Global Information Assurance Certification Paper

Exploring the Effectiveness of Approaches to Discovering and Acquiring Virtualized Servers on ESXi

GIAC GCFE Gold Certification

Author: Scott Perry, perry.sans@gmail.com
Advisor: David Hoelzer

Special thanks to Dave Luehring, Alan Harper, and Dale Forrester

Accepted: November 13th 2017

Abstract

As businesses continue to move to virtualized environments, investigators need updated techniques to acquire virtualized servers. These virtualized servers contain a plethora of relevant data and may hold proprietary software and databases that are relatively impossible to recreate. Before an acquisition, investigators sometimes rely on the host administrators to provide them with network topologies and server information. This paper will demonstrate tools and techniques to conduct server and network discovery in a virtualized environment and how to leverage the software used by administrators to acquire virtual machines hosted on vSphere and ESXi.

1. Introduction

It has been estimated by Gartner that "as many as 80% of x86 server workloads are virtualized" (Bittman, Dawson, & Warrilow, 2016). As businesses continue to move to virtualized environments, investigators need updated techniques to acquire virtualized servers. These virtualized servers contain a plethora of relevant data and may contain proprietary software and databases that are relatively impossible to recreate. Before an acquisition, investigators sometimes rely on the host administrators to provide them with network topologies and server information. This paper will also demonstrate some basic tools and techniques to conduct server and network discovery in a virtualized environment to ensure all relevant virtualized servers are discovered and acquired. Currently, investigators create forensic evidence files of logical partitions, a portion of selected data, or power down the server to acquire physical hard disk drives. These methods may miss data relevant to the investigation, or they may take a critical server down for an unreasonable amount of time. Instead, investigators may need to leverage the software used by administrators to manage those virtualized environments such as vSphere and specifically ESXi. These updated methods will build upon previously published research (Henry, 2010 and Barrett & Kipper, 2011) and will inform the forensic examiner community how to acquire relevant data while still minimizing the impact to the server's operations and exercising forensic "best practices." Beyond updating the methods for acquiring data from an ESXi server, this paper will also show the relative acquisition times achieved during

perry.sans@gmail.com

testing of different network bandwidths and source disk types to serve as a benchmark for investigators acquiring virtual machines (VMs) from ESXi servers.

1.1. Server Virtualization Background

Gone are the days of the large data centers of the 1950's full of mainframes. By the 1990s these mainframes were being replaced by banks of servers. Servers brought improvements over mainframes by being modular and smaller, but in the 2000's the trend turned to virtualization (Rathod & Townsend, 2014).

The growth in server virtualization is based on the following characteristics (VMware Inc., 2014) (Rathod & Townsend, 2014):

- Lower cost to maintain a virtualized server versus its physical counterpart. Stated plainly, there are fewer physical components to buy, manage, and maintain.
- Faster and more efficient provisioning of resources.
- Fewer disruptions to operations. Physical servers can be significantly harder to restore than a comparable virtual server.
- Simplified backups and restoration of data.
- Simplified IT management

Besides virtualizing local servers, the next step in the evolution of virtualization is cloud computing and applying virtualization to a larger scale and providing it as a paid service. While not all cloud computing is virtualization, it is virtualization that has allowed cloud computing to flourish. As stated by Mike Adams, Director of Product Marketing at VMware, "Virtualization is a foundational element of cloud

perry.sans@gmail.com

computing and helps deliver on the value of cloud computing" (Angeles, 2014). The lead provider, Amazon Web Services (AWS) is expected to bring in over "$14 billion in revenue this year" (Darrow, 2017). Additionally, Cisco predicts that the global data center traffic will reach 7.7 zettabytes of data in 2017 and 9.8 zettabytes of data in 2018, with increased growth after that (Cisco, 2016). This growing trend of cloud computing provides a benchmark of how popular virtualization has become.

Global data centers and the local servers have something in common: they both host virtualized servers. With an almost 80% market share of virtualized servers, VMware is one of the most popular vendors supplying their vSphere suite of virtualization, to include ESXi (Bittman, Dawson, & Warrilow, 2016). At the heart of any virtualized server is the hypervisor, which is software that allocates resources to the VMs. Installed on the host computer is the hypervisor, in this case, a server (Perneel, Fayyad-Kazan, Peng, Guan, & Timmerman, 2015). There are two main types of hypervisors, commonly referred to as Type 1 or Type 2 hypervisors. Type 1 hypervisors run directly on the physical server and directly control the hardware and manage the guest VMs and hosted operating systems. These types of hypervisors will partition the server and allocate resources for the VMs (Rathod & Townsend, 2014). VMware's ESXi is a Type 1 hypervisor and will be focused on in this research. The other type of hypervisor, Type 2, is called "hosted hypervisors" and are installed on top of the existing operating system (OS) such as Windows or Linux. A Type 2 hypervisor will then manage the connections and resources

perry.sans@gmail.com

between the host OS and the VMs (Rathod & Townsend, 2014). An example of a Type 2 hypervisor is VMware's Workstation program.

1.2. vSphere and ESXi

Announced in April 2009, vSphere 4 was designed to be the next evolution in virtualization by providing the "first operating system for building the internal cloud" (VMware, 2009). Put simply, vSphere is the overarching suite of software components that includes many tools and components. The focus of this paper is ESXi, vSphere Client (or referred to as "vSphere Desktop Client" from this point on to avoid confusion with the Web Client) and vSphere Web Client ("VMware vSphere," 2017).

ESXi can be considered the most significant part of the suite because it is the Type 1 hypervisor which directly interacts with the server hardware and hosts the guest OS's (Giri, 2012). For acquisition purposes, ESXi can be managed through components supplied with vSphere such as vSphere Web Client, ESXi Command-Line Interface (CLI) or vSphere Desktop Client, or through other VMware products like Workstation.

In the conceptual graphic (Figure 1) below it is easy to see that VMs can be stored in many places on a network to include SANs and other storage arrays. The focus of this paper is on acquiring the VMs hosted on the ESXi on the individual servers.

perry.sans@gmail.com

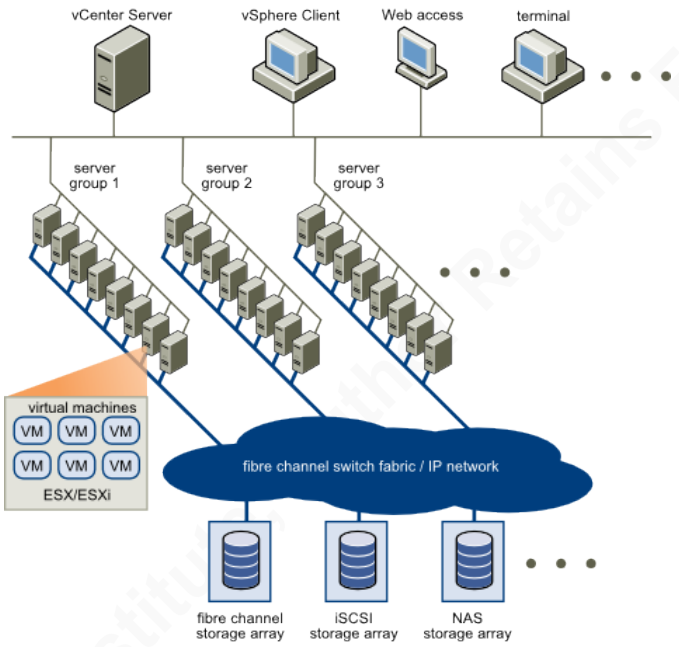

Figure 1: Conceptual VMware Environment (Source: VMware 2017)

The data which supports criminal and administrative investigations resides on the VMs hosted by ESXi, which is the reason for the focus on accessing ESXi and downloading the VMs. The VMs are saved to a datastore on ESXi, which is a storage container explicitly designed for ESXi and exists on the Virtual Machine File System (VMFS) partitioned by ESXi and vSphere. A datastore can be on a single hard drive, or it can span multiple storage systems like an iSCSI and NAS storage array depicted above (VMware, 2006).

2. Network Mapping and Discovery

Before beginning the task of acquiring specific data from an exact VM or multiple servers to determine what to take-regardless of the goal, it is recommended to conduct network mapping and discovery. The ideal approach is to have an administrator assist the investigator, as he or she knows the network and servers

better than anyone. Hopefully, the administrator can provide the analyst with an updated and current network diagram which can then be verified through network mapping tools and a physical inventory of the equipment. Besides a network diagram, an investigator can access vSphere directly through the vSphere Web Client or the Desktop Client to view the topology listed by vSphere in the Virtual Machines or Configuration tab as shown in Figure 2.

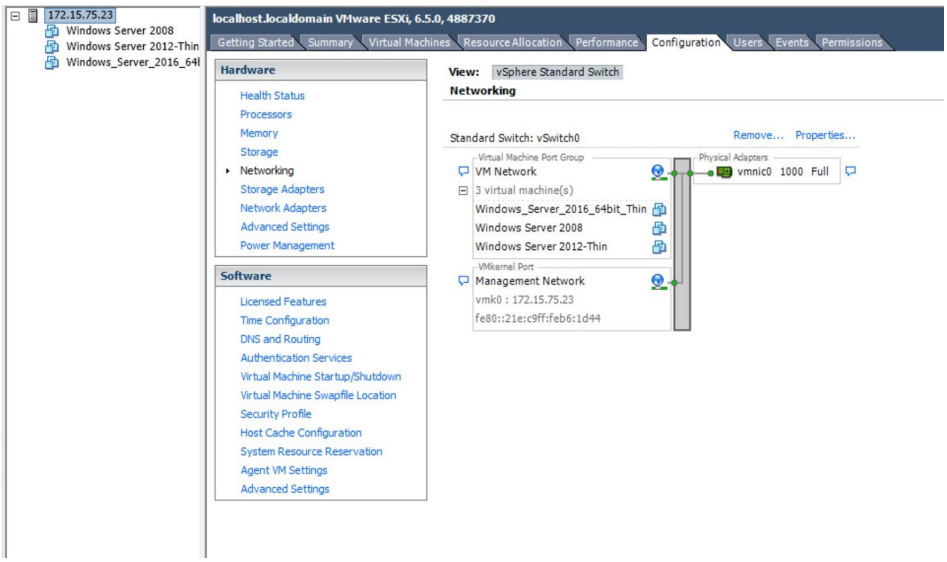

Figure 2: vSphere Desktop Client Networking Screen

Regardless of how permissive the acquisition environment and how much data provided, the investigator must always validate the information and data provided.

