Apr 24th, 2:10 PM

The Virtual Digital Forensics Lab - Expanding Law Enforcement Capabilities

Mark McCoy
Forensic Science Institute, University of Central Oklahoma, USA, mmccoy@ucok.edu

Sean A. Ensz
University of Oklahoma, Oklahoma, USA, ensz@ou.edu

Scholarly Commons Citation

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL

Briefing Paper

The Virtual Digital Forensics Lab: Expanding Law Enforcement Capabilities

Sean A. Ensz
University of Oklahoma
200 Felgar Street, Norman, Oklahoma 73019
405.325.3954 Office
405.325.1633 Fax
ensz@ou.edu

Mark R. McCoy
University of Central Oklahoma
Forensic Science Institute
100 N. University, Edmond, Oklahoma 73034
405.974.5617 Office
405.974.3871 Fax
mmccoy@ucok.edu

ABSTRACT

Law enforcement is attempting to respond to the growing and complex need to examine all manner of digital evidence using stand-alone forensic workstations and limited storage solutions. Digital forensic investigators often find their cases stalled by cumbersome and inflexible technology limiting their effectiveness. The Virtual Digital Forensics Lab (VDFL) is a new concept that applies existing enterprise host, storage, and network virtualization technologies to current forensic investigative methods. This paper details the concept of the VDFL, the technology solutions it employs, and the flexibility it provides for digital forensic investigators.

Keywords: Virtual Digital Forensics, digital forensic investigations, law enforcement, virtual lab, Digital Forensics

1. INTRODUCTION

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 limiting storage solutions. Forensic investigators 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 to face of the digital forensics laboratory. This paper details the concept of the Virtual Digital Forensics Laboratory (VDFL), the technology solutions it employs, and the flexibility it provides for digital forensic investigators.

2. VIRTUALIZATION

A Virtual Computer Forensics Lab (VCFL) is a 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. They are virtual private networks, virtual machines, and virtualized storage. A fourth (non-virtualized) component, using two-factor identity management technologies, is also needed to create a secure and confidential lab environment. This technology can be applied to existing computer forensics labs to create a complete virtualized layer that still meets rigid ASCLD (American Society of Crime Laboratory Directors) requirements (ASCLD, 2008).

3. VIRTUAL PRIVATE NETWORK

VPN connections are accomplished through the use of network firewalls that create an encrypted tunnel between the user and the network being accessed. VPN technology uses strong encryption mechanisms that make it almost impossible to snoop the network traffic. Recently, a new type of VPN called an SSL VPN became available that allows traffic to essentially be tunneled through a web proxy.

VPN technology can be used to provide secure remote access by computer forensic investigators to work cases from a remote office. (See Figure 1).The firewalls can be configured in such a way that prevents remote workstations from accessing any hosts on the internet other than the virtual workstations. Once the original evidence has been duplicated and placed on virtualized storage, it can be accessed from a fully functioning virtual workstation loaded with any forensic software needed by the investigator. The remote investigator should see no difference between working a case within the lab or remotely.
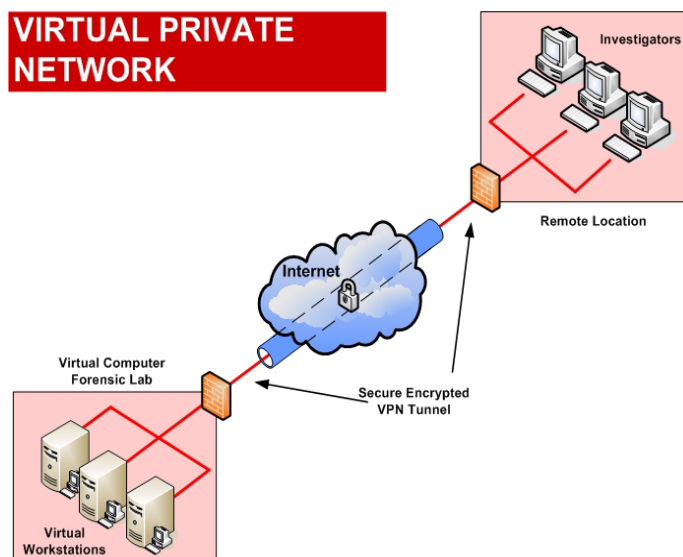

Figure 1.

