The Essentials of Digital Forensics

By Sharon Nelson, Esq., John W. Simek, Michael C. Maschke and Brandon Barnes

The popularity of electronic devices is greater than ever, focusing more attention on the valuable data these devices hold. In legal matters, electronically stored information (ESI) is involved in nearly every matter, requiring ESI to be collected, searched, and interpreted. To ensure proper procedures are followed and the most up-to-date techniques are utilized, a digital forensics expert is often required. The expertise needed to accurately collect, examine, and report on digital evidence requires a skill level above and beyond the capabilities of most end-users or information technology personnel.

The term digital forensics originated from the term *computer forensics* and has been upgraded to include various devices that hold ESI other than computer systems. Digital forensics experts are now preserving and analyzing more mobile devices than computer systems.

Some examples of data found on both computers and mobile devices include electronic communications such as email messages, instant messages (IMs), chats and text messages, databases, web-browser history, multimedia such as pictures, audio and video, configuration and activity logs, and third-party application data.

Some frequent sources of ESI include:

- Mobile phones
- USB flash drives and external hard drives
- Laptops, desktops, tablets (Surface Pro devices)
- Social media accounts
- Backups
- Cloud storage
- Web-based or locally stored Email sources
- Email accounts (Microsoft 365)

There are many steps involved in digital forensic analysis. Depending on case specifics, an examination can include planning, collection, and preservation of data, evidence processing, analysis, data production, and expert testimony. Some of the common tasks encountered during a digital forensic examination include finding evidence that is not readily available and preserving that evidence for admissibility in court, recovering previously existing information, and reconstructing data and tracing artifacts for clues about how a computer device was used.

A digital forensic expert must be knowledgeable about current, past, and emerging technologies in addition to understanding the forensic methodologies, techniques, and tools that apply to the technology architecture. This knowledge is obtained through years of education, training, and performance. In this field, education never ends.

The Stages of a Digital Forensic Investigation

Planning – An examiner must understand what the client's requirements are and know what information they are seeking to document or recover. The examiner must also be knowledgeable about where the responsive information may be stored and what tools or techniques they will use to review the information that is found. Knowing all of this information and being cognizant of any deadlines or budget constraints, the examiner will formulate a plan to create a faster and more efficient workflow as well as meeting the client's expectations.

Collection and Preservation – The collection of ESI is the second stage that allows the examiner to make a copy of all available data stored on the electronic data source. To start, the examiner will determine the best methods to access the storage locations and collect the targeted data.

Generally, there are two preservation options: absolute and partial. Absolute preservation can be achieved by acquiring a bit by bit copy of each storage device on which the ESI is stored. This process is sometimes referred to as a "physical acquisition", or "physical image", or "physical dump" when dealing with mobile phones. A physical image contains all of the data on the original storage media. This includes existing and previously existing files, free space, slack space, and unused space. A physical image provides certainty that all accessible and inaccessible ESI has been captured and preserved.

Partial preservation is typically achieved by only collecting "readily accessible", "existing", or "active" data. This preservation method is also referred to as a "logical acquisition" or a "logical image." A logical image contains a selection of data from the original storage media or physical image. Logical images are acquired in situations where a physical image cannot or does not need to be obtained or where selected ESI from a physical image is being segregated for further examination.

Whatever preservation method is used, verification procedures should take place which ensure the authenticity and admissibility of the ESI in court and help eliminate any basis for claiming that spoliation may have occurred. This is often performed by comparing *hash values* taken before and after the imaging process to ensure the data has not changed.

Evidence Processing – Once the available data has been preserved, it can now be processed by utilizing industry-standard software. To reduce the volume of data collection, a common practice is to perform a de-duplication process. This includes suppressing files that are exact matches, as determined by hash values, to avoid additional processing. An additional step to reduce the amount of unnecessary data is to exclude all known operating system and application program file types. Once the data to be searched has been segregated, an examiner can sort, filter, and search the ESI for responsive items.

Analysis – Now that the responsive data has been collected and processed, the analysis portion allows the examiner to correlate and interpret the available data to form opinions. The method used to analyze the available data depends solely on case specifics. For example, if a previous employee for a company was accused of using a work laptop to steal data before their departure, the examiner may review the device for previous file access, external storage devices that have been plugged in and evidence of cloud storage being used while the device was in operation. This stage will typically be the most time-

consuming, as the examiner will have to compile information from a variety of sources to render an informed and accurate opinion.

Data Production – The next stage allows for the responsive ESI to be exported, formatted, and produced to the client for their review. The time necessary to provide a client with their work product will vary depending on the amount of data necessary to be produced. There are many different types of formats available for data production, ranging from a PDF document to a searchable Excel worksheet.

Expert Testimony - The final stage includes the drafting of a formal report and/or providing expert witness testimony at depositions or in court. This stage is often not necessary, as the examination results may not be favorable, and a report or testimony may not be needed. And, of course, there is always the possibility of the case settling before the trial occurs. If testimony is needed, an expert report will often be produced. An expert report will document the steps taken during the previous project stages and provide a detailed outline of the examiner's findings and their interpretation of those findings.

