AVANSIC®
E-Discovery & Digital Forensics

You Still Need Forensics, Even in a World of E-Discovery

Forensics and e-discovery share a goal: to locate digital evidence to support investigations or fact discovery. E-discovery is content-based but digital forensics focuses more on context. E-discovery helps inform the "what" of a given scenario and forensics can help identify the "how" and "when."

For example, an e-discovery document review would identify a key email. However, a forensics investigation of that email and the computer it resided on, would show how the email arrived at the computer, how often it was opened, if it was sent to another location, and more. Digital forensics can tell the rest of the story.

Getting Through the Data

In digital forensics, the basic unit is a data element (such as a registry entry, a link file, or log file). In e-discovery, the basic unit is a document (such as a file or an email). It is common for a digital forensics investigator to review millions of data elements in a single day in order to locate the evidence for a particular investigation; however, e-discovery teams might take weeks to review millions of documents even with the help of modern analytics tools.

A forensics investigator can see how an individual document fits in the context of the rest of the computer. For instance, an investigator could determine that a particular file was modified by a user but not while they were sitting at a computer by looking at the registry historical information, computer log files, and individual documents.

Cool Things Forensics Can Do

Forensics excels in authentication but e-discovery does not lend itself to it. Imagine a scenario where a key email produced by the opposing party is detrimental to the case. A search of the documents for this and similar emails doesn't locate anything. A forensics investigator notices inaccurate extended header information – the email was dated after its supposed transmission – and further investigation supports the theory that the email is not authentic and had not been sent.

Digital forensics can provide a clear picture of user activity on a given device including dates and times that documents were copied onto thumb drives (or other external media), when documents were deleted, what websites were visited, and more.

Carved, Deleted, Orphaned Data

It is commonly known that when a file is deleted on a computer it may not be immediately inaccessible. Deleted files can be recovered from recycle bins and trash cans. Even after emptying these, files can persist as orphaned or double-deleted data that may be instantly recovered using the file system. In a case where data is not instantly recoverable, data carving may locate fragments of files through intensive data scanning.

In forensics, carved, deleted, and orphaned data is always considered because deleted items can have a place in the story about what happened on a computer - in some cases, they are the story. In e-discovery, such data may not be considered because they are not the focus of the case and data fragments are difficult to analyze for those without computer science expertise.

Personnel: Procedural vs. Investigatory

E-discovery technical personnel follow procedures to process data, handle exceptions, and perform extensive quality control checks. Digital forensics examiners use an investigatory process that shares similar elements from case to case but largely depends on the type of case, operating system, and investigative requests.

Forensics requires a much greater knowledge of computer operating systems and the way that various pieces of those systems interact. Digital forensics investigators are generally given a scenario, told what they might be looking for, and are then left to perform the investigation under the basic investigative framework. E-discovery can come closer to an investigative model when the results of an initial review of a custodian are used to inform the filtering and search methodologies for additional custodians.

Conclusion

Both digital forensics and e-discovery are important pieces of the toolkit. Attorneys and corporations are wise to use their different approaches – investigative vs. process-based – for their strength in a given case. Goals can change mid-case and having both e-discovery and digital forensics experts available ensures a smooth and timely progression of a case.