SAND2015-0554C

Exceptional service in the national interest

Sandia National Laboratories

Practical Tech Advice for the Non-Techy Attorney

By Corey Reitz

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Agenda

Sandia National Laboratories

- The Computer Forensics Toolkit
- Common Computer Challenges With E-Discovery, How to Avoid Them and What to do When They Happen
- Getting Familiar with File Systems, File Types and Locations for the Most Common Sources of E-Discovery
- Practical Tech Tips
  - Recovering Data
  - Archiving and Preserving Data
  - Sharing and Retrieving Data
  - Presenting Online Data
- The Latest and Greatest Tech Tactics and Handy Tips

The Computer Forensics Toolkit

Sandia National Laboratories

- Hardware
  - Computer with a lot of quick memory (RAM), high performing processor(s), and adequate internal or external hard disk(s) to handle the amount of data to be forensically imaged.
  - Write blocker
  - Cables for mobile devices
- Software
  - Open Source forensic tools
    - SANS Investigative Forensic Toolkit (SIFT)
  - Proprietary forensic tools
    - Encase
    - FTK
    - Cellebrite UFED (mobile devices)
- A practitioner with experience analyzing the operating system and applications involved in the investigation.

Acquisition and Analysis

Sandia National Laboratories

- Acquisition is performed by creating a bit by bit copy of the computer hard drive. The forensic image is then copied so that there are two copies- one for analysis, and one as a clean backup.
- Computer forensic analysis can provide the following services and information:
  - Identifying and recovering deleted information from a computer
  - Creating a timeline of what took place on a computer
  - Capturing electronic communication other than email (e.g. instant messages)
  - Identifying and explaining internet & social media activity
  - Identifying applications that were installed and executed on a computer
  - Identifying pictures and movies (e.g. when people try to hide them)
  - Peripheral device usage in a computer (USB drives, printers, etc.)

Computer Forensics v. E-discovery

Sandia National Laboratories

- Computer forensics deals with all of the data on a computer hard drive.
  - Allocated and unallocated clusters, operating system files, log files, file remnants, etc.
- E-discovery primarily focuses on a subset of the data on a computer, generally user created.
  - Microsoft office files, Email, PDFs
- In E-discovery the expert provides the results for the attorney to perform the analysis (i.e. document review). In computer forensics, the expert performs the analysis and reports their findings to the attorney.
- E-discovery provides responsive files from a computer, Computer forensics provides context of what took place on a computer

Common Computer Challenges in E-Discovery

Sandia National Laboratories

- Volume/Cost of review
- Ease of distributing
- Metadata
- Informal form of communication
- Ease of inadvertently modifying
- Ensuring evidence is not deleted
- Manner of destroying
- Encryption
- Password protected files
- Non-standard software that creates proprietary files
- Files that are not text based, and therefore are not searchable
- Lack of software tools that can process all the various file types

How to Avoid Computer Issues

Sandia National Laboratories

- Awareness of potential computer issues
- Need tools and new approaches to avoid computer issues and adequately leverage e-discovery in your case

- **Data Organization and Analysis Process**
  - Both legal and technology based
  - Requires coordination between the attorney, legal support staff, client, and any service providers
  - Managed by the responsible attorney
    - Counsel can avoid unnecessary exposure to potential sanctions by simply implementing and monitoring compliance with a data organization and analysis process. The following approach and accompanying descriptions should assist in formulating such a process.

