

Preservation

Due to the new federal rulings that took effect in December 2006 the preservation of digital information has become a major concern to attorneys and their clients. During the discovery process clients are now responsible for ALL the information on the computer including deleted or destroyed information still residing on the hard drive.

Preservation is the first and most critical step in digital forensics, and necessary if there is the possibility of litigation. The most cost effective preservation method we have found is to take a forensic image of the hard drive inside the computer in question. A forensic image is taken to avoid potential risks of spoliation of evidence. This creates a detailed snapshot of the media, and all the information it contains at the time of imaging. All data is stored in a 1 and 0 (bit and byte) format.

*A **FORENSIC IMAGE** is the exact copy of all live and dead data stored on the drive. Every 1 and 0 stored on the evidence media is copied onto a clean media, utilizing specialized hardware and software tools that will not affect the media being forensically imaged.*

To further reduce the potential of spoliation, many attorneys counsel their clients to create a second image, or “usable clone”, as well. A usable clone allows clients the opportunity to continue using the electronic device by replacing the original media with the usable clone. The original media (potential evidence) and forensic image are then stored off-site in a secure environment for later review or use.

*A **USABLE CLONE** is a copy of the live data from the evidence media to a clean media. Specialized hardware and software tools are utilized to ensure the live data is unaltered and accessible to the user*

Imaging is always the first step taken before any investigation of the hard drive. From the image, information is reconstructed and analyzed and information attained made discoverable. However it can be difficult to know if this attained information is going to be needed for litigation. The best way to preserve information, and protect yourself and your client, is to have images made as soon as litigation becomes a possibility. Having images made early will not only serve the purpose of preservation but it will give you a head start on the digital forensics process. The information is already acquired and processing and analysis, if necessary, can begin immediately resulting in a quicker turnaround time.

From a digital forensics perspective, here are the steps you need to take:

- 1) Make a list of all electronic equipment that may be called into question during the litigation process. This could include: computers, servers, PDA's, Blackberry's, digital cameras, thumb drives, iPods... any device that can store electronic information – NOTE: If you aren't sure, put it on the list and ASK!

THE LORENZI GROUP

- 2) Have your Digital Forensics Experts (The Lorenzi Group) create and store digital images of all the listed devices.
- 3) If you are planning to continue using the devices during the litigation process, request your Digital Forensics Experts (The Lorenzi Group) create an “imaged clone” of the devices.
- 4) Bag and label the original media (hard drive, memory stick, thumb drive, etc.) and the forensic images.
- 5) Return the “imaged clones” into the appropriate devices for daily use.
- 6) Store the original media and imaged media in a secure, fireproof environment for later use.

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.