The Essentials of Digital Forensics

by Sharon D. Nelson, Esq., John W. Simek and Jesse M. Lindmar

Collecting, assessing, investigating, and analyzing digital evidence requires specialized knowledge, skills and abilities – making digital forensics as much an art as a science. Computers, mobile phones and other data storage devices can hold a wealth of electronically stored information (ESI) that mandates a level of expertise above and beyond that of most end-users or Information Technology personnel to discover.

What exactly is Digital Forensics? Simply put, it is the preservation, identification, recovery, authentication, extraction, documentation, investigation, analysis, and interpretation of electronically stored information (ESI). Simple, right? Some of the common tasks encountered during a digital forensics examination include: finding evidence that is not readily available and preserving that evidence for admissibility in court, recovering previously-existing information, reconstructing residual data and tracing artifacts for clues about how a computer device was used. A digital forensic expert (DFE) must be knowledgeable about legacy, current and emerging technologies in addition to understanding the forensic methodologies, techniques and tools that are applicable to the technology architecture. This knowledge is obtained through years of education, training and performance. In this field, education never ends.

As the name would suggest, Electronically Stored Information (ESI) is information that is stored electronically. A broader definition would include any information created, manipulated, communicated, stored and best utilized in digital form. Some examples of ESI include word processing documents, spreadsheets, presentations, electronic communications such as e-mail messages, instant messages (IM), chats and text messages, web-browser history, multimedia such as pictures, audio and video, and configuration and activity logs. Most of us assume that ESI is almost always found on a computer system, such as a desktop, laptop, workstation or server – and for the majority of situations that would be correct. However, in this digital age, there are many more locations where ESI can be found:

- Mobile Phones
- Digital cameras
- Flash Memory
  - SD cards, USB drives
- Compact Discs (CD), Digital Video Discs (DVD), Blu Ray Discs (BD)
- Backups
- Cloud Storage
  - *Dropbox*, *Amazon Cloud Drive*, *Google Drive*, *Box.net*
  - Webmail
    - *Google Mail*, *Yahoo Mail*, *Windows Live* (*Hotmail*, *MSN*), *AOL Mail*
- Databases

Depending on the type of ESI that is being searched for, it could be found in multiple locations.

The digital forensic project lifecycle involves six main stages:

1. Planning
2. Collection / Preservation
3. Processing / Evidential Assessment
4. Investigation/Analysis
5. Production
6. Reporting / Expert Testimony

Like any successful project, planning is key and, in our opinion, is the most important stage of the project lifecycle. A DFE will need to understand what the client's requirements are – what information they are seeking, where the responsive information may be stored, how they plan on reviewing the information that is found, and the deadlines or budget constraints. Knowing all of this will allow the DFE to formulate a plan for successfully completing the project and maximizing the amount of responsive data and, very importantly, meeting the client's expectations. Many DFEs and clients want the physical work to begin immediately. However, taking the time to map out how the project will move forward will not only allow for a more granular level of control by the DFE and client, but will also result in a faster and more efficient workflow.

The collection and preservation of ESI is the second and most critical stage. Obviously, if the ESI is not collected thoroughly or correctly, there could be a multitude of issues. If a comprehensive plan has been developed, the DFE will understand the places in which relevant ESI may be found. From there, they 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-stream" image of each storage device on which the ESI is stored; this is sometimes also referred to as a "physical acquisition" or "physical image", or a "physical dump" when dealing with mobile phones. Partial preservation is typically achieved by only collecting "readily accessible", "existing" or "active" data; this is sometimes also referred to as a "logical acquisition" or "logical imaging".

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. This is typically created in a way that leaves the original source device unaltered and provides a certainty that all accessible and inaccessible ESI has been captured and preserved. It also eliminates the need to examine the original source device, whose continued operation could result in the permanent loss of previously-existing ESI. 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 select ESI from a physical image is being segregated for further examination. The acquisition and verification procedures

that take place during the creation of an image substantiate the authenticity and admissibility of the ESI in court and helps eliminate any basis for claiming that spoliation may have occurred.

In addition to its preservation qualities, a forensic image can also be explored with processing and investigation software in order to locate and recover all categories of ESI that may pertain to the case. There are numerous ways in which a DFE can interrogate an image. By compiling a list of words, phrases, dates, e-mail addresses, and other criteria, a search for responsive ESI will harvest both existing and previously-existing results. For the requesting party, the advantage of having input into the search criteria list is significant – leading to the recovery of relevant evidence that might otherwise had never been located using non-forensic methods.

Once the ESI has been collected, the next steps involve the general processing and evidential assessment of the ESI. Processing allows for the ESI to be read and displayed by the processing or investigation software. It also allows for previously-existing files to be recovered, as well as the identification of those files that require further, specific processing, such as encrypted, incomplete, compound, container, or database files. In order to reduce the volume of data, the collected ESI can be run through a de-duplication process. Files that are exact matches (determined by hash value) can be suppressed to avoid further processing. In addition, all known file types (e.g. operating system files, application programs, etc.) can be excluded from the ESI. A DFE can then organize, sort, filter and search the ESI for the responsive items. It is at this stage that the DFE will begin focusing on those types of ESI that will contain information that satisfies the client's requirements; e.g. existing or previously-existing files, metadata, web-browser history, and electronic communications. This assessment will allow the DFE to identify whether responsive ESI is present in the data set, the types of responsive ESI and the potential volume.

