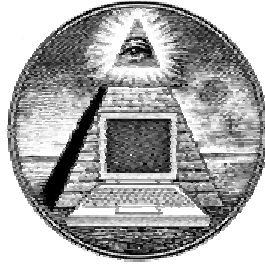


ASR



DATA ACQUISITION & ANALYSIS, LLC.

Forensic Methodology

ASR Data has developed a computer investigation protocol that has been optimized to integrate computer science and forensic science. This protocol is in use by virtually every major law enforcement agency in the United States and Canada and has never been successfully challenged in court.

Data Acquisition

Unless specialized software is used, the simple act of booting a computer system is almost certain to change data on disk drives connected to the computer. This results in the contamination of digital evidence and often causes vast amounts of data to be destroyed or altered before it can be copied.

Copying files or backing up a disk drive are ineffectual forensic methods for a variety of reasons. Deleted files are not copied, nor are files or partitions that are hidden. Often times, backup programs modify the attributes of files and folders by flagging them as having been backed up.

The forensic methodology employed by ASR Data is completely non-invasive to the original evidence and does not change any data on disk sub-systems before, during or after the data acquisition process. All information is copied, including deleted files, unallocated disk space, slack space and partition waste space.

Gaining access to a disk drive non-invasively may be accomplished in several ways, depending on various technical configurations. Often times, the fastest and easiest way to image an internal disk drive is to remove it from its native environment and connect it to a computer which has had its hardware and software optimized to support the forensic process. Alternatively, the drive may be left in the computer and the computer booted using a modified version of an operating system which has been "neutered" to prevent it from changing any data on disk drives connected to the computer.

3505 Cumberland Gap • Cedar Park, Texas 78613
(512) 918-9227 • FAX 512-918-9393

WWW.ASRDATA.COM • Email: info@asrdata.com

Data Authentication

Providing a quantifiable measurement of authenticity and integrity of data is essential for satisfying admissibility standards such as Federal Rules of Evidence - Article X - Rule 1003 and Federal Rules of Evidence - Article IX - Rule 901.

The data acquisition and authentication protocol employed by ASR Data has been developed to facilitate the discovery process and addresses issues raised in Federal Rules of Civil Procedure, Rules 26 and 34.

ASR Data integrates digital evidence and chain of custody information and extends the authentication paradigm to include the embedded chain of custody information.

ASR Data's methodology is fault tolerant and can authenticate data on damaged media. The protocol also supports the exclusion of privileged information while retaining the ability to acquire, authenticate and analyze hard disks, floppy disks, Zip and Jaz disks and many other types of rotating magnetic and optical data storage mediums.

Data Analysis

ASR Data has developed tools and techniques that allow us to recover data other utilities and data recovery companies miss. More than simply recovering deleted files, our advanced tools and techniques allow us to defeat passwords, discern subtle patterns of computer usage and much more.

Reconstructing an accurate history of computer activity and identifying the "signature" of user initiated actions requires an in depth understanding of computer operating systems, file systems and disk storage subsystems.

ASR Data employs a standardized scientific methodology that has been proven to be sound, effective and reliable. Optimized to anticipate a wide variety of legal foundation and theoretical challenges, our findings and opinions are virtually incontrovertible.

Soft Skills

Information obtained from the technical analysis of a computer may be of little practical value unless the information can be effectively disseminated. The presentation of information is often times as important as the information itself. Findings and opinions are presented in clear, concise terms.