2.1. Network Mapping Tools and Techniques

The goal of network mapping in support of acquisitions is to determine and validate the topology of the network and to identify hosts, servers, and VMs that are in the scope of the investigation, whether that is a search for evidence in a criminal investigation or a response to an incident. The network mapping is not a

perry.sans@gmail.com

penetration test. While an investigator needs the information, he or she cannot use overly invasive techniques, try to break systems and services, or evade security and monitoring. The investigator needs to identify the management network for the ESXi and the production network that is connected to the VMs being hosted on the ESXi. Typically, ESXi will have a separate network interface card (NIC) for the management network.

There are a lot of scanning tools available, but GUI-based tools such as LanSpy, GFI LanGuard, and Zenmap are preferred to be used on-scene because they are relatively easy to use and generate a readily available and easy to read report or log file to document results. Figure 3 below shows an example of a LanSpy scan of one of the ESXi servers used for testing.

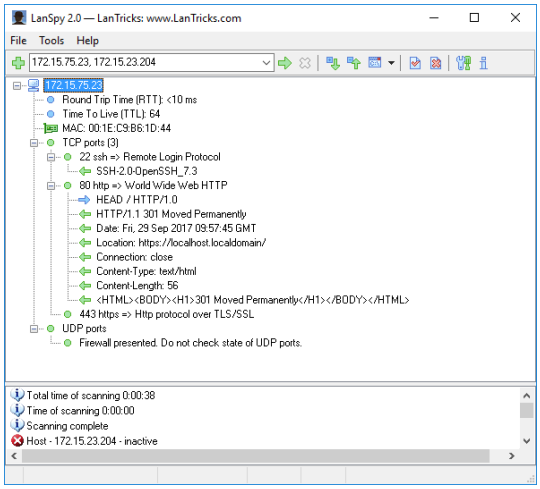

Figure 3: LanSpy Scan Result

Because of the default installation and a lack of running services on the ESXi server used for testing, there is not a lot to see from the LanSpy results, only that there is a computer running at that IP address with interesting protocols used, such

as SSH. A second "intense" scan with Zenmap, the Graphical User Interface (GUI) version of nmap, was conducted on the same network. Zenmap was able to identify the OS and the VMware authentication daemon running on port 902, as seen in Figure 4.

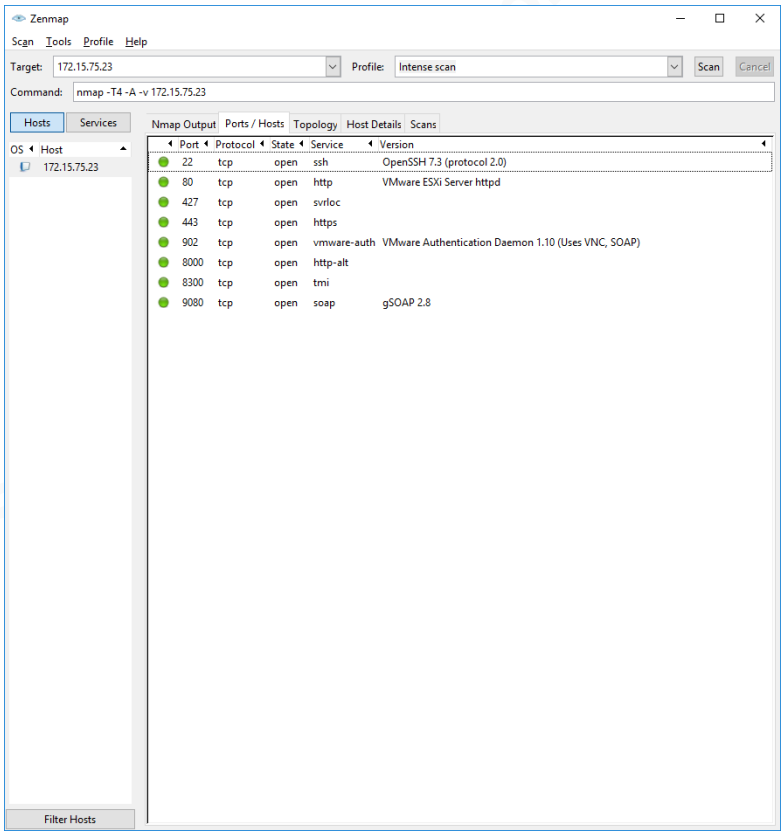

Figure 4: Zenmap Scan Results

When analyzing traffic and attempting to locate ESXi servers and managing hosts, an investigator should look for TCP or UDP traffic over port 902 and the VMware authorization daemon, vmware-authd. This daemon serves as a regular heartbeat via UDP to the vCenter server system (VMware 2017), as displayed in Figure 5 below.

perry.sans@gmail.com

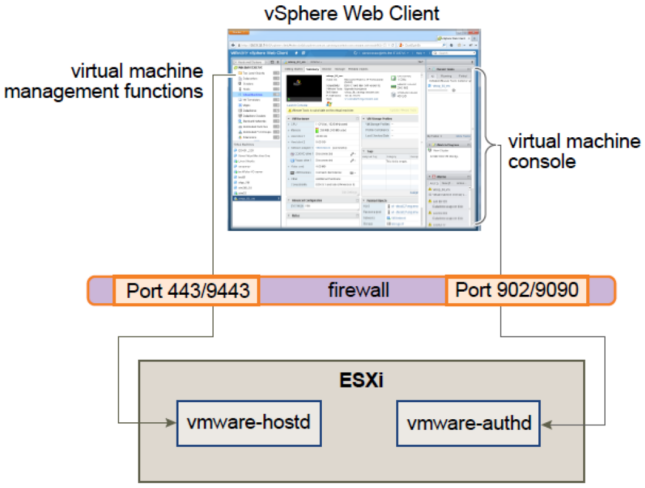

Figure 5: Port Use for vSphere Web Client Communications with an ESXi Host Managed by vCenter Server (Source: VMware 2014)

After using network scans and identifying potential ESXi servers of interest for acquisition, the next step is a physical server inventory.

2.2. Physical Server Inventory

An often overlooked, but essential step, is the physical inventory of servers on-scene. If connecting remotely and acquiring a VM over the network, it is easy to forego the step of verifying the network scanning results. The preferred method is to ask a cooperating administrator to provide an updated and accurate network diagram and to show each server. While this is ideal, it is not always practical. To identify the servers and hosts, the investigator should take the MAC addresses received from the ARP requests in the network scan detailed previously and ensure the device listed matches the Organizational Unique Identifier (OUI) for the first three parts of the MAC address. The OUI will only be unique for the manufacturer, so the OUI will not be helpful if all the servers are from the same manufacturer. If

perry.sans@gmail.com

unknown, the MAC addresses can be looked up online at a site such as www.Wireshark.org/tools/oui-lookup.html.

While the intricacies of VLANs and enterprise level networking is extremely detailed and beyond the scope of this paper, VMware uses 00:05:69; 00:0C:29; 00:1C:14; and 00:50:56 as their OUI. VMs running on the network with a software-based NIC may display these OUIs; however, MAC addresses for VMs can be easily changed and VMs are not required to use the VMWare OUI. Any VMs running on the Type 1 hypervisor ESXi will use the MAC address for the NIC of the ESXi server if running on a physical network. Searching for OUIs and creating an inventory will help establish the network topography.

3. Acquiring ESXi

3.1. Acquiring ESXi, The Basics

Whether acquiring multiple VMs hosted on an ESXi, or just a select set of folders and databases, there are some basic steps and guidelines to follow. First and foremost, before beginning the process and even touching a computer, an investigator must establish what he or she will be seizing is within the scope of their authority. Acquisitions and imaging are always time-consuming, and it is easy for an investigator to rush to begin the process. The investigator must firmly establish jurisdiction to make the acquisitions, be that from legal process or consent of the owner.

perry.sans@gmail.com

If the investigator is in a "permissible" environment where the local administrator is cooperating with the investigation and willing to help, then be sure to leverage their knowledge and abilities. It is recommended that the investigator should ask the administrator for:

- Administrator level/root passwords;
- Network diagrams, or in the absence of an updated network diagram, a list of what servers' host what VMs, databases, IP addresses, network share names, etc.
- A list of scheduled tasks or "Cron jobs" which may execute during the acquisition. Ask the administrator if any scheduled tasks may either effect the acquisition or, if not allowed to execute, will be detrimental to operations.
- A list and location of backup drives and devices.
- Identification of disaster recovery backups, either on-site or off-site.
- A set of keys to the server rack if it is locked.
- A key to the server room(s).
- If there is Closed-Circuit TV (CCTV) or another on-premises recording system, ask the administrator to disable the CCTV so the investigation is not recorded. The CCTV can also be a valuable source of evidence and an investigator may consider collecting the recordings as well to view who has physically accessed the servers.

If the administrator is unavailable or unwilling to help, the investigator will need to follow the steps detailed in the Network Mapping and Discovery portion of this

perry.sans@gmail.com

paper as well as the steps detailed in the "Acquiring ESXi in a Non-Permissive Environment" section of this paper.