4. VIRTUALIZED STORAGE

Enterprise level storage virtualization that facilitates access from multiple workstations and servers requires the use of Storage Area Network (SAN) architecture. SAN is a storage system that uses

remote storage arrays in such a way that a disk appears to be locally attached. The physical disks use Redundant Array of Independent Disks (RAID) technology to protect against disk failure and are scalable to allow additional storage to be added when needed. Many large regional and state computer forensic labs currently use SAN technology, but they fail to fully take advantage of the benefits virtualized storage provides. Virtualized storage is considered the process of abstracting logical storage from the physical disks. Traditional drive mapping requires groups of physical disks (called a LUN) to be assigned to a host. The virtualization system, however, presents the logical storage space for data storage and the controller handles the process of mapping it to the physical disks. This technology helps by providing efficient utilization, shared storage without restrictions and increased performance.

Efficient utilization is accomplished by managing disks as a single pool and presenting disk resources to any server. Utilizing all disk resources all the time provides for maximum efficiency. Shared storage without restrictions is provided by removing the limitations of physical drives by aggregating them into logical, virtual volumes. Write virtual volumes to the entire disk pool or any subset of the disk pool; provision without restrictions. Increased performance is gained by scaling performance linearly across all the available drives; making each disk drive's performance characteristics accessible to each server. Any volume can simultaneously utilize all of the disk drives in the shared pool to access data (Compellent, 2008).

Virtualization technology can also include presenting a set volume size that is larger than the sectors allocated on the physical disk drives (called thin provisioning). With traditional storage, disk space must be pre-allocated and is often not fully utilized by the host. This can create a large amount of storage space that goes unused. Consider a situation in which five forensic investigators each request 500 gigabytes of SAN space to work their case, but they only end up using 300 gigabytes of actual storage space. In this scenario, 1 terabyte of space, using a traditional SAN, would go unused. With thin provisioning the 1 terabyte would still be available to work other cases.

5. VIRTUAL WORKSTATIONS

Virtualization is an abstraction layer that decouples the physical hardware from the operating system. Using virtual machine software, it is possible create a virtualized forensic workstation environment that completely emulates all aspects of a real physical workstation. This technology allows multiple virtual workstations to run on a single server that can act independently of each of other with granular permissions. Access to storage and network resources can also be tightly controlled and monitored to only allow virtual machines to access the resources assigned to the investigator. Since all hardware at the virtual layer is standard, it is possible to create uniform forensic workstation builds that can be duplicated for each new case. Forensic investigators will be able to use a pristine build that has not been contaminated by previous cases.

Virtualization provides for partitioning, isolation, and encapsulation. Using partitioning multiple applications and operating systems can be supported within a single physical system. Computing resources are treated as a uniform pool to be allocated to virtual machines in a controlled manner. Virtual machines are completely isolated from the host machine and other virtual machines. If a virtual machine crashes, all others are unaffected. Data does not leak across virtual machines and applications can only communicate over configured network connections. With encapsulation, complete virtual machine environment is saved as a single file; easy to back up, move and copy. Standardized virtualized hardware is presented to the application to guarantee compatibility (VMWare, 2008).

It is possible to start and assign multiple virtual machines to investigators that allow them to work multiple cases at one time. Investigators often contend with downtime because a workstation is tied up making images, or conducting text searches or data carving. With a robust virtual machine infrastructure it is possible to assign multiple virtual workstations, with dual processor support and ample memory, to an investigator with varying operating systems if needed.

6. PROPOSED DESIGN

The transition from the traditional forensic lab to a virtualized forensic lab is as simple as adding a virtualization technology layer over existing infrastructure and processes. The lab design will meet, and in some cases exceed, stringent standards for data security, evidence handling, and investigation techniques. Strong network encryption and two-factor authentication schemes will be used to ensure confidentiality and integrity of all lab equipment. Evidence handling and investigative processes will meet standards set for by the ASCLD Laboratory Accreditation Board Manual (ASCLD, 2008).

6.1 Network

The network design will use hardware based site-to-site VPN tunnels between remote investigator PC and the physical computer forensics lab. The use of hardware VPN appliances ensures that only equipment properly configured by lab personnel will be able to gain entry into the secure network. The VPN tunnels will use strong 128-bit AES (Advanced Encryption Standard currently adopted by NIST and FIPS) encryption algorithms to prevent data leakage and network sniffing over internet links. Remote VPN appliances will be configured in such a way that investigator workstations will be restricted to only access the hosts on the VPN. Internet access will be completely restricted from the workstations. The design, using VPN technology, will mimic a standalone physical network in which all workstations are connected to the same physical switch. See Figure 2 for a logical diagram of the virtual digital forensics lab design.

