C31 Overcoming the Hurdles of Imaging, Storing, and Archiving Digital Evidence

Kristy Tredway, 1220 6th Street, Huntington, WV 25701*

The goals of this presentation are to determine the best ways to increase efficiency and decrease storage space during digital imaging.

This presentation will impact the forensic science community by helping digital forensic examiners reduce imaging time and decrease the amount of storage each image takes.

Digital forensics is an integral part of the forensics field. Digital evidence is information stored or transmitted in binary form that may be introduced and relied on in court. Digital evidence can be found on a computer hard drive, a mobile phone, a Personal Digital Assistant (PDA), a Compact disc (CD), and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud.[1]

When digital forensic examiners obtain a digital device to be analyzed, they first image and save an exact, bit-for-bit copy of the original storage media on another storage device, such as a hard drive. This is known as the forensic image. Forensic imaging involves two types of images: a logical image and a physical image. A logical image is a copy of all the files on a storage device, except deleted files, file fragments, and deleted space from a partition. This allows an investigator to quickly scan the contents of a hard drive. An E01 file is an example. A physical image is a bit-for-bit copy of the storage device, including the deleted files and file fragments. A RAW file is an example.

Once imaging is completed, a digital fingerprint of the media is acquired, known as a hash. The hash generation process involves an algorithm calculation of all the zeros and ones that exist across the sectors examined. Altering a single zero to a one or a one to a zero will cause the resulting hash value to be different. If the hash values match, then the image is an exact copy and is used as the working copy to analyze the data.[2]

Because of the increase of digital evidence being submitted for analysis and the length of time evidence is required to be kept, untested digital evidence and already processed evidence are accumulating. The purpose of this research was to look at ways to image, store, and archive digital data to take up less storage space and provide greater efficiency. This will help decrease the time spent to test pieces of evidence, thereby decreasing backlogs, and decreasing costs.

The following questions guided the research: (1) What is the best way to create a forensic image (E01 file or RAW file)?; (2) What is the best way to store that E01/RAW file?; (3) What is the most efficient way to process that image?; and, (4) In the most efficient, cost-effective way, how should that data be archived?

Eight different types of storage devices were imaged using two different types of files, E01 and RAW. This was performed with two forensic imager tools, AccessData® FTK® and SUMURI® PALADIN®. A comparison was performed using different paths, with and without a write blocker, and using different levels of data compression. This determined the fastest way to image digital evidence and the best way to minimize the space taken by saved evidence. Since PALADIN® has a software write blocker, the images produced using the hardware write blocker in FTK® were compared to the images without an additional hardware write blocker in PALADIN® (only using the software as write protection).

The results demonstrate that RAW images sent directly to the server using PALADIN® without a hardware write blocker was the fastest and most efficient way to image, but E01 in FTK® took up 5%–18% less storage space. Imaging E01 files in PALADIN® resulted in failure approximately 50% of the time, especially when using an additional hardware write blocker. In FTK®, adding compression did not change the amount of time or storage space taken. In PALADIN®, adding compression increased the time while decreasing space. Future research would include imaging larger storage devices, testing different software and write blockers, and adding a virtual machine.

Reference(s):

1. *Digital Evidence and Forensics.* (n.d.). https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.

2. *Forensics: What is imaging?* (2009, June 27). https://whereismydata.wordpress.com/2009/06/27/forensics-what-is-imaging/.

Digital, Forensic, Imaging

*Presenting Author