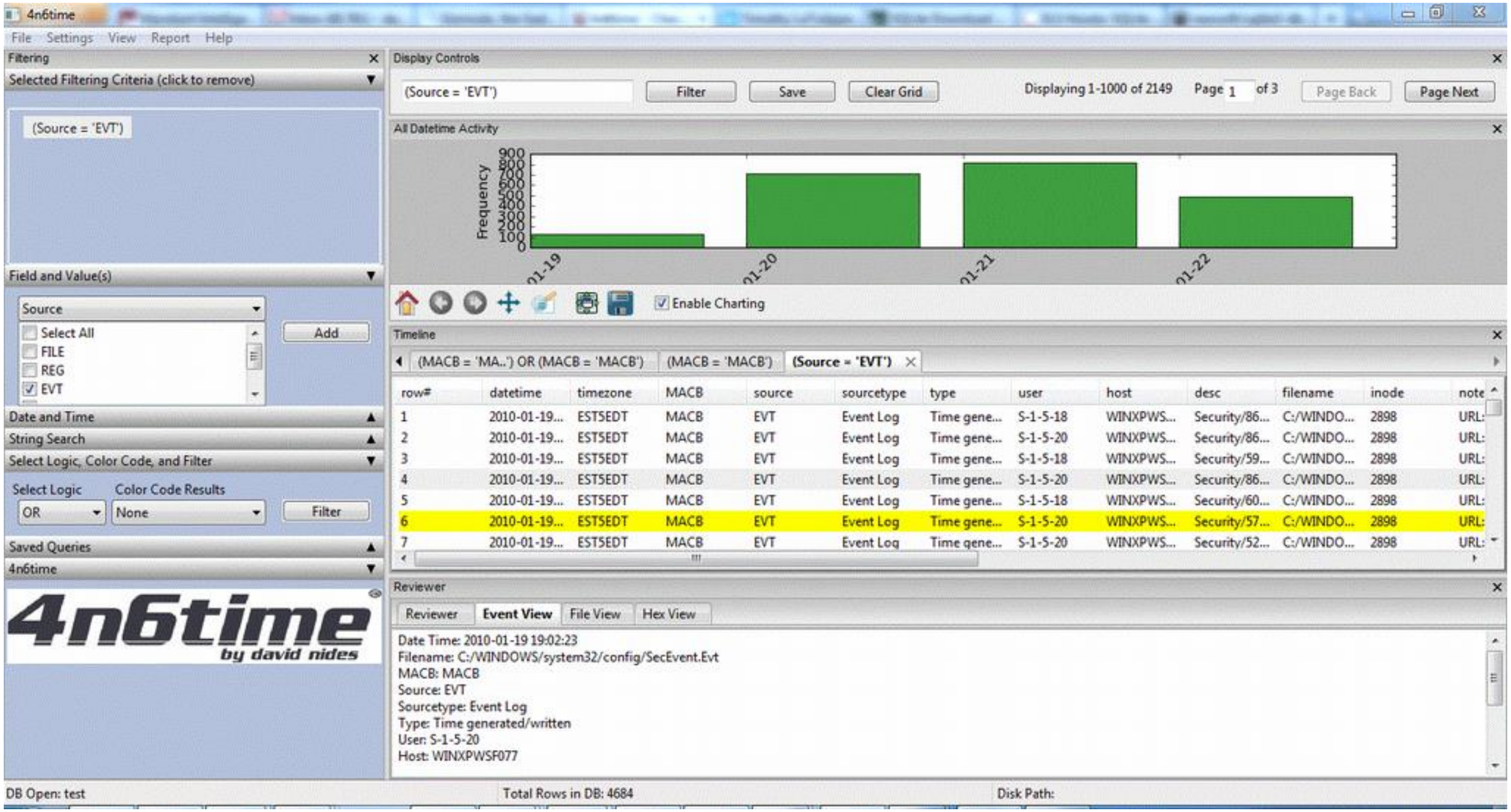
☑ Enable Charting ☑ Include Sources

Timeline

All ((MACB = 'M...') OR ((MACB = '....') OR (MACB = '..C.')))



