B12 Strategies for the Forensic Collection of Digital Evidence From Shared Storage and Virtualized Environments

Danielle M. Desfosses, MFS, 3152 Covewood Court, Unit K, Falls Church, VA 22042; and Brian D. Nunamaker, BS*, and Paul Cibas, BS, Drug Enforcement Administration, 10555 Furnace Road, Lorton, VA 22079*

After attending this presentation, attendees will gain a basic understanding of proposed strategies to obtain digital evidence from shared storage technologies such as, iSCSI, Fiber Channel (FC), and Network Attached Storage (NAS), which are commonly used with virtualization.

This presentation will impact the forensic science community by empowering digital forensic examiners with strategies involved in acquiring, investigating, and preserving digital evidence from shared storage technologies and virtualized environments that have become increasingly prevalent.

With the increase of virtualization being adopted by the IT industry, coupled with the continued decrease in data storage costs per gigabyte, shared storage technologies have become more prevalent. The advantages of shared storage technologies are vast. They allow for extremely large amounts of data to be disseminated to both individual computers and servers. These storage areas can then be presented to the individual computers and servers as local disks. With only a few clicks of the mouse and with no additional physical hardware changes, these disks can be re-sized, moved, added, and deleted with ease. Furthermore, the centralization of these storage technologies allows for easier management and secure segregation of data within a business enterprise. As a result, significant performance gains can be achieved by spreading data across multiple drives.

The traditional computer forensic examiner who is comfortable with locating and preserving evidence from stand-alone computers that have locally attached hard drives may have difficulty in finding and preserving digital evidence located on shared storage technologies. In the case of encountering shared storage, a forensic examiner must first be able to identify the type of technology being utilized. For example, the presence of a host bus adapter card physically attached to the computer hardware will indicate to the forensic examiner that FC technology is being employed. Additionally, a forensic examiner must be able to develop a concise and practical strategy to obtain digital evidence from storage arrays, which may consist of terabytes or even petabytes of data; and may possibly need to be obtained without the assistance or knowledge of the local system administrator. As a result, the strategy developed must encompass the ability to target specific data, as it may be impractical and too time-consuming to duplicate the entire shared storage array.

Because shared storage technologies are often affiliated with virtualized environments, a forensic examiner must be able to identify and locate the virtual computer(s). The forensic examiner must have an understanding of the types of files generated, managed, and saved by each virtualized environment. For example, VMWare uses "VHD" virtual disk files to store virtual machine(s). A forensic examiner also must be able to identify specific information they are seeking, even if it is encapsulated within a virtual disk.

The purpose of this presentation is to address all of the above listed needs. An overview of the most commonly used virtualization software packages, including VMWare's VSphere, Microsoft's Hyper-V, and Linux solutions such as XEN, and the system requirements for implementing shared storage technologies, will be provided. This overview will cover specific hardware and software configurations affiliated with each shared storage technology, how to identify them, and proposed strategies for gaining access to the shared storage areas. Based on the type of virtualization environment, proposed strategies will be identified and presented for the recovery of digital evidence from the associated virtual machines.

At the conclusion of the presentation, attendees will be more familiar with virtualization, shared storage, and strategies for recovering digital evidence from these environments.

Shared Storage, Virtualization, Digital Evidence

 ** Presenting Author*