One of the goals of digital evidence collection is to not modify the evidence during the acquisition. However, the investigator must interact with ESXi to download VMs. Following forensic best practices for acquiring evidence, actions must be documented as well as how the investigator interacts with and modifies ESXi to complete acquisitions.

ESXi runs a minimized version of Linux called BusyBox, which is based on Unix and has some Linux/Unix-like commands, but does not have all the programs and binaries typically installed with Linux. While the user can manipulate and download VMs from the CLI in ESXi, it is a more complex procedure and requires knowledge of the unique BusyBox commands. Using SSH and GUI-based tools are detailed in this paper because they are easy to use, readily available, and in the case of programs like PuTTY, provide a logging feature to document all actions.

To prepare ESXi for acquisition, to the investigator must:

1. Access the ESXi at the server to document settings and to enable SSH (SSH is disabled by default on ESXi) if you are going to use a remote access program to interact with ESXi.
2. Use an SSH remote access program to catalog the VMs on the ESXi.
3. Use either the vSphere Desktop Client or the Web Client to fully access the ESXi to complete acquisitions.

These steps are further detailed in the sections below.

perry.sans@gmail.com

3.1.1. Accessing ESXi at the Server

To acquire any VMs being hosted on the ESXi, the investigator will need to access it to determine the IP address of the server as well as to enable SSH to allow PuTTY or other remote CLI tools. PuTTY was used for this paper because it is Windows based, easy to use, and provides a logging feature to provide documentation of commands and output.

The screenshot below (Figure 6) was taken from ESXi 6.5.0 installed as a virtual machine in VMware Workstation 12. The version of ESXi is listed at the top, which is important as the same version of vSphere Desktop Client as the ESXi must be used. If the ESXi is 6.0 or greater, the investigator can use the ESXi provided vSphere Web Client as well.

Further down the screen is the IP address the investigator will need to access the ESXi via PuTTY or a client program.

perry.sans@gmail.com

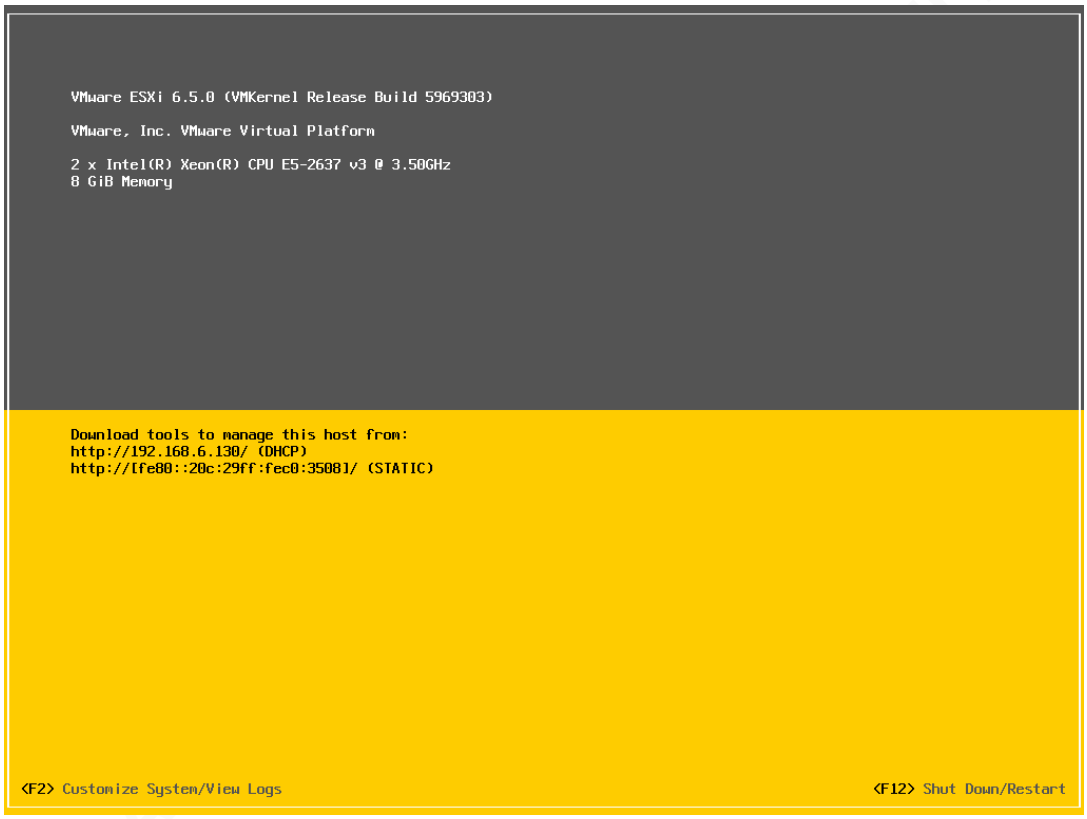

Figure 6: ESXi Home Screen

To configure the ESXi at the server, actions taken at each of the following steps must be documented:

1. Press the "F2" function key and enter the appropriate credentials to access the System Customization menu. If you do not have the credentials, then refer to the "Acquiring ESXi in a Non-Permissive Environment".
2. The System Customization menu has limited functionality and no access to the VM's hosted on the ESXi. Confirm the Management Network settings are accurate and set to what you need to access ESXi with a remote management tool.

perry.sans@gmail.com

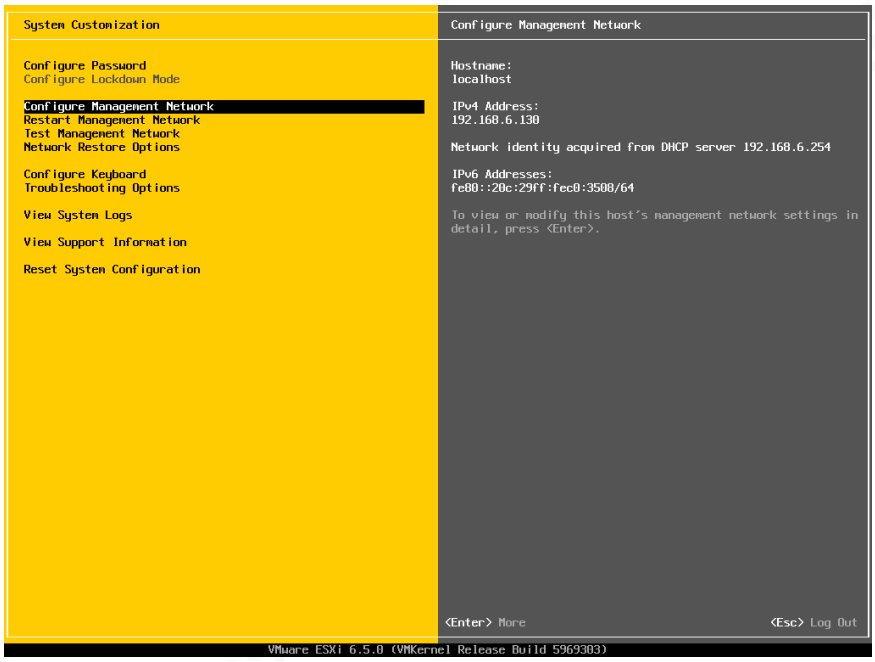

Figure 7: ESXi Configure Management Network Screen

3. Enable SSH in the Troubleshooting Mode Options menu as shown below in Figure 8.

Figure 8: ESXi Troubleshooting Mode Options

perry.sans@gmail.com

An investigator can further access ESXi through CLI at the server and garner more information such as running VMs, etc. but the suggested method is to access the ESXi through a remote access program such as PuTTY, which is easy to use and provides logging for documentation of the investigation and acquisitions.

3.1.2. Accessing ESXi with PuTTY, Preparing for Acquisition

PuTTY is the recommended remote access program for accessing, cataloging, and preparing ESXi for acquisition because it is easy to use and provides a logging system to document an investigator's interactions with the ESXi server.

1. Connect to the ESXi network. You must ensure you are connected to the same subnet as the target ESXi or vSphere server. A cooperating administrator should be able to provide a subnet and static IP for this step. Otherwise directly connect to the server on an open port. The IP address for the ESXi server should be displayed on the screen of the ESXi.
2. Open a remote access client, such as PuTTY.exe, on the computer accessing the ESXi, as seen in Figure 9.

perry.sans@gmail.com

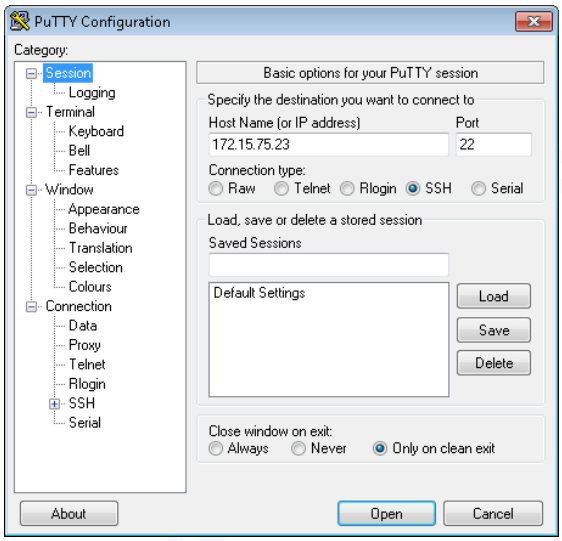

Figure 9: PuTTY Session Screen

3. Type the IP address of the ESXi host, port 22, SSH selected, Logging with "All session output" and provide a location for the logs (Figure 10).

