

•• Mitigating Risk with Digital Forensics and EDD

How Best to Apply These Services

John H. Evans of Project Leadership Associates

Due to the proliferation of electronically stored information, nearly every type of legal matter can require digital forensics and/or electronic discovery. While some may think these services are too expensive to outsource, the inherent risk of an improper investigation or data collection can be much more damaging and costly.

About Digital Forensics

Digital forensics may be defined as the search for, collection of and analysis of electronic evidence in a standardized and well-documented manner to maintain admissibility and probative value in a legal proceeding. More simply put, it is a controlled investigation of electronic data, with the operative word being “controlled.” Through the use of industry-standard and court-approved forensic software, a trained and experienced digital forensics investigator can help reduce risks associated with an investigation. When conducting an investigation, a digital forensics investigator strives to do the following:

Preserve and secure electronic evidence using methods that withstand judicial scrutiny

Obtain all potentially relevant data

Maintain chain of custody at all times

Minimize cost and business disruption

Conduct a structured, repeatable investigation

Document, document, document!

To achieve these goals the investigator follows a standardized approach that can be divided into five phases: identification, preservation, collection, analysis and presentation.

Identification

Identification is a crucial first step that sets the tone for all subsequent steps. To conduct a thorough investigation, the investigator must consider all possible locations of pertinent data. These locations may include computer hard drives, network resources, handheld devices such as smart phones, and loose media such as USB flash drives, CDs and DVDs. The investigation may also uncover additional sources of data. The investigator must work closely with the client to identify all possible data points and ensure that no potential crucial data set is overlooked.

Preservation

Once the data has been identified, appropriate preservation processes should be applied to ensure the collected data

remains unaltered. This may be accomplished through the use of specialized hardware and software. For example, hardware “write blockers” allow for the collection of data without altering the source; such devices are critical in this phase. There is tremendous risk involved at this stage. Evidence that is improperly collected or spoiled may be inadmissible in court. For this reason, organizations should strongly consider the use of outside experts for collection.

Documenting chain of custody is also integral to proper collection. The purpose of chain of custody documentation is to account for the whereabouts of data or devices from the point of collection to the moment they are offered into evidence. Often, internal collections are not properly documented.

Collection

Once the appropriate preservation and documentation processes have been applied, the collection takes place. In a forensic collection, a “bit-stream” or “bit-for-bit” image of the data storage device is created. This means that the image is an exact duplicate of the source, including all possible physical storage space of the device. Verification is necessary to confirm that the image is in fact an exact replica of the source. This is accomplished by calculating hash values for the source data and the image. A hash value can be thought of as a fingerprint for a quantity of data. The hash value is a fixed-length string of letters and numbers that is computed by applying a mathematical algorithm to the data set. An image is considered verified when the computed hash values match. From this point forward, the forensic examiner will only operate on the image, not the original media. It is also standard procedure to make a backup copy of the image at this point to safeguard against the risk of hardware failure or loss.

Analysis

The next phase is to analyze data within the image. Many analysis tools are available, but it is generally considered best practice to employ forensic tools that are widely used, tested and court-recognized. Two of the most common and well-known tools are Guidance Software’s EnCase, and AccessData’s Forensic Tool Kit.

The analysis phase is generally the most time-consuming in that the goal is to locate evidence that answers questions about particular activities. The investigator needs to know as much about the matter as necessary to answer questions such as: Was the computer used to access certain documents? Did a user communicate with someone else about a particular topic? Were external storage devices connected to a computer? Were particular items deleted? Discrete analysis is performed to answer these questions. Ideally, the result of this analysis will locate evidence that proves or disproves a certain activity. A qualified,

- experienced and properly trained investigator will possess the know-how to find answers, recreate timelines and recover notable data.

The two general areas of potential evidence on an electronic data storage device are allocated space and unallocated space. Allocated space refers to those areas of an electronic data storage device that are tracked by or allocated for use by the computer's operating system. This may include user documents, program files, operating system files, temporary files and Internet history files. Unallocated space comprises all remaining areas of the electronic data storage device. This space is not tracked by or allocated for use by the operating system. Unallocated space may contain deleted files and fragments of deleted data or "artifacts." Experts employ several tools and techniques to cull the collected data and locate evidence, including searching keywords, conducting file hash and signature analysis, reviewing graphics files, analyzing file activity, analyzing user activity, analyzing device activity and recovering data from unallocated space.

Presentation

The final phase, presentation, commits all previous phases to writing. Investigators' reports should articulate what data was identified, the preservation methods employed, how the data was collected, the tools used to analyze the data, what evidence was being sought and, finally, the results and conclusions. As circumstances warrant, investigators' reports or findings may be included in affidavits, declarations and other documents submitted to the court. Furthermore, investigators may need to testify in court to establish their education, training and experience as well as to explain their analysis for the particular matter.

About EDD

Electronic data discovery may be defined as the process by which potentially relevant data residing in a particular computer system is identified and collected. The key difference between electronic data discovery and digital forensics is the scope or volume of data collected. As described above, a forensic collection, or forensic image, copies literally every bit of information, whereas an electronic data discovery collection copies only particular data. This particular data may be designated by file types such as word processing documents, spreadsheets, e-mail messages and CAD drawings. It may be further defined by additional parameters such as a date range. Electronic data discovery collections are sometimes referred to as "active data collections" because only active items residing in the allocated space of electronic storage devices are collected.

While an electronic data discovery collection is generally less involved than a digital forensic investigation, it is no less fraught with risk. As with a forensic collection, the use of proper tools and techniques can mitigate risks such as undercollecting, overcollecting, or altering metadata during an electronic data collection.

Given the relatively high costs of digital forensic analysis and electronic data discovery, organizations may be tempted to allow in-house IT or information security personnel to conduct some or all of the tasks described. The business manager or internal legal counsel may think that self-discovery is more economical, but the inherent, embedded risks outweigh any potential cost savings. The primary weakness is that the IT staff is not typically trained in the proper techniques and tools used to conduct forensic or active data collections. They rely on

the tools with which they are familiar, and which can lead to partial collection, inconsistent methods and unintentional spoliation of the data. In addition, response time may be slow as they continue to perform their regular job duties. Questions of bias and the potential for intentional exclusion of sensitive data also exist. Finally, individuals responsible for the data collection may be called to testify in court regarding their expertise in evidence handling. An untrained person is an easy target under cross-examination.

Digital forensics investigations and electronic data discovery are far-ranging and complicated processes that are best handled by properly trained and experienced professionals. By engaging these trained professionals, organizations can mitigate risk, avoid the pitfalls and optimize chances of achieving the desired results.

About our author :: :: ::

John H. Evans is a senior forensics consultant working for Project Leadership Associates in Chicago. He can be reached at jevans@projectleadership.net.