What is ESI (Electronically Stored Information)?

Description

ESI (Electronically Stored Information) is the general term for all of the data stored on the hard drives, camera cards, cell 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 Electronically Stored Information:

Files â?? Files are by far the most common arrangement for ESI data. Files (also referred to as loose files or active files) can be thought of as data containers similar to files in the real world. They can be copied, moved, and distributed freely on a variety of different media from DVDs to hard disk drives.

Emails â?? Emails are messages sent from user to another. In their raw form, they are simply a stream of data that contains everything needed to get the message from one user to another user. 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.

Database Entries â?? Database entries is data stored in a database. This type of data is usually context-specific and may be information pertaining to financial records, personnel entries or other data that is interrelated. Single entries in a database require export to another format in order to be useful or even readable by humans. Most databases include this ability.

Log Entries â?? Log entries are lines in files or entries in databases that contain information about activity on a particular computer. The more commonly useful log entries pertain to users logging into and out of a computer, accessing specific internet sites, the sending or receiving of email or other messages and the moving, copying or accessing of files on the computer. Log entries may require conversion into human-readable form before they can be processed.

Raw or Unallocated Data â?? 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. It can also contain deleted internet history, old information from the computerâ??s RAM (Random Access Memory) or even old configuration data about the computer itself. 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 Collecting ESI

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 examiner be hired for the collection and analysis of the data.

Date
11/19/2026
Date Created
12/01/2010