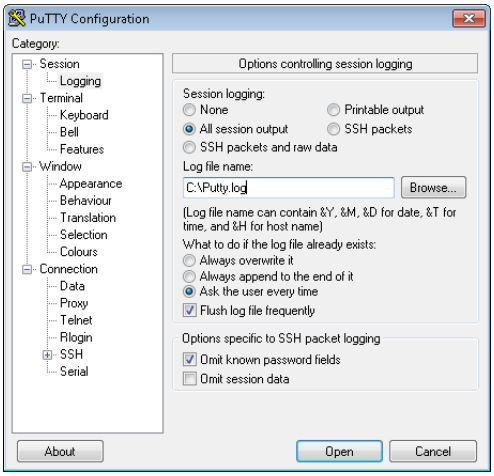

Figure 10: PuTTY Session Logging Options

4. To see a list of stored VMs on the ESXi host type "vm-support --listvms" in the command prompt inside PuTTY.
5. To see a list of running VMs on the ESXi host type "vmdumper –l" in the command prompt inside PuTTY.

perry.sans@gmail.com

To see an example of the output of inventorying the VMs via PuTTY, refer to Appendix A.

To view the VMs listed in the datastores on the ESXi host via PuTTY:

1. After connecting with PuTTY, type the below commands at the home screen:
   a) "cd /vmfs/volumes" to change directory to the directory containing information about the volumes currently on the VMFS.
   b) "ls -al" to list the files located in that directory.
2. Change to the desired datastore/VM folder and use the md5sum command to hash the files:
   a) "cd Datastore" to change to the directory storing the VMs. The datastore's location can vary widely as the administrator of the system can place them in a variety of locations.
   b) If there are running VMs that need to be downloaded, follow the steps detailed in the "Accessing ESXi by VMware Desktop Client" and pause or stop any running VMs.
   c) "md5sum *" to calculate MD5 values for the files located in the datastore directory. ESXi 6.5 and earlier still has md5sum installed.
3. After the hashing completes, type "exit" to close the PuTTY connection window.
4. Open the PuTTY log file that was produced to see a history of the commands that were entered, as well as the hash values that were produced. To see an example of the output of running md5sum of the VMs via PuTTY, refer to Appendix B.

perry.sans@gmail.com

3.1.3. Accessing ESXi by VMware Desktop Client

VMware has stopped their support of VMware Desktop Client in favor of its Web Client since the release of vSphere 5. The Desktop Client has not been officially supported since vSphere 5. While the Web Client is feature rich and is supposed to support all the functions available in Desktop Client, testing has shown the ability to download entire VMs is not fully supported and operational in ESXi 6.5 for Web Client, only in Desktop Client. For that reason, Desktop Client was chosen as the method for accessing and downloading entire VMs (Marshall, Orchard, & Atwell, 2015). Other techniques such as using PowerCLI, Secure Copy (SCP), or Secure File Transport Protocol (SFTP) are viable options as well but the Desktop Client was also chosen for ease of use and GUI. The Desktop Client enables a wider audience with less experience in acquisitions to be able to download VMs from ESXi.

Figure 11 below shows a screenshot of the vSphere Desktop Client that was used for testing. The interface is self-explanatory and relatively easy to navigate. If a complete VM is going to be downloaded, it needs to be stopped or suspended. If the VM is suspended a VMSS file is created that will contain the state of the suspended VM (Shavers, 2008). Also contained in the screenshot below is a view of the Datastore Browser, which contains the VMs to be downloaded (Henry, 2010).

perry.sans@gmail.com

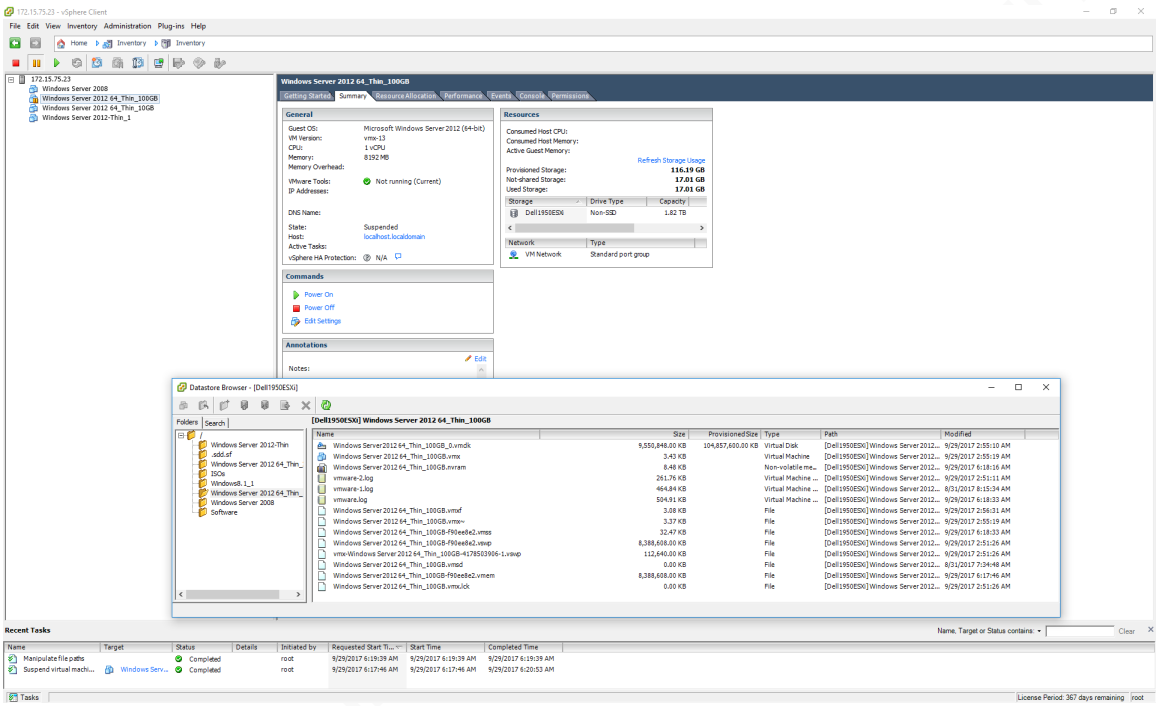

Figure 11: vSphere Desktop Client

After downloading the VM, it is recommended to follow best practices by hashing the files to compare the hash value to the md5sum hash value recorded previously when accessing the ESXi with PuTTY. After an acquisition, the investigator should return the server to the state it was before the investigation. This may include:

- Turning back on VMs.
- Turning off SSH or other services (if applicable).
- Turning back on services which were stopped for acquisition.
- Plugging back in network cables and returning the server to service.
- Disabling ESXi shell.

If the server or hosted VMs were compromised, then the investigator should consult with the administrator or the owner to determine if the server should be returned to its original state, pre-acquisition.

perry.sans@gmail.com

3.2. Acquiring Specific Folder or Files on ESXi

Acquiring an entire server is not always advisable-or even possible-for numerous reasons. Most acquisitions are limited by many factors, including: time; data storage for the acquisition; and legal and compliance constraints. One major hurdle is owners of the server being acquired do not want to lose revenue due to a disabled server hosting a website or loss of access to a database needed for business operations. Servers by their very nature host a lot of data, a majority of which will not be pertinent to the investigation. Triaging the data and limiting the acquisition will vastly speed up the acquisition process and the eventual processing and analysis.

Every business and operation is unique and their servers and IT infrastructure will also be unique and structured to support their operations. Depending on the operating requirements, the data may be encrypted. Some of the virtualized servers may have data spread out across multiple servers, operating systems, databases, and even workstations. If a product like vMotion, is installed and in use, VMware's clustered Virtual Machine File System (VMFS) would allow multiple ESXi to access the same files concurrently (VMware, Inc., 2007). An investigator cannot simply shutdown a physical server and image individual drives because of the possibility or distributed or encrypted data (Henry, 2010). Instead, the investigator may need to acquire specific files or folders of the VM and store them to locally attached or networked storage used by the investigator for the acquisition.

If an investigator is in a permissive environment with a cooperating administrator, he or she can always ask for the data needed while ideally and

directly supervising the administrator copying the data. It is imperative the investigator document how the data was collected and from whom it was received to create a chain of custody. It is advisable to create logical evidence files (or forensic images) or hash the files provided to establish a firm baseline of their contents. The logical evidence files can be created in a tool such as AccessData's Forensic ToolKit (FTK) Imager which will create an AD1 file of logical files. The AD1 forensic evidence files will serve as a container for the files and can be hashed and verified.

Use the following steps to acquire specific files or folders on ESXi:

1. Follow the steps detailed above in Acquiring ESXi, The Basics. These steps should include accessing ESXi at the server, accessing ESXi with PuTTy, and documenting all your steps.
2. Create a shared folder which will be where the acquired data will go. That folder can be on the computer used to acquire the data or external media attached to the target computer. The shared folder must have all permissions and full control for the user account on the target laptop.
3. Using either vSphere Desktop Client or vSphere Web Client, connect to the ESXi server and start the source VM if it is not already running.
4. From the source VM (via the vSphere Client window), open a browser or the Run command and connect to your shared folder. In the example below (Figure 12), the shared folder on the target computer was connected to by typing the address listed above and providing the proper credentials.

perry.sans@gmail.com

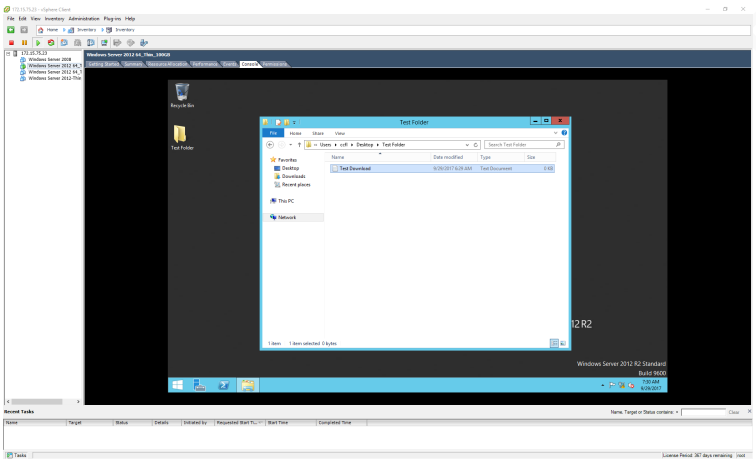

Figure 12: vSphere Web Client, Console View to Running VM

5. Copy the desired files from the VM to the share on the target computer. Perform post-acquisition actions such as hashing and documentation.

