**What Is A Forensic Image?**

‘Imaging a hard drive’ is a phrase that is commonly used for preserving the contents of a custodian hard drive or server. It can also be used to describe when a custodian hard drive is cloned. It is worth taking some time to understand the differences and the advantages and disadvantages of each process.

**Forensic Imaging**  
A forensic image or evidence file container (such as EnCase, DD, Expert Witness, and SMART) is often created using software that is running on a computer forensic examiner’s laptop or lab computer. The examiner will connect the drive to a write blocker and use software to create a forensic image of the entire contents of the source drive on a separate target hard drive. The process may also capture multiple forensic images to a single hard drive.

**Hard Drive Cloning**  
Cloning a hard drive during collection uses a target drive to make an exact duplicate (bit stream copy) of the original hard drive. This process is normally completed using hardware referred to as hard drive cloning equipment.

A primary difference between imaging and cloning is that the files in a forensic image can’t be accessed by common litigation support applications or electronic discovery software (such as LAW PreDiscovery, Discovery Cracker, and IPRO) or litigation support databases (such as Concordance, Summation, and Ringtail).

Forensic images are designed to be accessed by computer forensic software (such as Encase, FTK, Winhex, and ProDiscover). If you need to access the original custodian information in a forensic image without using computer forensic software, then you will need to have it restored to a hard drive in the original native format. You could also look into purchasing the Mount Image Pro software (<http://www.mountimage.com/purchase-forensic-software.php>) that will allow you to view the contents of a forensic image without converting or restoring it to the native format.