B21 Virtualizing the Computer Forensic Examination Platform

Brian D. Nunamaker, BS, Drug Enforcement Administration, 10555 Furnace Road, Lorton, VA 22405*

After attending this presentation, attendees will learn how to implement a virtualized examination platform to conduct computer forensic examinations. Attendees will also have a greater knowledge of the advantages and disadvantages of this configuration.

This presentation will impact the forensic science community by showing how a computer forensics laboratory implemented a virtualized

examination platform integrated with a Storage Area Network (SAN) to improve performance.

Most computer forensic laboratories suffer from the same problems, too many exhibits to process, with too little time to complete the task. Virtualization with SAN storage may help reduce preparation time between cases. Overall examination time can also be reduced. Virtualization allows for the standardization of examination platforms, a template for updates and deployments, and multiple isolated examination platforms to exist on a single physical server. By using virtualization and a fiber channel SAN, multiple examination platforms can take advantage of shared hardware between the servers and the SAN. This allows for a higher density of examination platforms on the same physical hardware. The virtualized examination platforms can take advantage of the increased disk performance of the SAN while still sharing a single fiber connection to reduce networking costs and complexity.

Examination platforms, such as server operating systems (OS) (Windows NT 2000 2003 2008, SQL Server, MySQL, Linux, BSD, SCO, etc.), can be rapidly rolled out from templates. These templates contain operating systems stored on wiped virtual drives. The fully configured examination platforms are ready for case processing in a matter of minutes, as opposed to the hours needed to wipe a hard drive and install a new OS. Redundant Array of Independent Disks (RAID) volumes located on the SAN containing evidence can be moved from one virtual examination platform to another with a few clicks of a mouse. The centralization of the evidence allows for less handling of physical hard drives and equipment. This should allow for an increase in the longevity of equipment.

An additional advantage to virtualization is the isolation of the examination platforms on a single physical server. This isolation allows examiners to work multiple cases at the same time without the concern for cross contamination of the evidence. The isolation of the examination platforms on the network is achieved through strong security polices and the use of a stand-alone network. This allows examiners to log into their local desktop computer and remote into their examination platform. The examiner can switch between multiple remote examination platforms containing different case materials. Multiple examination platforms can reside on a single server and share the hardware resources.

Due to the network infrastructure of this configuration, the network of computers can be exploited for other purposes. The laboratory can now take advantage of distributed password breaking applications. These applications will distribute attacks against a single password protected file across multiple servers (nodes) and act as a collective password breaker. Resources can be controlled to balance the performance of the examination platforms running processes overnight versus the resources for password breaking.

Virtualization, SAN, Examination Platform

 ** Presenting Author*