An external drive can also be attached to the actual ESXi server and then added to a running VM. Files and folders can then be copied to that newly attached external drive. This method obviously requires physical access to the ESXi server and a free port to connect the external media.

Testing was also done using the Virtual Guest Console (VGC) from VMware Flings, which was last updated in 2010. The VGC could connect to the ESXi 6.5 server, but was unable to access the test folder with the "File Explorer" function. Copying folders and files is also an option with PowerCLI but is beyond the scope of this paper.

3.3. Acquiring an Entire VM on ESXi

The steps to acquire a VM hosted on an ESXi server are straightforward but do require root and administrative-level access to the network and the ESXi. The steps

perry.sans@gmail.com

detailed below are for acquiring a single VM on ESXi 6.5 operating as a Type 1 hypervisor.

1. Follow the steps outlined above in “Acquiring ESXi, The Basics”. These steps should include accessing ESXi at the server, accessing ESXi with PuTTy, and documenting all your steps.
2. While ESXi is managed by a variety of applications and programs, testing has shown that VMs can only be downloaded by the vSphere Desktop Client on a reliable and consistent basis. The vSphere Desktop Client version also must match the version of the ESXi you are accessing.
3. Using vSphere Desktop Client, connect to the ESXi server with the administrator credentials.
4. From the home screen, VMs that are installed and possibly running or suspended can be seen. Select the VM to download and select the "Summary" tab.
5. If the VM is running, pause or shutdown the VM.
6. The Summary tab lists important details about the VM and allows the user to browse the datastore in the "Resources" portion of the screen. Right-click the datastore and choose "Browse Datastore…". A new screen will pop up showing the VMs in the datastore.
7. Select the root folder for the VM chosen to download and select the “Download a file from this datastore to your local machine”.
8. Select a destination folder and begin the download.

perry.sans@gmail.com

Figure 12 below shows the vSphere Desktop Client home screen, the Summary tab, the selected datastore for the Dell 1950 server used for testing, and the pop-up window to choose a destination folder.

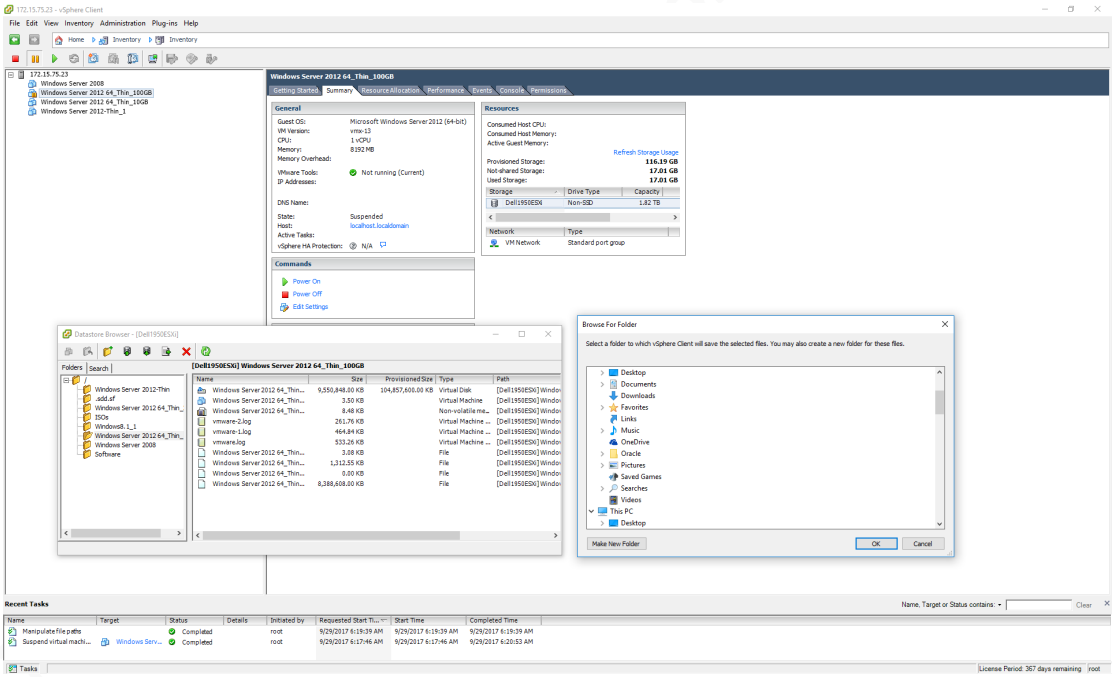

Figure 13: Downloading a VM with vSphere Desktop Client

3.4. Acquiring ESXi in a Non-Permissive Environment

While it is always preferable to have the cooperation of an experienced and knowledgeable administrator who can provide passwords and access to the data needed, it is not always going to happen. Sometimes in the case of exigent or emergency circumstances, the administrator or someone knowledgeable is not available, or that person is not willing to cooperate with the investigation and acquisitions of their data. There is one technique that will be covered in this paper to potentially bypass the root or administrator password on the ESXi and gain

perry.sans@gmail.com

access to the VMs and data you need to acquire: reinstalling the ESXi system partition to reset the root password.

3.4.1. Reinstalling the ESXi System Partition

Reinstalling the ESXi partition, also known as a "repair install," will overwrite any system partitions and configurations, altering the ESXi and potentially making it unusable. However, it will preserve any VMFS datastores and the VMs and data they contain. There are two main concerns with reinstalling the ESXi system partition:

- During the reinstallation, the product license/key will be lost. ESXi will revert to a 60-day temporary license by default. The current license can be re-entered after re-partitioning, but it should be noted it may be lost if not already recorded outside the system.
- Any networking configurations will be over-written, to include the IP address of the ESXi. The IP address of the ESXi will most likely be different after reinstalling the ESXi partition. Because the networking configurations will be over-written, any connections to shared storage will also be overwritten and lost.

Use the following steps to reinstall the ESXi system partition (Marshall, 2015):

1. Create the appropriate ESXi boot media using the ESXi ISO file from VMware. The boot media can be a DVD or a USB device, depending on the available hardware and circumstances.

perry.sans@gmail.com

2. Ensure the server is configured to boot to your ESXi boot media. This step varies greatly depending on the server manufacturer. The following screenshot (Figure 14) shows a BIOS boot menu from VMware Workstation 12.

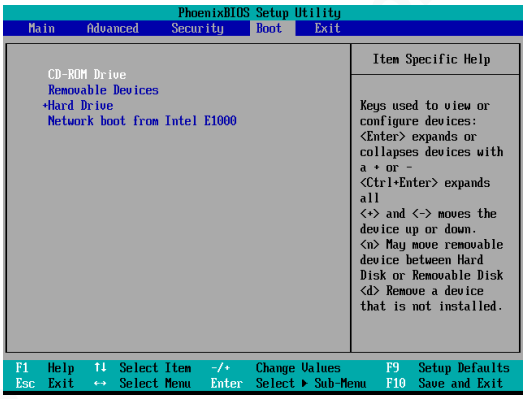

Figure 14: BIOS Menu

3. Power on the server and ensure it boots to the ISO file. The following screenshot (Figure 15) shows the boot menu screen.

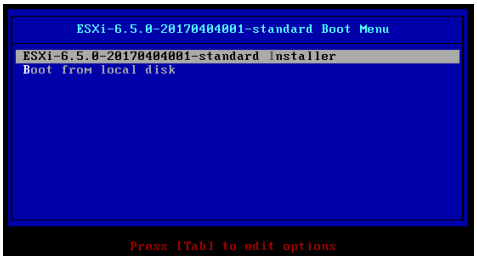

Figure 15: ESXi Installation Screen

4. Press enter to boot to the standard installer. Follow the on-screen prompts and select the option to “Install ESXi, preserve VMFS datastore”. ESXi will detect a currently installed VMFS partition.

perry.sans@gmail.com

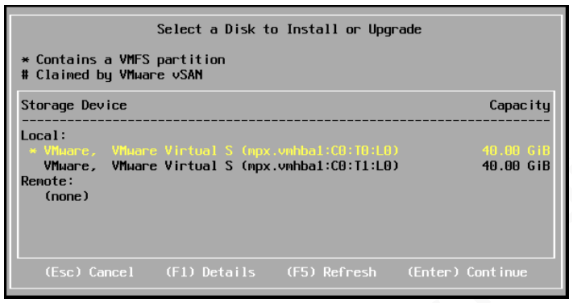

Figure 16: ESXi Install or Upgrade Screen

5. When the following screen is displayed, select "Install ESXi, preserve VMFS datastore".

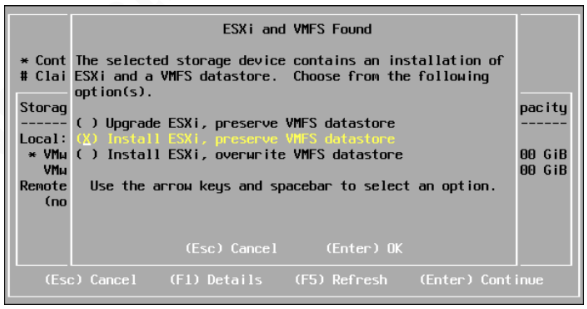

Figure 17: Install ESXi, Preserve VMFS Datastore Screen

6. Type a new password to assign to the root account.

Figure 18: ESXi Root Password Screen

7. Confirm the install by pressing the F11 key:

perry.sans@gmail.com

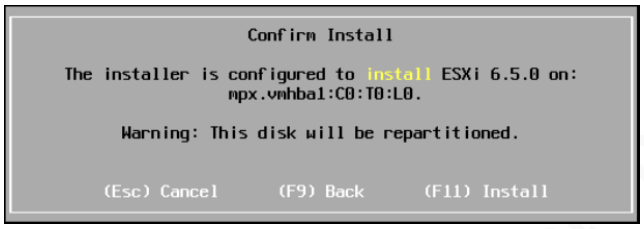

Figure 19: Confirm Install Screen

8. ESXi will indicate that the installation was successful and prompt for a reboot.
9. The ESXi server will more than likely have a different IP address than what was assigned before the re-partitioning and resetting the root password.

