Virtual Forensics

A Discussion of Virtual Machines Related to Forensics Analysis

Brett Shavers

The Virtual Machine (VM)

Description of the Virtual Machine

The Virtual Machine Concept in Brief

Virtual machines are not new and have been in use for well over a half century. The fundamental concept of a virtual machine revolves around a software application that behaves as if it were its own computer. The VM application ("guest") runs its own self-contained operating system within the actual machine ("host"). This virtual operating system can be of almost any variant of design. Perhaps put more simply, it can be described as a ***virtual computer running inside a physical computer***.

One of the benefits of virtual machines is the ability for a virtual machine to operate on nearly any underlying hardware and software configuration. In this manner, there is an ease of flexibility of sharing and duplication of virtual machines for many purposes, such as software testing. Additionally, one host machine (the actual computer) can run multiple guest machines (virtual machines) at the same time. A visual example of a virtual machine running on a host system is shown below.

Figure 1-Virtual Machine (VMware Server)

Brett Shavers *Virtual Forensics © 2008*
bshavers@gmail.com

The Uses of Virtual Machines

The number of uses for virtual machines is **limited only by the imagination and needs** of an organization or individual. For the individual, a virtual machine can be a sandbox for not only development and testing of new software applications in a controlled environment, but also for the testing of unknown malware on various operating systems. Virtual systems can be isolated from other virtual and actual systems for tests and analysis, or they can be networked with other machines to determine interaction and processes between machines. Isolated systems can allow for the operation of various types of applications that normally may cause conflicts if run on the same system.

Through the testing of software applications, virtual machines can be replicated in a short amount of time to validate and verify tests. **Testing software** on physical machines require the flattening of the entire hard drive and rebuilding the system to continue testing on numerous occasions. This is not economically feasible due to the time involved to rebuild computer systems nor is it needed.

An organization can have their entire system virtualized to maximize resource potential and decrease the time and effort involved in **disaster recovery** and **business continuity**. Considering that a virtual machine is technically only a file (or more accurately, several files), VMs can quickly be copied and distributed network-wide. In regards to legacy software that may not be supported or operate on newer operating systems, virtual machines can remain in use for specific legacy applications in the workplace for any foreseeable future.

Educational institutions can use virtual machines to teach a variety of information technology topics and courses. Many different operating systems can be demonstrated on a single student desktop requiring little time in setting up the systems. The benefits to the students include more instruction and hands on in a shorter period of time.

For the scope of this paper, the focus will be on the uses of virtual machines as it relates to forensic analysis, with both a virtual machine as your evidence and as an asset to your forensic tool box. Although only one virtual application is noted in this paper, the concepts and theories of their focus can be applied to other applications that are not described. The operating systems referenced are of Microsoft Windows (all versions) as this is the most prevalent operating system used worldwide. Some of this information may apply to other operating system in varying degrees, but again, it is the concept and theory of the examinations concerning virtual machines that will remain consistent across various platforms.

A Brief on VMware Files

Workstation, Player, and Server

An unintended and beneficial use for several VMware products is for the 'non-developer Workstation' users', i.e. forensic examiners. There are three products in particular that fit well in the topics presented; VMware Workstation, Server, and Player. VMware Workstation is perhaps the most versatile of the three products as it allows for more features. This is at a financial cost however since it is not freely available (other than a 30-day trial). VMware Server follows a close second with fewer features, but is freely available. VMware Player, also freely available, has the ability to run VMware virtual machines, but allows for almost no options for configuration, which is needed for forensic examinations.

Given the growing use of virtual machines on personal computers as well as the benefit of being able to boot forensic images using VMware, it is highly recommended to have VMware Workstation as part of any examiners toolbox. There are no other virtual applications (currently) that have the features and functions in VMware Workstation; it's almost as if it were almost developed for forensic use.

The following is a listing of the files associated with a VMware virtual machine. With other VM applications, the files may be fewer or even more, so it is imperative to be aware of the associated file types when dealing with different types of virtual machines other than VMware. The existence of only one of these files can indicate that a virtual machine may have existed on the media being examined.

.Log files –Simply a log of activity for a virtual machine.

.VMDK– This is the actual virtual hard drive for the virtual guest operation system, which may be either a dynamic or fixed virtual disk. With dynamic disks, the disk will start small and grow to a predetermined limit. A fixed disk does not change size.

.VMEM –A backup of the virtual machine's paging file which only exists of the VM is running or has crashed.

.VMSN – These are VMware snapshot files, named by the name of the snapshot. A VMSN file stores the state of the virtual machine when the snapshot as created.

.VMSD–A VMSD file contains the metadata about the snapshot.

.NVRAM– This is the file that stores the BIOS information for the virtual machine.

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

.VMX– This is the configuration file for a virtual machine, such as the operating system, disk information, etc… This is a simple text file that can be easily edited.

.**VMSS**-This is the 'suspended state' file, storing the state of a suspended virtual machine.

.**VMTM**-This is configuration file containing team data.