Timeline Analysis (cont.)



row#	datetime	timezone	MACB	source	sourcetype	type	user	host	desc	filename	inode	note
1	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-18	WINXPWS...	Security/86...	C:/WINDO...	2898	URL:
2	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-20	WINXPWS...	Security/86...	C:/WINDO...	2898	URL:
3	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-18	WINXPWS...	Security/59...	C:/WINDO...	2898	URL:
4	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-20	WINXPWS...	Security/86...	C:/WINDO...	2898	URL:
5	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-18	WINXPWS...	Security/60...	C:/WINDO...	2898	URL:
6	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-20	WINXPWS...	Security/57...	C:/WINDO...	2898	URL:
7	2010-01-19...	EST5EDT	MACB	EVT	Event Log	Time gene...	S-1-5-20	WINXPWS...	Security/52...	C:/WINDO...	2898	URL:

Date Time: 2010-01-19 19:02:23
Filename: C:/WINDOWS/system32/config/SecEvent.Evt
MACB: MACB
Source: EVT
Sourcetype: Event Log
Type: Time generated/written
User: S-1-5-20
Host: WINXPWSF077

DB Open: test
Total Rows in DB: 4684
Disk Path:

A Very Common Question

- "What files were put on a USB device?"
  - ►Not straightforward unless the USB device is available
    - This analysis can be complicated.
  - ►Why?
    - Windows does not track the *path of a file from one place to another,* just its existence
  - ►What can help?
    - Recent file activity
    - Last Accessed or Last Written (saved) dates
    - USB device insertion/removal times
    - User activity during USB insertion
- Software is available to track this, but almost no companies use it.

Other Common Requests

- Recover data from iPhones, BlackBerry, and Android devices without knowing the associated password:
  - ►Many owners backup their mobile device data to their computers or to the cloud.
  - ►Password recovery software can analyze and recover data that exists within these password-protected backups quickly and efficiently.
  - ►Many forensic tools have methods of cracking passwords included by default.
  - ►Ability is subject to firmware bypass methods
    - Depends on non-commercial community of “hackers”

Other Difficult Requests

- Deleted email
  - ▶ Bad actor sends an email, and immediately deletes it
  - ▶ Can the email be acquired from any other location, such as email archiving software?
- Deleted files from iPhone/iPad
- What was there before a data wipe
  - ▶ The point of wiping is to make answering this impossible
  - ▶ But, the fact *of the wipe itself* shows intent
- Encrypted and Password-Protected Files
  - ▶ Hardware Encryption
  - ▶ Software Encryption
  - ▶ Password-Protected Files

Forensic Considerations

- What are you truly after in the long run?
  - ►Think of your end goal, as a full forensic analysis is often unnecessary.
- What is relevant and what is not?
  - ►Dates are very important
- Forensic examinations can run indefinitely if not carefully controlled.
  - ►Example: "Report on the leaves you see in the forest"
- Iterative process
  - ►Many times one initial scope analysis uncovers a new thread of investigation
  - ►One case may have many "rabbit holes," so you must determine when to stop following trails that are unlikely to be helpful

Results of Forensic Analysis

- Reports
  - ►This is the typical output from a forensic analysis
  - ►Excel spreadsheet
  - ►Extracted files
- Testimony of Subject Matter Expert
  - ►Will rely on report
  - ►Non-privileged
- The role of the Consulting Expert
  - ►Privileged
- The role of the internal forensic team
  - ►Can be privileged if examiner is attorney
  - ►Provides "quick peek" and client guidance on whether to proceed or risk/rewards

Additional Resources

- Seventh Circuit Electronic Discovery Pilot Program
  - ►http://www.discoverypilot.com/
- The Sedona Conference Glossary: E-Discovery & Digital Information Management (Third Edition)
  - ►https://thesedonaconference.org/publications
- eDiscovery Reference Model (“EDRM”)
  - ►http://www.edrm.net

Questions?

Contact Information

Richard D. Lutkus, Esq.

EnCase Certified Computer Forensic Examiner (EnCE)

EnCase Certified eDiscovery Practitioner (EnCEP)

Certified Ethical Hacker (CEH)

rlutkus@seyfarth.com

(312) 460-5312

Matthew C. Christoff, Esq.

EnCase Certified Computer Forensic Examiner (EnCE)

mchristoff@seyfarth.com

(312) 460-5315