An investigator in ideal circumstances will have full cooperation of an administrator and be provided all the passwords necessary to acquire a VM on ESXi. However, the steps detailed in this section will enable an investigator to access ESXi without the password.

4. VM Acquisition Speed Testing

Previous network testing conducted on ESXi with Netperf confirmed ESXi has better TCP and UDP throughput compared to Xen, Hyper-V, and KVM (Hwang, Zeng, Wu, & Wood, 2013); however, this testing did not focus on downloading VMs from datastores, nor did the testing occur over different network connections with different throughput.

perry.sans@gmail.com

To determine how fast a VM hosted on an ESXi server could be acquired, an initial testing environment was built with one ESXi server connected to a single workstation. A default installation of ESXi 6.5 was installed on a Dell PowerEdge 1950 server with two Intel Xeon X5460 processors and 32GB of RAM. The ESXi OS was placed on a 15,000 RPM SAS drive and the datastore was placed on a 7200 RPM SATA drive. A Dell 7910 workstation was used as the acquiring computer. The two systems were directly connected via Ethernet cable. Two VMs of Windows Server 2012 64-bit, thin provisioning, were created to be acquired over the network, one 10GB in size and one 100GB in size. Testing was conducted by acquiring each VM over a 1GbE network connection and then the over a 10GbE network connection to determine if improved network throughput would speed up network acquisitions.

After comparing the results of the initial testing, a second ESXi server was built with Solid State Drives (SSD) to see if download speeds would improve. A default installation of ESXi 6.5 was installed on a Dell 7600 workstation with an Intel Xeon E5-2687W processor and an SSD drive for the ESXi OS and an SSD drive to host the datastore containing the VMs. The testing was performed with the same Dell 7910 workstation and VMs of Windows Server 2012 listed above. After testing the SSD drives, 7200 RPM SATA drives were installed in the Dell 7600 with the same configuration.

4.1. Network Bandwidth Testing

Network bandwidth testing was conducted to verify the connection speeds between the ESXi server and the workstation and to establish a baseline for

comparison for each download. The program iperf was used for network bandwidth testing because it comes already installed on ESXi, is compatible with many different OSs, and can be tuned for various protocols and parameters (Dugan, Elliott, Mah, Poskanzer, & Prabhu, n.d.). To configure iperf for testing I connected to the ESXi via PuTTY and SSH. A working copy of iperf was created on the ESXi to avoid known operation errors working off the original binary of iperf (Lam, 2016) and I disabled both the firewall on the server and the firewall on the workstation ("Troubleshooting ESX/ESXi virtual machine performance issues (2001003) | VMware KB," 2017). Then iperf was ran in client mode on the workstation and server mode on the ESXi server. Results of the testing were recorded to the PuTTY log of the SSH connection to the ESXi server used to manage the testing.

The network bandwidth testing on the Dell 1950 ESXi server demonstrated the data transfer speed for the 10GbE was approximately 60% of the theoretical maximum, while the 1GbE was approximately 93% of the theoretical maximum. The results can be seen below in Table 1.

perry.sans@gmail.com

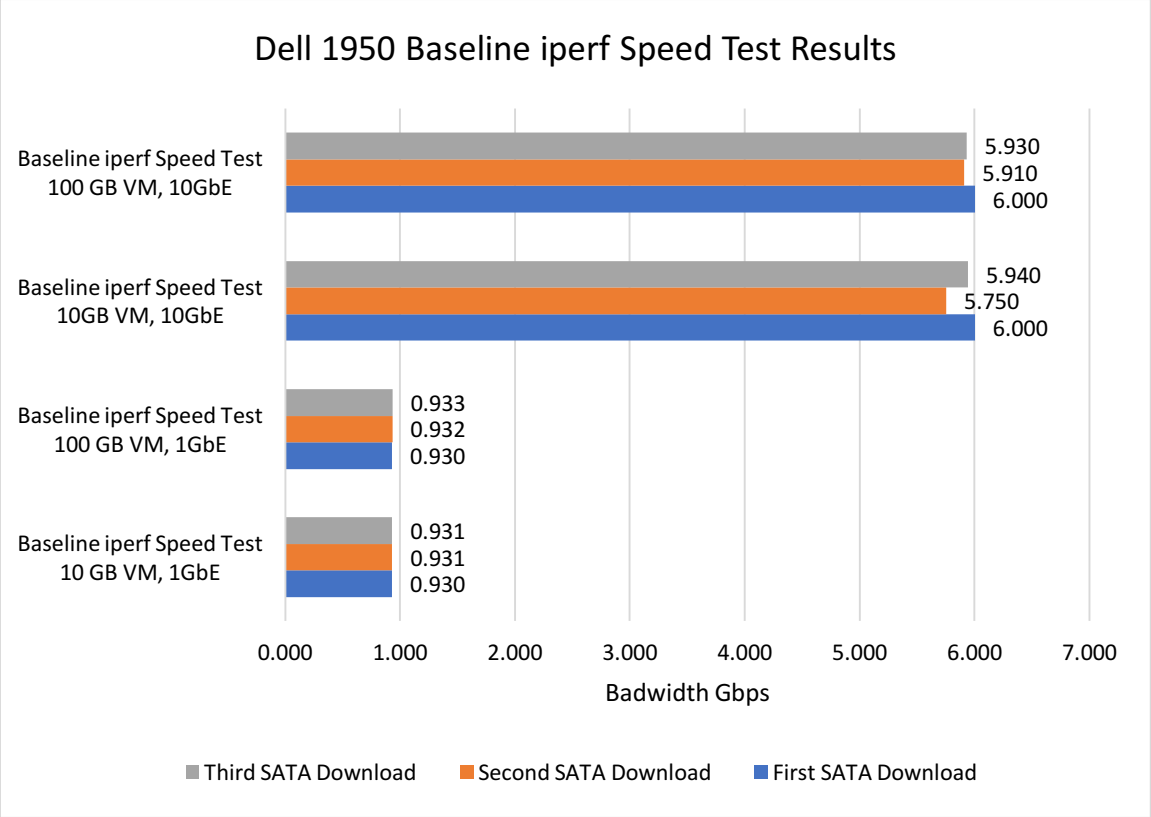

Table 1: Dell 1950 Baseline iperf Speed Test Results

The network bandwidth testing on the Dell 7600 ESXi Server showed the transfer speed of the 1GbE network connection consistently stayed at 93% of the theoretical maximum throughput and the 10GbE network connection averaged 78% of the theoretical maximum throughput. The results for the 1GbE were so consistent that the baselines overlap in Table 2 below.

perry.sans@gmail.com

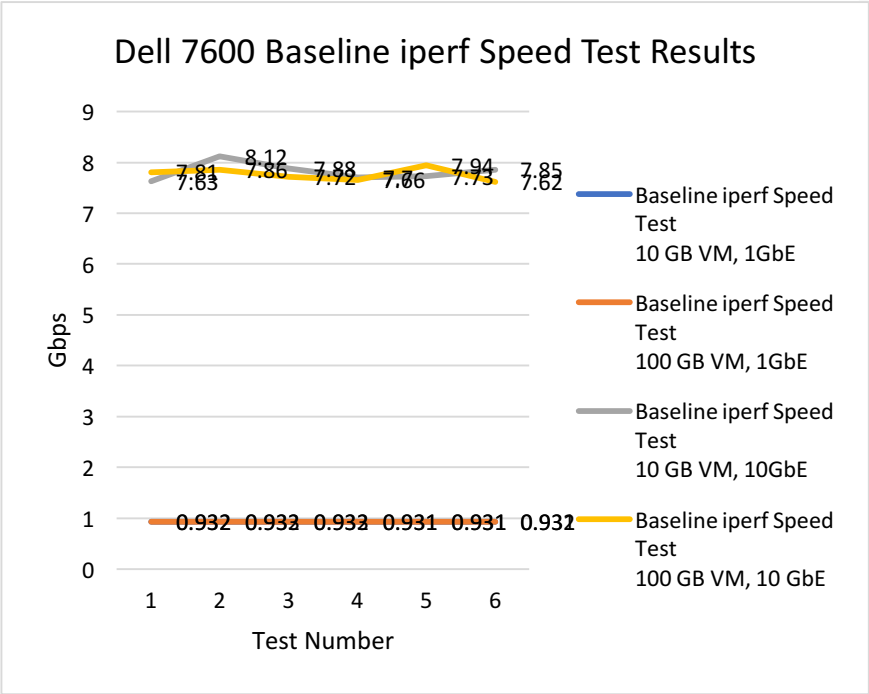

Table 2: Dell 7600 Baseline iperf Speed Test Results

Network bandwidth testing with iperf was performed before each VM acquisition.

4.2. VM Download Speed Testing

Using the techniques detailed in this paper, the 10GB and 100GB VMs were downloaded with vSphere Desktop Client from the Dell 1950 and Dell 7600 ESXi servers to the Dell 7910 workstation. The initial testing environment of the Dell 1950 showed little difference in speed and overall download time between the 1GbE and the 10GbE connection, so a second testing environment was built to test if there was a difference in downloading VMs located in datastores on traditional spinning SATA drives (labeled "SATA" or "HDD" in the testing data and tables) and Solid State Drives (SSD).

perry.sans@gmail.com

To record the download of the VMs, tshark was used for full-content captures. The tools Wireshark, tshark, and capinfos were used to analyze the contents of each download and to determine the speed of each. The overall speed in seconds was then used to calculate Megabytes per second (MBps or MB/s) of transfer speed. Megabytes per second was selected instead of Megabits per second because it is a traditional measurement used for the transfer of data and can be easily compared to other connections common in the computer forensic community. The results of the testing are detailed in Table 3.

