B27 The Virtual Digital Forensics Laboratory

Mark R. McCoy, EdD, University of Central Oklahoma, Forensic Science Institute, 100 North University, Edmond, OK 73034*

After attending this presentation, attendees will understand the concept of the Virtual Digital Forensics Laboratory (VDFL), the technology solutions it employs, and the flexibility it provides for digital forensic investigators.

This presentation will impact the forensic science community by proposing an innovative concept to expand the capabilities of digital forensic examiners to examine digital evidence and distribute the results of those examinations.

Law enforcement investigators have attempted to respond to the growing and complex need to investigate all matter of computer related incidents by using stand-alone forensic workstations and limited storage solutions. Digital forensic examiners often find that their cases are held up by cumbersome and inflexible technology that limits their effectiveness. The need to store and examine large quantities of data and the need to provide easy access to examination results to investigators in remote locations has changed the face of the digital forensics laboratory.

A Virtual Computer Forensics Lab (VCFL) is a fairly new concept that applies existing enterprise virtualization technology to current forensic investigative methods. Virtualization technology was introduced in the 1960s to allow the full use of mainframe hardware, but more recently virtualized network, storage, and workstation technologies have matured to the point where they can be used to effectively overcome computer forensics lab constraints. Today virtualization is helping many Information Technology (IT) organizations solve problems with scalability, security, and management. Virtualization can help computer forensic labs do the same.

A computer forensics lab must be able to keep pace with the technology it analyzes, and it must allow investigators secure remote access to forensic tools. Virtualized hosts and virtualized storage, along with strong network encryption, allow organizations the flexibility for multiple investigators to collaborate using the same evidence, while using as many virtual forensic workstations as needed, with a storage system that can scale to hundreds of terabytes.

Virtualization technology is the abstract layer that resides between what is presented and the physical hardware. There are three core virtualized technologies needed to create a virtual lab environment: virtual private networks, virtual machines, and virtualized storage. A fourth (non-virtualized) component, two-factor identity management technologies, is also needed to create a secure and confidential lab environment. This technology can be applied to existing computer forensic labs to create a complete virtualized layer that still meets rigid ASCLD (American Society of Crime Laboratory Directors) requirements.

Digital Forensics, Virtual Digital Forensics, Virtual Lab

 ** Presenting Author*