Litigation Hold/Early Case Assessment Phase

Sandia National Laboratories

- **Timing:** Beginning with the decision to sue for the plaintiff, or for the defendant from the time that they are in reasonable anticipation of litigation, until the FED. R. CIV. P. 26(f) meet and confer.
- **Goal:** "Scoping" the matter by understanding the information that you have.
- **Phase 1 Tasks:**
  - Issue a litigation hold
  - Identify parties, key custodians, and non-custodial data sources
  - Begin legal research and establish legal theories
  - Technical decisions
    - Decide on data structure
    - Select, implement, and load an analysis tool to effectively analyze and review the data
  - Collect paper and ESI from key custodians and parties that are available
  - Begin looking broadly at the collected data

Litigation Hold

Sandia National Laboratories

- Issue a written legal hold to each custodian
- Define and provide the scope within the litigation hold
  - Be clear about the types and subjects of information that need to be preserved
  - Modify as the details of the matter become more clear
- Maintain a record
- Monitor and send out reminders

Select, Implement, and Load Analysis Tool(s)

Sandia National Laboratories

- Analysis is easier when all case information is in one format and in one place

- Considerations/Potential Issues
  - Skill set and budget
  - Encrypted Files
  - OCR accuracy of scanned paper varies
  - ESI may contain data types that are proprietary or are not supported by review tool
    - May have to review these natively

Early Case Assessment

Sandia National Laboratories

- As data is loaded, the attorney has the opportunity to use Early Case Assessment Tools to:
  - Determine/Confirm the relevant time period of the matter
  - Identify key words that produce relevant ESI
  - Identify additional custodians and non-custodial data sources
  - Review e-mail communication chains
  - Adequately prepare for the Rule 26(f) Meet and Confer so that the document review is scoped effectively.

Active Discovery Phase

Sandia National Laboratories

- **Timing:** Beginning with the FED. R. CIV. P. 26(f) meet and confer and proceeding until the scheduled close of discovery
- **Goal:** Analysis of the data continues and the focus is further narrowed to the most relevant case issues and data
- **Phase 2 Tasks:**
  - Narrowing Case Issues
  - Culling Data in Accordance with the Rule 16 order
  - Document Review
    - Tips for Effective Final Document Review
  - Managing the Data Volume
  - Authenticating Data

Narrowing Case Issues

- FED. R. CIV. P. 26(f) "Meet and Confer"
  - Results in Joint Status Report with Provisional Discovery Plan
  - Combined determination of the relevant time period, custodians, file types, and subjects/keywords that will receive emphasis during discovery.
    - Maintain the spirit of FED. R. CIV. P. 1 to work towards a "just, speedy, and inexpensive determination of every action and proceeding."
  - Key opportunity, based on Early Case Assessment results, to tailor discovery appropriately to minimize costs
  - Decide on the format of disclosures 26(f)(3)(A)
    - PDF, single or multi-page TIFF, native, with/without load file, or paper based
  - Decide how to handle inadvertent disclosure of privileged ESI through "claw back" Agreements 26(f)(3)(D)

Culling Data in Accordance with Rule 16 Order

Sandia National Laboratories

- From this point forward, focus is on the “responsive” data only and all other collected data is filtered out.
  - Data not previously collected, but requested via RFP or interrogatories can be collected and added as needed if modifying the order.
  - If not done already, load initially “responsive” documents into a review platform.

Document Review Platforms

Sandia National Laboratories

- Review Platform- software packages that allow the attorney and other selected reviewers to quickly review large sets of documents for litigation purposes
  - Allow the reviewer to search, filter, annotate, and categorize the data to facilitate litigation
  - Additional Benefits
    - Ability to filter out duplicate documents
    - Capability to mass categorize many documents at once
    - Ability to redact from a document slated to be produced.

Tips for Effective Final Document Review

Sandia National Laboratories

- Apply principles of project management
  - ID Key Deliverable Dates (initial disclosures, close of discovery, etc.)
  - ID and Mitigate Risks to Project Success
    - Lack of trained reviewers, ongoing collection/incomplete data
- Define Process
  - How to identify a responsive document in the case
  - How to resolve issues with the software

Phase 3: Data Archival

Sandia National Laboratories

- **Timing:** begins after the close of discovery and ends with the conclusion of the matter.
- **Goal:** properly identifying data that needs to be archived from data that can be safely deleted and proceeding accordingly.
- **Phase 3 Tasks:**
  - Review data retention policies, archive and delete in accordance with the policies.
  - Once the matter is resolved, release the litigation hold