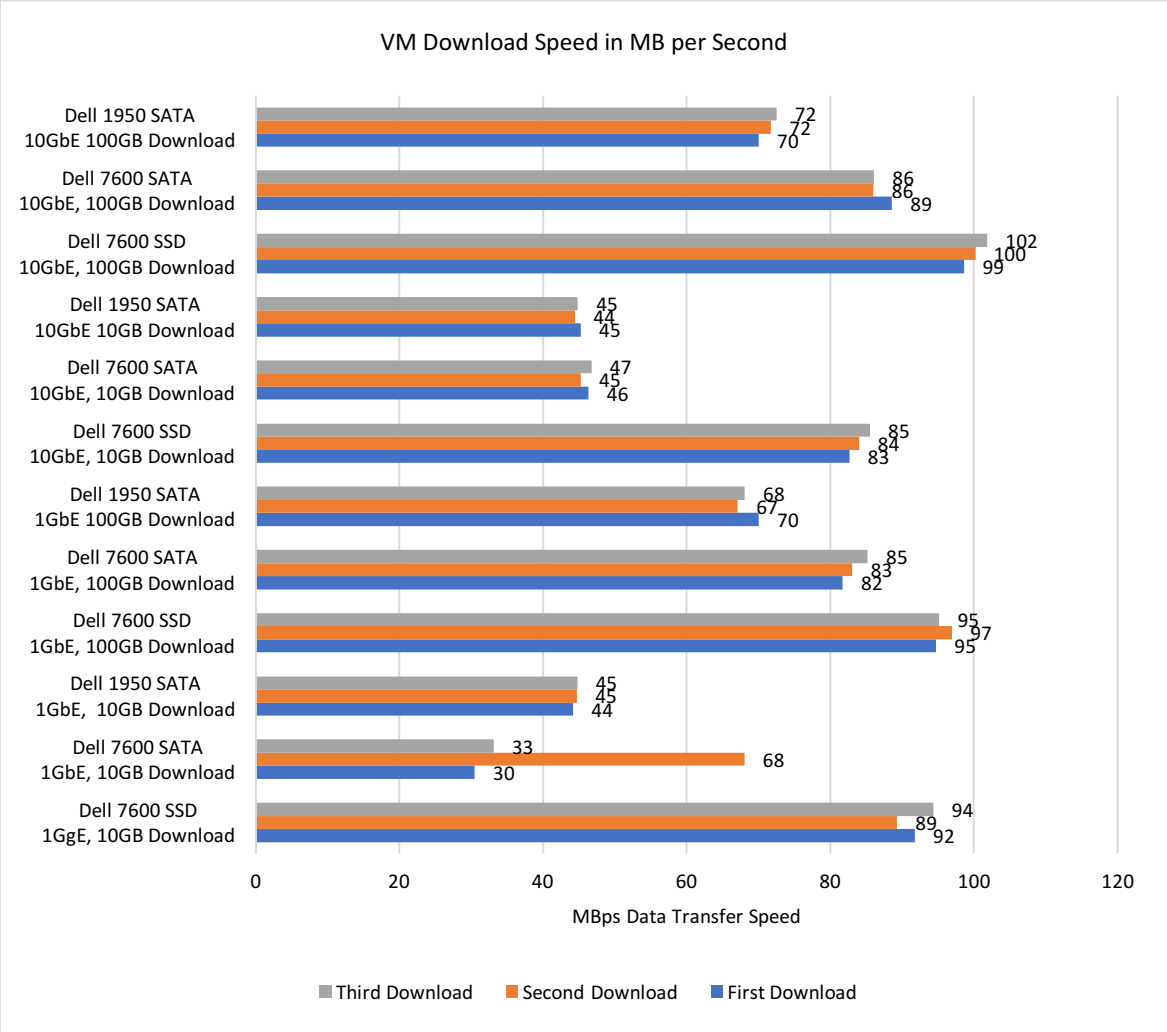

Table 3: Overall Download Speeds of ESXi 6.5

perry.sans@gmail.com

For ease of comparison, the results were then averaged by type of hard drive and connection type, then compared against data transfer speeds for USB 1.1, 2.0, and 3.0 and are displayed in Table 4 ("USB - Wikipedia," 2017).

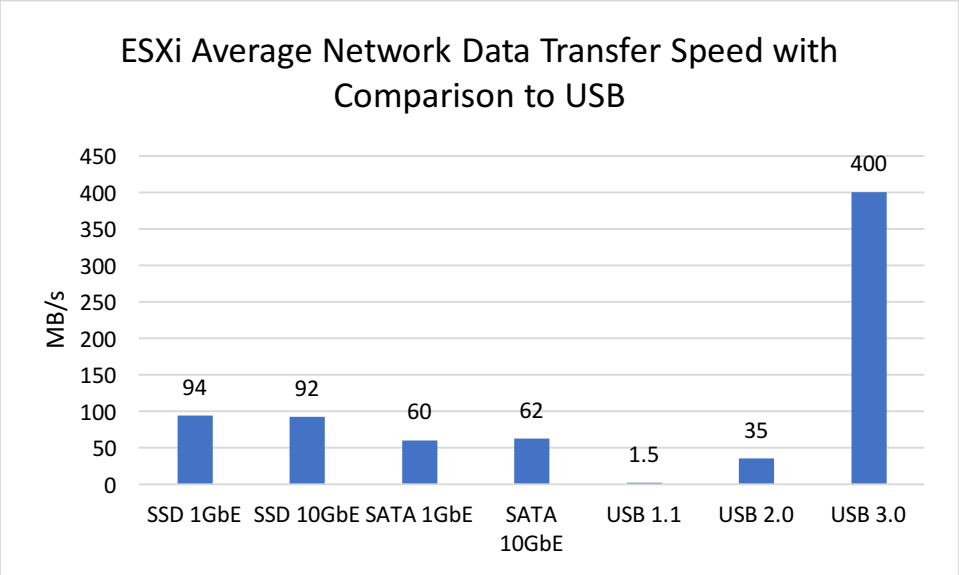

Table 4: Average Network Data Transfer Speed of ESXi 6.5 with Comparisons

5. Conclusion

Updated methods of discovering and acquiring VMs hosted on vSphere's ESXi was demonstrated by building upon previous research and leveraging VMware's provided tools such as vSphere Desktop Client, ESXi's md5sum, and third-party tools such as PuTTY, Zenmap, and LanSpy. Furthermore, the updated techniques were validated with testing in a purpose-built environment consisting of different source media and network connectivity settings an investigator is likely to encounter during an investigation attempting to acquire a VM hosted on ESXi. The results of the testing revealed the use of increased network connection speed (e.g., using 10GbE instead of 1GbE) was not directly proportional to increased download

perry.sans@gmail.com

speed. In fact, the average download speed for each VM downloaded stayed consistent between 1GbE and 10GbE of like-type source media as detailed in Table 3 and Table 4. The only significant VM download speed increase came from downloading the VMs from an SSD disk as opposed to a traditional SATA disk. This research can be used to guide investigators when choosing techniques and procedures to acquire virtualized servers hosted on ESXi and to give them realistic timeframes to complete the acquisitions.

This research can be expanded upon in the future by incorporating other techniques such as using PowerCLI, SCP, SFTP, or third-party tools used by administrators to manage vSphere and ESXi.

perry.sans@gmail.com

References

Barrett, D., & Kipper, G. (2011). *Virtualization and forensics: A digital forensic investigatorś guide to virtual environments*. Oxford: Elsevier.

Bittman, T. J., Dawson, P., & Warrilow, M. (2016). Magic quadrant for x86 server virtualization infrastructure. *Gartner*. Retrieved from https://www.gartner.com/home

Cisco. (2016). *Cisco global cloud index: forecast and methodology, 2015–2020*. Retrieved from https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

Darrow, B. (2017, June 15). Amazon, Microsoft, Google Still Lead Gartner Cloud Rankings | Fortune.com. Retrieved September 11, 2017, from http://fortune.com/2017/06/15/gartner-cloud-rankings/

Dugan, J., Elliott, S., Mah, B., Poskanzer, J., & Prabhu, K. (n.d.). iPerf - The TCP, UDP and SCTP network bandwidth measurement tool. Retrieved from https://iperf.fr/

Giri, B. (2012, August 24). Difference between vSphere, ESXi and vCenter. Retrieved August 26, 2017, from http://www.mustbegeek.com/difference-between-vsphere-esxi-and-vcenter/

Henry, P. (2010, September 28). SANS Digital Forensics and Incident Response Blog | How To - Digital Forensics Copying A VMware VMDK | SANS Institute. Retrieved September 2, 2017, from https://digital-forensics.sans.org/blog/2010/09/28/digital-forensics-copy-vmdk-vmware-virtual-environment/

perry.s

Hwang, J., Zeng, S., Wu, F., & Wood, T. (2013). A component-based performance comparison of four hypervisors. *IEEE International Symposium on Integrated Network Management*, 269-276. Retrieved from http://ieeexplore.ieee.org/document/6572995/

Lam, W. (2016, March 15). Quick Tip – iPerf now available on ESXi | virtuallyGhetto. Retrieved from http://www.virtuallyghetto.com/2016/03/quick-tip-iperf-now-available-on-esxi.html

Marshall, N., Orchard, G., & Atwell, J. (2015). *Mastering VMware vSphere 6*. Indianapolis, IN: Wiley.

