E-Discovery Collection

Description

E-Discovery Collections also known as Electronic Evidence Discovery (EED) or Electronic Data Discovery (EDD) can include a review of all the data stored on employee desktop or laptop computers, company servers, camera cards, cell phones, smart phones, GPS devices, digital video recorders, digital answering systems, thumb drives, RAID arrays and any other form of electronic media capable of storing data.

Types of Electronic Discovery Content

Employee Work Product â?? Computer Files are by far the most common arrangement for a forensic e-discovery collection. Files (also referred to as loose files or active files) are similar to their paper equivalent. They can be copied, moved, and even â??shreddedâ?•. Work product could include sales reports, QA reports, product or service information, client lists, engineering designs and much more.

Employee Correspondence â?? Email has practically replaced letters and interoffice memos. A forensic e-discovery collection of correspondence is often a critical piece and can often contain the â??smoking gunâ?•. What someone said, to whom, and when are some of the first questions asked in a legal matter. Since emails are a form of documented communication, they comprise highly sought-after data when it comes to legal matters. Emails themselves may be contained in databases, files, or unallocated space.

Customer Relations and Accounting Data â?? Customer lists, internal notes, and financial records are also a critical component in forensic e-discovery collection or computer forensic investigations. Properly collecting the live database files that store this information can be a challenge. Single entries in a database often require export to another format in order to be useful or even readable by humans. Most databases include this ability.

User Logs â?? Collecting user logs isnâ??t always as relevant in an e-discovery collection/review as it is in computer forensics analysis, however, they can be and are worth mentioning. User logs will contain entries about the activities performed on a computer and different user accounts. Attorneys may want to know when emails were sent or received between accounts in case the emails were deleted. Log entries may require conversion into human-readable form before they can be processed.

Raw or Unallocated Data â?? Unless a forensic image of the source data has been requested a forensically sound e-discovery collection will focus on â??activeâ?• files. However, it is helpful to understand the difference between â??unallocatedâ?• and â??activeâ?• data. Raw or unallocated data is data that resides in segments of the storage media (hard drive, camera card, etc) that are not being used by files. This data can contain all or part of files that were once referenced in the file allocation table but were subsequently deleted. Much of this data can even survive a reformatting of the disk itself. Since this

data can come from any number of sources that had once been active on the drive, it can make or break a case where it is suspected that deletions may have occurred.

Tools for Forensic E-Discovery Collection

With the exception of unallocated space, tools such as One Click Collect Harvester from Pinpoint Labs have the ability to collect loose files, emails and whole databases with the added benefits of being able to specify key words, date ranges, domains and email addresses among other very useful filters.

Tools for collecting the unallocated space on a drive usually require an experienced forensic examiner in order to get useful interpretations of the data collected. In cases where this is necessary, it is recommended that a certified computer examiner be hired for the collection and analysis of the data.

Date
11/03/2026
Date Created
12/08/2010