Tips for Effective Final Document Review

Sandia National Laboratories

- Create Categories based on issues
  - Be careful with the number of categories due to human limits
  - Create a category for documents that require a second look
- Sample reviewed documents for accuracy on regular basis and regularly share lessons learned with review team
- Leverage internal capabilities of the tool
  - Search for documents marked both as ‘responsive’ and ‘non-responsive’
  - Rules that enforce category logic

Getting Familiar with File Systems…

Sandia National Laboratories

- File Systems- a system that stores, tracks, and retrieves data on a storage device (hard drive, flash memory, etc.). The file system interfaces with the operating system and the operating system interfaces with the user.
  - File Allocation Table 12 (FAT12)
    - Filenames can only be eight characters, three character file extension, older file system (predecessor to NTFS).
      - Most USB keys come preformatted to use FAT 32
  - New Technology File System (NTFS)
    - The file system of modern Windows OS (Since Windows NT 3.1), can track additional metadata, provides access control lists, journaling, supports larger volume sizes, longer file names, longer paths, a maximum file size of 16 Exabytes.
  - Hierarchical File System Plus (HFS+)
    - The file system of modern Macintosh OS X, provides access control lists, maximum file name length of 255 characters, a maximum file size of 8 Exabytes.

Getting Familiar with File types

Sandia National Laboratories

- Microsoft Office & Adobe Acrobat
  - Word (.doc, .docx), Excel (.xls, .xlsx), PowerPoint (.ppt, .pptx), OneNote (.one), Adobe Acrobat (.pdf)
- Email
  - Exchange/Outlook- .pst, .msg, .eml
  - Lotus Notes- .nsf
  - Applemail- .mbox,
  - Entourage- .emlx
- Web pages
  - .htm, .html, .aspx, .jsp
- Compressed files
  - .zip, .gz, .rar, .jar, .tar
- Image, Video, and Audio files
  - .jpg, .gif, .tiff, .png, .bmp, .mpg, .mov, .mp3, .wav, .wma, .m4a

File Locations Common to E-disco

Sandia National Laboratories

- Within a computer
  - The User's profile contains data and settings associated with a specific user. The location varies depending on the operating system.
    - Windows XP
      - C:\Documents and Settings\<UserName>
    - Windows 7
      - C:\Users\<UserName>
    - Mac OS X
      - /Users/<UserName>
    - May contain any number and type of user created files, downloaded files, bookmarks, browser cache, audio files, video files, music files, picture files
  - Default Software installation location
    - Mac OS X: /applications
    - Windows 7: C:\Program Files, C:\Program Files (x86)
    - Contains application specific files that will inform you of what applications are installed on the drive
  - Look for other user created folders within the computer

File Locations Common to E-disco

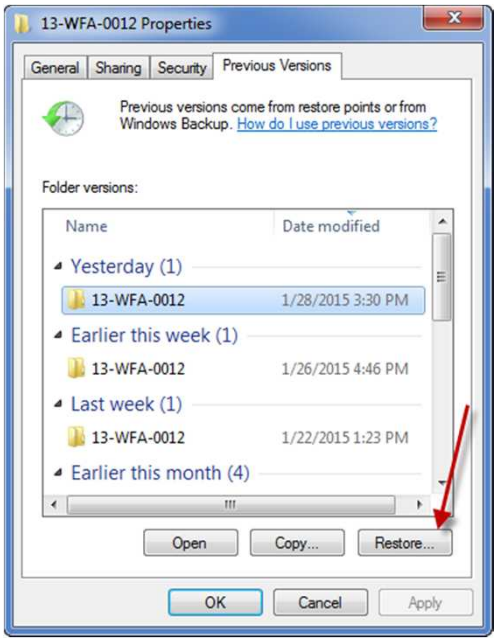
Sandia National Laboratories

- Within a mobile device
  - Locations and file types vary widely between devices
  - Information you may be able to obtain from a mobile device:
    - Calendar, call log, chats, contacts, GPS locations, installed applications, SMS messages, voice mails, notes, bookmarks, web browsing history, wireless networks accessed, audio files, video files, and image files.
- Within a corporate environment
  - E-mail servers- Exchange, Lotus Notes
  - File servers- project specific and corporate
  - Collaboration servers (e.g. SharePoint Sites)
  - Databases that support corporate systems (SQL Server, Oracle)
    - financial systems, HR systems, etc.