Moore, S. (2016, May 12). Gartner says worldwide server virtualization market is reaching its peak. Retrieved from http://www.gartner.com/newsroom/id/3315817

Perneel, L., Fayyad-Kazan, H., Peng, L., Guan, F., & Timmerman, M. (2015). Business hypervisors for real-time applications. *Engineering, Technology & Applied Science Research*, *5*(4), 832-840. Retrieved from www.etasr.com

Rathod, H., & Townsend, J. (2014). *Virtualization 2.0 for dummies* (2.0th ed.). West Sussex, England: John Wiley & Sons, Ltd.

Shavers, B. (2008). *Virtual forensics, a discussion of virtual machines related to forensics analysis*. Retrieved from https://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf

Troubleshooting ESX/ESXi virtual machine performance issues (2001003) | VMware KB. (2017, August 7). Retrieved September 17, 2017, from

perry.sans@gmail.com

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2001003

USB - Wikipedia. (2017). Retrieved October 1, 2017, from https://en.wikipedia.org/wiki/USB

VMware Inc. (2014, 7). *virtualization essentials*. Retrieved August 12, 2017, from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/ebook/gated-vmw-ebook-virtualization-essentials.pdf

VMware vSphere. (2017). Retrieved August 26, 2017, from https://docs.vmware.com/en/VMware-vSphere/index.html

VMware, Inc. (2007). VMware VMotion. Retrieved September 2, 2017, from https://www.vmware.com/pdf/vmotion_datasheet.pdf

VMware. (2006). *VMware infrastructure architecture overview*. Retrieved from https://www.vmware.com/pdf/vi_architecture_wp.pdf

VMware. (2009). Introduction to VMware vSphere. Retrieved August 27, 2017, from https://www.vmware.com/pdf/vsphere4/r40/vsp_40_intro_vs.pdf

VMware. (2009). VMware Unveils the Industry's First Operating System for Building the Internal Cloud—VMware vSphere™ 4. Retrieved from https://www.vmware.com/company/news/releases/2009/vsphere-launch.html

VMware. (2014). *vSphere security, 5.5, update 2*. Retrieved September 19, 2017, from https://docs.vmware.com/en/VMware-vSphere/5.5/vsphere-esxi-vcenter-server-552-security-guide.pdf

perry.sans@gmail.com

VMware. (2017). *vSphere security, 6.5, update 1*. Retrieved September 19, 2017, from https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-651-security-guide.pdf

VMWare. (2017). [Physical Topology of vSphere Datacenter]. Retrieved from https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/com.vmware.vsphere.intro.doc_41/c_physical_topology_of_vi_datacenter.html

perry.sans@gmail.com

Appendix A

Putty Log of VM Inventory

```
=~=~=~=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2017.09.29 10:44:09
=~=~=~=~=~=~=~=~=~=~=~=~=~=~=~=
login as: root
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

[00mVMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] vm-support --listvms
/vmfs/volumes/56dd91a6-77ff2bf6-9502-001ec9b61d46/Windows Server
2008/Windows Server 2008.vmx (Registered)
/vmfs/volumes/56dd91a6-77ff2bf6-9502-001ec9b61d46/Windows Server 2012-
Thin/Windows Server 2012-Thin.vmx (Registered)
/vmfs/volumes/56dd91a6-77ff2bf6-9502-001ec9b61d46/Windows Server 2012
64_Thin_100GB/Windows Server 2012 64_Thin_100GB.vmx (Running)
/vmfs/volumes/56dd91a6-77ff2bf6-9502-001ec9b61d46/Windows Server 2012
64_Thin_2/Windows Server 2012 64_Thin_2.vmx (Registered)
[root@localhost:~] vmdumper -l
wid=70138    pid=-1 cfgFile="/vmfs/volumes/56dd91a6-77ff2bf6-9502-
001ec9b61d46/Windows Server 2012 64_Thin_100GB/Windows Server 2012
64_Thin_100GB.vmx"          uuid="56 4d 87 03 3d 47 40 07-73 82 3d 0c 76 ef 1c 6a"
        displayName="Windows Server 2012 64_Thin_100GB"   vmxCartelID=70137
[root@localhost:~] exit
```

perry.sans@gmail.com

Appendix B

PuTTY Log of md5sum

```
=~=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2017.09.29 11:37:29
=~=~=~=~=~=~=~=~=~=~=~=~=~=
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

[00mVMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] cd /vmfs/volumes
[root@localhost:/vmfs/volumes] ls
[1;34m51e6627a-255c06e8-47fb-dff0dd343f67[0m  [1;34m59c8b206-31926141-
96df-a0369f1d6576[0m
[1;34m59c4bca5-204350be-19d8-90b11c646145[0m  [1;34m99dc5973-bb7f2bd7-
0801-cdfcf3af645a[0m
[1;34m59c8b1fd-5fe379ab-faa1-a0369f1d6576[0m  [1;36mDatastore_SSD[0m
[1;34m59c8b205-85f6da63-b91c-a0369f1d6576[0m  [1;36mdatastore1_HDD[0m
[root@localhost:/vmfs/volumes] cd Datastore_SSD
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145] ls
[1;34m100GB Server 2012 VM[0m  [1;34m10GB Server 2012 VM[0m
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145]
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/100GB
Server 2012 VM] md5sum *
md5sum: can't read 'Windows Server 2012 64_Thin_100GB': Is a directory
 [root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-
90b11c646145/100GB Server 2012 VM] cd Windows\ Server\ 2012\
64_Thin_100GB/[J
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/100GB
Server 2012 VM/Windows Server 2012 64_Thin_100GB] md5sum [J5[J *
md5sum: can't open 'Windows Server 2012 64_Thin_100GB-f076da98.vswp':
Device or resource busy
086160b9f2b3fbf9cc907ef23284971d  Windows Server 2012
64_Thin_100GB.nvram
d41d8cd98f00b204e9800998ecf8427e  Windows Server 2012
64_Thin_100GB.vmsd
af0ac6acbce79c5da316c7d177968073  Windows Server 2012 64_Thin_100GB.vmx
```

perry.sans@gmail.com

```
md5sum: can't open 'Windows Server 2012 64_Thin_100GB.vmx.lck': Device or
resource busy
58eed1bd8d599fd6ddc16c16eb1dec87  Windows Server 2012
64_Thin_100GB.vmxf
e715cb063b6707d6759888af830f7a24  Windows Server 2012
64_Thin_100GB.vmx~
md5sum: can't open 'Windows Server 2012 64_Thin_100GB_0-flat.vmdk': Device or
resource busy
02d627ea8e2813f22ae2cf5b335f9579  Windows Server 2012
64_Thin_100GB_0.vmdk
9acef90445aafc21a5b16809414a3af5  vmware-1.log
8af71669ad446eefc408bf1897002a93  vmware.log
md5sum: can't open 'vmx-Windows Server 2012 64_Thin_100GB-4034321048-
1.vswp': Device or resource busy
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/100GB
Server 2012 VM/Windows Server 2012 64_Thin_100GB] cd ..
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/100GB
Server 2012 VM] cd ..
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145] cd
10GB\ Server\ 2012\ VM/[J
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/10GB
Server 2012 VM] md5sum *
md5sum: can't read 'Windows Server 2012 64_Thin_2': Is a directory
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/10GB
Server 2012 VM] cd 10GB[J[J[J[J[J[J[Jls
[1;34mWindows Server 2012 64_Thin_2[0m
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/10GB
Server 2012 VM] c [Jd Wi[1A
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/10GB
Server 2012 VM] cd Windows\ Server\ 2012\ 64_Thin_2/[J
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/10GB
Server 2012 VM/Windows Server 2012 64_Thin_2] ls
[0;0mWindows Server 2012 64_Thin_2-Snapshot1.vmsn[0m
[0;0mWindows Server 2012 64_Thin_2.nvram[0m
[0;0mWindows Server 2012 64_Thin_2.vmsd[0m
[0;0mWindows Server 2012 64_Thin_2.vmx[0m
[0;0mWindows Server 2012 64_Thin_2_0-000001-delta.vmdk[0m
[0;0mWindows Server 2012 64_Thin_2_0-000001.vmdk[0m
[0;0mWindows Server 2012 64_Thin_2_0-flat.vmdk[0m
[0;0mWindows Server 2012 64_Thin_2_0.vmdk[0m
[0;0mvmware-1.log[0m
[0;0mvmware-2.log[0m
[0;0mvmware.log[0m
```

perry.sans@gmail.com

```
[root@localhost:/vmfs/volumes/59c4bca5-204350be-19d8-90b11c646145/10GB
Server 2012 VM/Windows Server 2012 64_Thin_2] me[Jd5sum *
0a1e2666b6df0c0202e2a7c58195c6d2  Windows Server 2012 64_Thin_2-
Snapshot1.vmsn
7d82c2d4153cd0bbc0fb63388698aa69  Windows Server 2012 64_Thin_2.nvram
2e2958f665d93ceda51514243f12be61  Windows Server 2012 64_Thin_2.vmsd
c3fad61102acd612a16cb350b483d313  Windows Server 2012 64_Thin_2.vmx
67359e25ad5fa9e29d83e9f8a59e9088  Windows Server 2012 64_Thin_2_0-
000001-delta.vmdk
28ea6a9137d700b083940012cc340f37  Windows Server 2012 64_Thin_2_0-
000001.vmdk
7e206e8ae110873cbf625b4ab14f31f1  Windows Server 2012 64_Thin_2_0-
flat.vmdk
1995f8e8027833de5493255826e13bd1  Windows Server 2012 64_Thin_2_0.vmdk
2687e1cb309a47718b98e87fb6e1fbe8  vmware-1.log
a9a8b6ef26aba7782b408a87419fc0a5  vmware-2.log
bd393c1d59514176dee4111c0e8adc44  vmware-3.log
```

perry.sans@gmail.com