If a report or expert testimony is required, the examiner needs enough advance notice to prepare and/or discuss strategy with the client or their counsel. We often recommend that clients try the much cheaper route – getting a letter summarizing the findings – or having the experts for both sides talk while the attorneys are listening. Either path is much cheaper than having a full expert report prepared.

Types of Digital Forensic Examinations

Now that the basic steps of a digital forensic examination have been covered, it's important to be aware of some of the most frequent requests we receive, as well as some of the common misconceptions.

Deleted Data – It is possible to retrieve previously existing data from most devices. However, not every piece of data that was ever created by or viewed on the computer device remains indefinitely. Data will still be recoverable until it has been overwritten by other data; and because data is not overwritten in any defined order, what data remains is completely random – it may be the document deleted two minutes ago, or the email deleted two years ago. This is very frustrating to clients because it often means that finding the evidence they want is a roll of the dice.

Internet History - Most web browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari record a user's activity – logging what internet resources were visited and, in some situations, what files they accessed on the computer device itself. Even when a user attempts to delete this information, the browsing activity can often be recovered. If the ESI hasn't been overwritten, a forensic expert should be able to identify the exact time, resource, and sometimes the content of the web-browser activity.

Finally, private browsing, incognito mode, or whatever term a browser uses to classify internet activity that is not traceable, isn't private or hidden. Even though there tend to be fewer internet artifacts when private browsing is enabled, some data remains.

Email - The first step in an email examination is to understand the email environment and how email is being used by the relevant custodians. Is the relevant party hosting their email or is there a third-party host? What type of software is being used to store and communicate email? Is their access via a web browser or mobile device? Is email synchronized across multiple devices? The answer to these questions will help identify where email items may be found.

Most users believe that once they delete an email, the message is unrecoverable. However, an examiner will frequently recover items even after they've been sent to and removed from the "Deleted Items" or "Trash" – an action known as "double-deletion". Many users also fail to understand that an email has a sender AND a recipient or multiple recipients. So an email they deleted may also be found in another user's mailbox. Emails may also reside on servers or in backups that were created during the normal course of business.

In certain situations, a user may utilize an email-client program, such as Microsoft Outlook, Apple Mail, or the client built into their mobile device, to communicate with the webmail account and store a copy of the email in the account locally on the device's hard drive.

Text Messages - Text messages and iMessages are other highly sought-after items. With hundreds of billions of messages sent every month in the United States, the importance and use of text messages in litigation is ever-increasing.

For a digital forensic expert, the ability to recover previously existing text messages and communications from a mobile phone is dependent on the make/model of the phone, the length of time that has passed since the messages were deleted, the number of new text messages that have been sent/received since the messages were deleted, and whether the deleted messages have been overwritten. Furthermore, the make/model of the phone will need to be supported by the forensic hardware/software the expert uses – if the hardware/software cannot communicate with the phone, the data cannot be accessed and preserved.

In these situations, even the best digital forensics expert will be forced to painstakingly take digital photographs of the existing text messages as they natively appear on the mobile phone. And yes, these are admissible in court with your expert explaining the process used to capture the information.

Third-Party Application Data - Another recent source of communications is the increased usage of apps. In-app communications (applications that have built-in communications capability) such as Snapchat, Instagram, Signal, WhatsApp, and others have become much more popular than text messaging. Sometimes, in-app communications are held in a database on the smartphone and not discretely (message by message) stored as other messages. For many communication apps, the data and communications are stored in the cloud and not located on the actual device.

Considerations when Retaining an Expert

When considering a digital forensic service provider, make sure you request and review the current curriculum vitae (CV) of the person(s) who will be performing or peer-reviewing the examination. The CV is a roadmap of what makes the expert an expert and can provide insight into the expert's knowledge, skills and abilities as they relate to digital forensics. What is their professional experience, what training and certifications have they received and have they provided expert testimony? A well-rounded expert, one that is experienced, well-vetted, and able to relate the most complex issues to the average jury, will present your case in the best possible light. On the other hand, if the wrong expert is hired, the case may be over before it even gets to the courtroom.

Looking Forward: The Need for Digital Forensics

As each year passes, electronic storage devices continue to improve with larger storage capacities, faster hardware specs, and overall device improvements. These attractive features result in a higher amount of personal, individualized data being produced that may assist in personal or legal matters. Consulting with a respected digital forensic examiner at the onset of your matter will provide the opportunity to understand what data may be available and useful for your specific case.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com.*

Brandon Barnes *is a Digital Forensics Examiner at Sensei Enterprises, Inc. and specializes in electronic evidence analysis, data recovery, and forensic reporting. Brandon is an EnCase Certified Examiner (EnCE). He originates from Pennsylvania, where he received his Bachelors of Science in Digital Forensics at Bloomsburg University. bbarnes@senseient.com*