

What is Digital Forensics?

Digital forensics is the process of reconstructing and analyzing digital information. All digital information, regardless of file format, is stored in binary code, commonly recognized as 1's and 0's. Digital information can be stored on many different types of devices:

- Computers
- Cell phones
- PDA's
- ipods
- Memory sticks
- Etc.

Acquiring and Reconstructing

For all intensive purposes there are two types of data.

- Live Data- Data that currently exists in working form on the device.
- Dead Data- Data that has been deleted or destroyed and is in danger of being overwritten.

Utilizing forensically sound tools and techniques it is possible to not only analyze the live data but the dead data as well. When we say "forensically sound" we speak on process used to insure that the integrity of the evidence including a chain of custody is maintained. An "image" or forensically sound copy of the drive is made and which can than be processed and analyzed.

Hard Drives and Evidence Preservation

Hard Drives like most digital media store information electromagnetically. The data is not stored concurrently so a single file can be stored in multiple locations on the hard drive. When the file is deleted it has simply been designated by the operating system as no longer needed. This means that as far as the computer is concerned it is acceptable to begin overwriting this file with new information.

When a device is in question it is definitely a best practice to avoid turning the device on or using it before contacting your digital forensic provider. As the computer is used the operating system is constantly writing to the hard drive and information imperative to your case can be lost.

What information can be found?

Virtually anything that has taken place on the device can be recovered. If it a hard drive from a computer it is possible to recover emails, documents, spreadsheets, databases and any other types of files. If the device is a PDA or cell phone it is possible to see call and text logs as well and email and other data stored on the device.

The Lorenzi Group is a full service, New England based provider of Digital Forensic Services. We assist clients during the acquisition and imaging, processing, analyzing, and reporting and testifying process of digital evidence management. Born out of an expressed need by attorneys for a reliable and professional digital forensics team, we work with companies and firms across the country bringing them the evidence they need. If you would like to learn more about us, the processes and equipment we use, or how to utilize our services, we would enjoy hearing from you. Please visit our website at www.thelorenzigroup.com. We can be reached directly at 1-866-632-9880 or by email at info@thelorenzigroup.com.