

eMag Solutions offers a highly exhaustive consultative approach to computer forensic analysis to help clients recover, convert, review, and present the findings of a forensic investigation.



Computer forensics and data recovery are sometimes confused with each other. Data recovery is the process of *reconstructing* deleted or seemingly lost digital information, whereas computer forensics is the actual *recovering, preservation and analysis* of digital information.

**TAKE
CONTROL
OF YOUR
DATA**

Computer Forensics

Computer Forensics is the legally accepted practice of preservation and analysis of pertinent digital information. Its goal is to recover data that is valid, original and unaltered so it can be used as evidence in a court of law.

COMPUTER FORENSIC CAPABILITIES

- Retrieval of deleted and previously viewed E-Mails
- Retrieval of disguised and hidden files (renaming, password protecting, encryption up to 128-bit, steganography, compression, etc.)
- Able to determine installed/uninstalled applications and web sites visited
- Able to determine details of which programs were used and when the computer was last accessed
- Retrieval of timeline analysis (log file) to show what the user did and when it occurred

ITEMS TO CONSIDER

- E-Mails may be saved on a computer simply by viewing them
- E-Mails might be fragmented and need to be reconstructed
- Data can reside on a computer for many years
- Web page views leave “virtual footprints” which allow experts to determine which sites were viewed, when and if data was collected
- Secondary internet-based E-Mail account use (i.e. Hotmail, Yahoo!) can be determined and analyzed from individual work stations

This information is useful in the creation of event timelines, uncovering malicious content (ex. Spyware, wiper programs, etc.) and determining if a violation of agreements has occurred.

COMPUTER FORENSIC EXAMINATION STEPS

Forensic specialists take great care in extracting and consolidating data that could potentially be viewed as evidence in a case and could lead to possible litigation.

Data Preservation

It is crucial to understand that when any device (PC, laptop, etc.) starts, operates or suspends, data may be changed, modified or deleted. Before a device is turned on or off, eMag should be contacted to help avoid the potential for spoliation. State of the art forensic tools are used in this process to ensure the examination will be done without compromising the integrity of the data (potential evidence).

Investigation

The method in which data is collected can be the most scrutinized aspect of a digital investigation. The initial investigative response includes investigating the type of operating system running, interviewing key users of an organization and determining the best approach to protect the data involved.

Data involved in an investigation can come in all forms:

- PCs and laptops
- Cell phones and digital cameras
- Mainframes or servers
- Tape backups, thumb drives and PDAs



COMPUTER FORENSIC EXAMINATION STEPS continued

Imaging

Imaging is a bit-by-bit replication of the original digital evidence. eMag uses court approved methods and software in order to capture a forensic image copy (MD5 hash) of the hard drive, which ensures output is fully admissible in court.

eMag experts are able to copy all forms of active storage media and backups that could be used as potential evidence. eMag is also able to view deleted files, printed documents, internet related files and hidden directories, in most cases.

Analysis

The analysis phase consists of the recovery and interpretation of the information that has been collected and authenticated. In this phase, eMag is able to:

- Pinpoint a file's location on a disk
- Determine a file's creator
- Determine a file's created date, last-accessed date and deleted date
- Reveal file formatting and notes embedded or hidden
- Reconstruct computer usage

eMag experts consult with litigants and testify on their behalf regarding electronic data history, recreating a blueprint of what has happened. Because of eMag's forensically sound and court approved methodologies, the Company stands ready to defend its process.

**TAKE
CONTROL
OF YOUR
DATA**

3495 Piedmont Road
11 Piedmont Center, Suite 820
Atlanta, Georgia 30305
800.364.9838 ph
800.334.8273 fax
info@emagsolutions.com
www.emagsolutions.com