Practical Tech Tips: Recovering Data

Sandia National Laboratories

- Recovering lost or deleted files when using Windows 7/8.x
  - Restore files from backup if the user was using Windows backup by clicking on Start\Control Panel\System and Security\Backup and Restore, then select the backup that contains the file to restore and then search for the file.
  - Restore previous versions from restore points or Windows Backup by locating the folder that you believe might contain deleted data, right-click on it and then select "Restore previous". If there are older versions of folders and files they will appear, and you can then select and drag and drop the folder or file to restore them to a different location.



Practical Tech Tips: Recovering Data

Sandia National Laboratories

- Recovering lost or deleted files when using Mac OS X
  - If the user enabled “Time Machine” backups, open up the “Finder”, select “Time Machine” and then choose “Enter Time Machine”. Use the timeline on the right side of the screen to locate the date/time of the backup that you want to recover or search for a file/folder by name that you wish to recover. Once you locate the backup/folder/file that you wish to recover, click on the “Restore” button and select the location where you wish to have it restored.

Practical Tech Tips: Archiving and Preserving Data

Sandia National Laboratories

- Define an organizational structure for your files and folders with a naming convention and use it consistently.
- Utilize compression utilities to minimize the size of the data
- Utilize a backup utility
  - External media (hard drive, USB key, DVDs, etc.)
    - Ensure that a process is put into place to backup the files on a regular basis either manually or preferably by using software.
  - On-line cloud provider
    - Ensure that the data is encrypted while in transit and while at rest
    - Review the terms of the license agreement to ensure that you are comfortable with the details of how your data will be stored, the availability of that data, and what happens if the cloud provider should fold.

Practical Tech Tips: Sharing & Retrieving Data

Sandia National Laboratories

- Send data via the mail or similar delivery service
  - Utilize software to encrypt the media, utilize a strong password, and send the password via e-mail or provide over the phone.
  - Utilize hardware devices with built-in encryption
    - USB keys
    - External hard drives
- Send data via on-line cloud provider
  - Ensure that the data is encrypted while in transit and while at rest
  - Review the terms of the license agreement to ensure that you are comfortable with the details of how your data will be stored, the availability of that data, and what happens if the cloud provider should fold.
  - Setup accounts for users who are allowed to access and/or upload data.

Practical Tech Tips: Presenting Online Data

Sandia National Laboratories

- Online data cane be challenging, as it can be dynamic
  - Static and dynamic websites, blogs, video outlets, and social media sites such as Facebook, LinkedIn, and Twitter.
- Options:
  - Capture a “screen-shot” using an application that can take a picture of the screen.
  - Capture the HTML files that create the static web pages, save them locally to a computer, and display the files using the local browser on a computer.
  - Save video files, locate and acquire the software necessary to play the video, and play the video from a computer.
  - Purchase special software that collects data from social media, video, and dynamic websites via APIs (application programming interfaces) and in essence crawls links to pull in all the information and present it via the special software.

Latest/Greatest Tech Tactics & Handy Tips

Sandia National Laboratories

- Document and follow a process
  - E-discovery is first about good processes, then applying technology.
  - If not the “Data Organization and Analysis Process” that has been presented here, create a process that takes into account all the e-discovery steps and works for you.
  - There are just too many steps in e-discovery to not document the steps.
- Create cheat sheets for complicated procedures
  - Smart attorneys and smart information technology professionals create cheat sheets to remind them of important steps and “gotchas”.
- At the end of each case, review what went well and what could have gone better. Implement improvements.
  - Modify process and cheat sheets to capture improvements so you don’t repeat past mistakes.

Questions and Answers

Sandia National Laboratories