Now that responsive ESI has been identified, investigation and analysis techniques allow the DFE to correlate and interpret the available data in order to form opinions. For example, if a document's authenticity was in question, perhaps its content or purported creation date is in question. The DFE would review the available document versions and associated metadata, as well as any evidence of system-clock manipulation to help determine authenticity. This stage will typically be the most time consuming, as the DFE will have to compile information from a variety of sources in order to render an informed and accurate opinion. Some of the queried sources could include file system and internal metadata such as timestamps, file names and file paths, as well as encoded data, log files and databases. Most importantly, the DFE will need to know what sources to query for a given scenario.

The next stage allows for the responsive ESI to be exported, formatted and produced to the client for their review. This stage can also be time consuming depending on whether the data needs to be converted into a more readable format or to be made compatible with the client’s preferred method of review. During the planning stage, the DFE should have determined if the client has any review preferences or they should have advised the client on the available production formats. For example, will responsive files be produced in their native format (if

applicable) or will they be converted into a standardized format like PDF or TIFF (Tagged Image File Format)?

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, most cases settle. A forensics report will document the steps taken during the previous project stages and provide a detailed outline of the DFE's findings and their interpretation of those findings. As part of their policy and procedures, some DFEs will always provide a written report, while others will leave the request to the client after briefing them on examination results. If a report or expert testimony is required, the DFE 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-blown forensics report prepared.

Now that you have an understanding of the digital forensic project lifecycle, we'd like to touch on the aspects of some of the most frequent requests we receive, as well as some of the common misconceptions.

Yes, a DFE can recover previously-existing ESI, 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 written in any defined order, what data that remains is completely random – it may be the document deleted two minutes ago, or the e-mail deleted two years ago. This is very frustrating to clients because it often means that finding the evidence they want is really a roll of the dice.

Retrieving web-browser history has become a staple of digital forensic investigations. Most web-browsers, including *Google Chrome*, *Mozilla Firefox*, *Microsoft Internet Explorer*, 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 DFE should be able to identify the exact time, resource and sometimes the content of the web-browser activity. It's web-browser activity that sometimes allows a DFE to identify a particular person that may have been using the computer during a relevant time-frame.

One of the most sought after pieces of ESI is electronic communications, such as e-mail messages and text messages. We get many requests to produce "all the e-mail" or "all the text messages". However, most clients fail to understand exactly where that type of ESI may be found.

The first step in an e-mail examination is to understand the e-mail environment and how e-mail is being used by the relevant custodians. Is the relevant party hosting their own mail or is

there a third-party host? What type of software is being used to store and communicate e-mail? Is there access via a web-browser or mobile device? The answer to these questions will help identify where e-mail items may be found.

Most users believe that once they delete an e-mail, the message is unrecoverable. However, a DFE 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 e-mail has a sender AND a recipient or multiple recipients. So an e-mail they deleted may also be found in another user's mailbox. E-mails may also reside on servers or in backups that were created during the normal course of business.

Webmail is a different story. In the past, it was completely possible to forensically recover e-mail that was created or viewed by web-based e-mail systems and from free, web-based e-mail services such as *Google Mail*, *Yahoo Mail*, *Windows Live* (*Hotmail*, *MSN*) or *AOL Mail*. These types of e-mail use a web-browser to interface with the e-mail server in the cloud. Today, due to the security and functionality of the webmail services and web-browsers, less e-mail content is being recovered from computer devices. In certain situations, a user may utilize an e-mail-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 e-mail in the account locally on the device.

Text messages are another highly sought after item. With an average of 193.1 billion text messages sent every month in the United States, the importance and use of text messages in litigation is ever-increasing. The majority of text messages are sent or received by a mobile telephone falling within two major categories: Smartphones and Feature Phones. The most popular Smartphones would include *Apple's iPhone*, *Google's Android*, *Microsoft's Windows Phone*, and *RIM's BlackBerry* devices. Feature phones are pretty much everything else; having some of the basic "features" of smartphones, but lacking an overall integration with the phone's operating system and hardware, and with limited user-customization options.

Depending on the service provider, the mobile phone may or may not be equipped with a Subscriber Identity Module (SIM) card. The SIM card contains information that will validate the phone on the service provider's network, but can also be used as a repository for received text messages. Text messages can also be stored on the phone itself (as is the case with smartphones), and in some situations, messages are stored on the phone and SIM card. There are several products used within the forensic community to preserve text messages from many mobile phones – from both a SIM card and the phone itself. This will result in an electronic copy of the text messages being extracted and will include not only the content of the message, but also the date and time the text message was sent/received and information about the sender (phone number and/or contact information for a phone number if the user has added them to the phones address book).

For a digital forensic expert, the ability to recover previously-existing text messages 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 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 DFE 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 though your expert will likely be needed to explain the process.

Although complicated, a properly managed digital forensic examination can provide invaluable information. It can tell you whether you have a case that's a winner, or a case with a wagging tail. It helps you determine whether to discuss settlement or go the distance. 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; 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. And if it gets to the courtroom, the courtroom floor may be stained with a poor expert's figurative blood under cross-examination.

The authors are the President, Vice President and Director of Digital Forensics at Sensei Enterprises, Inc., a digital forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) sensei@senseient.com *(e-mail)*, http://www.senseient.com.