What is a Forensic Image?

Description

‘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 (https://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.

Cost and Redundancy Considerations
If you want to compare the cost of different computer examiners, keep in mind that the lowest hourly rate doesn’t mean the lowest total price. An examiner using hardware-based cloning equipment can usually complete the process faster than using software to create a forensic image.

If you rely on a single forensic image or hard drive clone and find out later that there was a problem, you probably won’t have a second chance to preserve and collect the information. It’s well worth the additional cost to create a 2nd backup of the source hard drive. When comparing examiner rates, you will need to compare the hourly and per drive costs to determine the total price. Also, consider what you will be

charged to restore a forensic image to a new drive, because this may have to be completed before the custodian files can be processed.

PINPOINT LABS VIDEO PRESENTATION

This information is provided by Jon Rowe, a Certified Computer Examiner (CCE) and the President of Pinpoint Labs. Please watch the video below to learn more about affordable and defensible tools for E-Discovery collections.

[tube]https://www.youtube.com/watch?v=Y-NtNWw2-Yg[/tube]

Date
01/19/2025
Date Created
01/29/2009