6.2 Storage

The storage will incorporate an enterprise SAN solution that will provide redundancy, fault tolerance, and scalability. The solution will also use cutting edge controllers that will provide virtualization technology, providing flexibility and ease of use. New virtual volumes will be created for each new investigation that can be resized and duplicated as needed. Virtual storage technology allows snapshots to be taken of existing virtual volumes if multiple investigators want to work with the same evidence. Virtualization technology is also on the horizon that will allow a virtual volume to be mirrored to a tape drive that will allow duplicate forensic images to be simultaneously written to a tape backup while a working forensic copy is written to the virtual volume. This is done entirely in the background without any additional steps needed by the forensic technician acquiring the original evidence. Destruction write technology will also be used to wipe physical sectors on the SAN hard drives before new data is written.

6.3 Workstations

The virtual forensic workstations will be running an enterprise version of VMware on server hardware to provide flexibility and performance. The remote investigator will use a low cost PC to access, through the VPN tunnel, the powerful virtual forensic workstation running locally in VMware. The Microsoft remote desktop client will be used to gain access to the virtual forensic workstation. Once the remote desktop connection is made the investigator will be required to enter his or her username followed by a PIN and six digit number presented on a key fob. The virtual forensic workstation will only have access to the virtual volume containing a working copy of the evidence that was assigned to the investigator.

Case workflow will occur in the following stages:
- Initial intake and tagging of original evidence
- Virtual Volume is created on the SAN to meet case storage requirements
- Original evidence is imaged to a virtual volume on the SAN
- New virtual workstation is started and assigned to an investigator
- Virtual volume on SAN is mapped to the virtual workstation
- Virtual workstation is granted network access to investigator remote PC

- Investigator initiates a remote desktop connection and authenticates
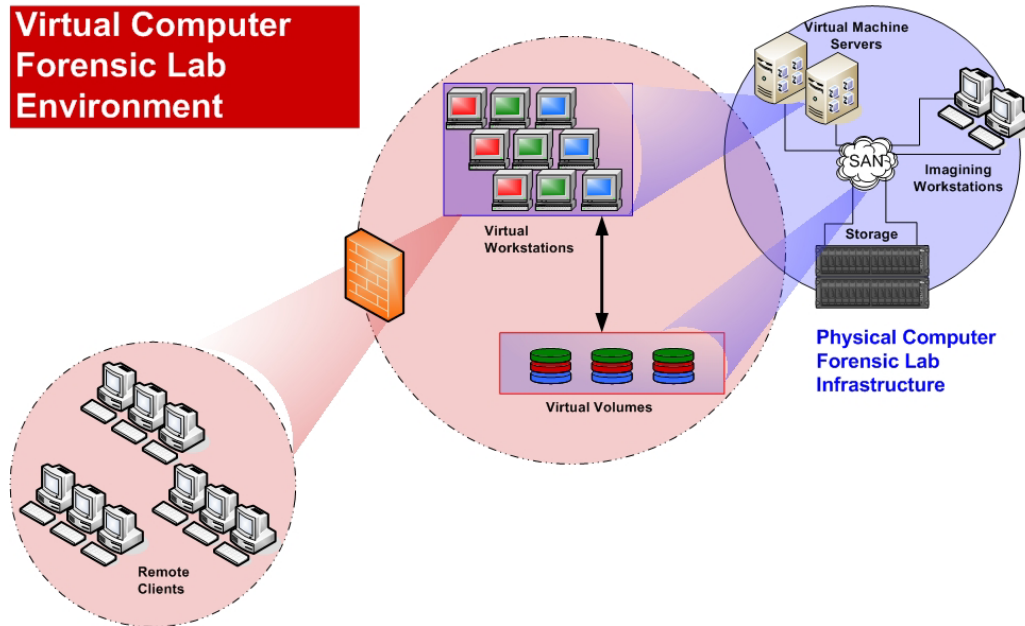- Investigator begins forensic analysis

Figure 2.

REFERENCES

American Society of Crime Laboratory Directors (2008), www.ascld.org, 2/28/2008.

Compellent (2008), http://www.compellent.com/products/software/virtualization.aspx, 2/28/2008.

VMWare (2008), http://www.vmware.com/virtualization/, 2/28/2008.

AUTHORS BIOGRAPHIES

Sean A. Ensz, CISSP, GSEC, EnCE, RHCE, is an Information Technology Security Analyst at the University of Oklahoma.

Mark R. McCoy is currently an Assistant Professor of Criminal Justice at the University of Central Oklahoma. In June 2008, he will join the faculty of the UCO Forensic Science Institute as the Digital Evidence and Cyber Security Program Administrator. He recently retired after over 20 years of service with the Oklahoma State Bureau of Investigation. He is a member of the International Association of Computer Investigative Specialists and is a Certified Forensic Computer Examiner. He was the first supervisor of the OSBI Computer Crime Unit and has conducted hundreds of forensic examinations involving digital evidence. He has a Masters Degree in Forensic Science and a Doctorate in Occupational and Adult Education.