SWAILES
Computer Forensics

Experts in Digital Forensics

Swailes Digital Forensic Terminology » DataSheet

Digital Forensic Terminology

Case assessment

Not all cases are created equal. Variables such as type of concern, number of computers, background of user, etc. can help determine the likelihood of locating useable evidence. Rather than making empty promises of guaranteed results, we make educated decisions based on our experience which is just good business for you and us.

Device imaging

This is the act of acquiring forensic images or copies of suspect machines and devices. The forensic part is where an entire bit for bit or bitstream copy of evidence is captured regardless of the operating system (Windows, Mac, Linux, Unix). No matter the device: Desktop computer, laptop computer, server, cell phone, smartphone (iPhone, Android, Blackberry, Symbian), tablet (iPad, Samsung, etc.), raw hard drive, flash drive or backup tape to name a few devices and mediums.

Evidentiary snapshot

In some cases it’s not possible to take a proper forensic image (running server, damaged media, online data, etc), in which case we take what we refer to as an evidentiary snapshot. Another time this is appropriate is when the device still stays in service but a current state capture is desired in the event its needed at a later date.

Swailes Differentiators

- Extensive Civil & Criminal Expertise
- Certified Forensic Examiners
- Experienced Expert Witness in Courts
- State Licensed Investigators
- Live Testimony Experience
- Digital Evidence Preservation Expertise

Backup tape restoration

This is applicable when no other evidence exists or as a way of evaluating readily available evidence without disturbing the source. Sometimes all the data needed to establish a case is on a server backup tape. Backup tapes are also important when restoring email when needed for litigation or in response to court ordered production. This can be done from a myriad of formats, current or out of date media (including obscure backup up tape formats!) SLDT, LTO, DLT, DDS, Travan, AIT, 4mm, 8mm, Iomega ZIP, JAZZ, and Onstream to name a few.

Email Search Processing

Whether retrieved from a computer’s forensic image, an onsite copy of an exchange database, restored from tape or even given to us as an outlook PST file, we can index and return specific results based on keywords, specific time periods or just data types.

Deleted file recovery

It seems everyone knows that when you hit the delete key it doesn’t really “delete” the file but there are a myriad of ways to retrieve deleted files once they’ve gone “beyond the recycle bin”! We employ programs, scripts and sometimes just some less than common thinking when recovering data that was thought to have actually been long gone.

Meta Data File Analysis

Want to know who created that document or worked on it last? How about how long its been edited or when it was printed last? Those are simple examples but many file types besides Microsoft Office formats keep “data about data” such as that above. Oftentimes getting to the data is less than straightforward and can reveal some crucial details important in establishing culpability in a case.

Swailes Differentiators

- Extensive Civil & Criminal Expertise
- Certified Forensic Examiners
- Experienced Expert Witness in Courts
- State Licensed Investigators
- Live Testimony Experience
- Digital Evidence Preservation Expertise

Log review

Logging can take place within operating systems, servers, programs, and on routers, switches or just about anything that may later need to have a log reviewed. Reviewing such logs can yield tangible information in and of itself or can point to other sources of evidence.

Keyword Searches for evidence

A longtime mainstay of forensics, searching for specific terms, names, or companies can prove helpful in retrieving evidence of theft or other malfeasance. From a practical standpoint, oftentimes these searches do not solve the case by themselves yet they lead to the uncovering of other data of importance. They are oftentimes the staring point in a case after the evidence has been indexed.

Data Carving

When a file is deemed no longer available on the storage medium (hard drive, flash drive, etc.), carving can help either extract the information you need or piece together that lost file. Carving is just as it sounds, carving data out of either unrelated files or from a larger cache such as a swap file, page file or hibernation file.

Reporting depending on audience

End result reports for managers, human resource professionals, owners or for court purposes. While the data uncovered in the course of an investigation is typically the same we can tailor the reporting so that it is most impactful to a specific need and audience.

Swailes Differentiators

- Extensive Civil & Criminal Expertise
- Certified Forensic Examiners
- Experienced Expert Witness in Courts
- State Licensed Investigators
- Live Testimony Experience
- Digital Evidence Preservation Expertise

Swailes & Company, Inc., is a recognized leader in digital forensics & computer investigations, business investigations, due diligence investigations, security consulting, and pre-employment backgrounds & background screening, providing innovative solutions to corporations, law firms and private entities. Mitigating business risk through investigations and security management consulting is our business. TXDPS License Number A06659.
For more information, visit www.swailescomputerforensics.com
.

1800 Saint James Place
Suite 625
Houston, Texas 77056

713.977.7600
www.swailes.com
info@swailes.com