.VMXF-If a virtual machine is removed from a team, this configuration file remains.

If the computer time is an important aspect of a virtual forensics examination, it is then important to realize how VMware manages time. A VM has the same issues managing time as does actual BIOS, such as daylight savings time issues. A VM also has other issues as well. The major issue is that the virtual machine relies on the host system's actual time and will correct itself to match the host time. This time adjustment is based upon UTC (Coordinated Universal Time or GMT), so the host computer's clock can be in a different time zone from the virtual machine, but the time will be the same if converted to UTC. Conversely, if the time is to be different from the host, which in all forensic examinations will be the case, then the setting must be made to not update the VM to the host's time. These settings are through the "VMware Tools" included with VMware Workstation.

The use of VMware in any forensic analysis is best when the features, functions, and limitations of the applications are known. VMware provides for extensive resource materials for download at www.vmware.com on a wide range of topics on the operating of each product. It is suggested to review and test functions prior to an actual examination in order to lessen the chances for error. VMware Workstation is very intuitive in its use.

The Virtual Machine as Your Evidence

Examination of the Virtual Machine

Traces of a Virtual Machine

Before analysis can be conducted on a VM, it must be found. In most instances, it is a simple as finding a folder named, “My Virtual Machines”. In other cases, there may only be traces of a virtual machine indicating that the actual VM may reside elsewhere, such as on external media or may have been deleted from the source drive. If it is suspected that a VM should exist on your evidence but is not found, a search for traces of VM systems can be conducted to determine if that actually is the case.

Recovering traces of a VM or a VM application will typically not yield the contents of the data residing in the VM, as the **trace remnants may only be references** (.lnk files) to a VM/VM application. However, the occurrences of these traces may give investigative leads to either look for the actual VM on other media or as an indication of computer user activity related to virtual machines. The existence of a VM application is not typically considered unusual or illegal. However, given computer user statements that may be counter to the evidence discovered, the mere existence of a VM can be potentially important in establishing credibility of the computer user if that user is denying the current or past existence of a VM.

Quite simply, the easiest and clearest example of trace evidence consists of recoverable deleted VM files and applications. This can include the “My Virtual Machines” folder, specific VM files, or uninstalled VM applications. Although the target VM may not exist, these obvious references will indicate that you may need to recover additional media for analysis that may exist elsewhere.

There are a number of VM applications available commercially and through both open source and freeware. Many of these applications require an installation on the host machine in order to run a VM. From these types of applications, inferences that a VM may exist is clearly evident in that the application to run a VM exists on the hard drive. Even if these applications are uninstalled, there are remnants left behind that can give the same indication that a VM exists or existed.

One remnant that may be ‘left behind’ after an application is uninstalled or a folder being simply deleted is that of the **program icon** residing on the hard drive. As an example, Mojopac[1], may leave its icon (ringthree.ico) on the hard drive. System files, such as a shared

[1] www.mojopac.com

dll file, may also exist, even after a '*complete'* uninstall of a VM application. With Mojopac, the dll "RingThreeInstallerHelp.dll" may be found in a temp folder even if the application no longer exists. These types of files, extraneous to the operation the programs and sometimes inadvertently left behind by their own uninstall program, can give additional information as to the installation and use of the programs. This information may particularly be of importance concerning the dates and times associated with the files. This would apply to related system files as well. Unfortunately, without knowing which files may be left behind with every type of VM application, it is very likely that these will be missed if uncommon VM applications had been used or are unknown to the examiner. With this thought, it could be a valid expenditure of time to determine what programs had been/are installed and the purpose of unknown program types.

Lnk files, prefetch files, and **MRU** references will typically exist independent of the applications. These file types can give relevant information that a VM application/file did exist as well as additional information relating to their MACE[2] metadata information.

The **registry** will most always contain remnants of program installs/uninstalls as well as other associated data referring to VM applications. **File associations** maintained in the registry will indicate which program will be started based upon a specific file being selected. In the Windows registry, under HKEY_CLASSES_ROOT, file associations can be seen. File extensions that exist which are identifiable as VM file extensions will show the application configured for opening that file. As an example, VM Player[3] will be shown to run when files with the vmdk extension are accessed, so even if VM Player does not currently exist on the media, the file association may be indication that it did exist at one time.

Considering that a text list of known VM applications can be created (an online search quickly reveals that there are over 50 different applications currently available, and certainly, more to be developed), a keyword search of as many virtual applications that can be found may reveal trace VM information residing on the hard drive.

Several VM applications, such as VMware[4] (Workstation/Server/Player), will install **virtual adapters** for use in their virtual machines. The existence of "VMware Network Adaptor" without the presence of a VMware application can be a strong indication that the application did exist on the computer in the past.

It is important to note, that although trace evidence may be found to indicate a VM application may have been accessed in some fashion on an electronic media, it does not

[2] Modified, last Accessed, Created, Entry dates and times-MACE
[3] www.vmware.com
[4] References to VMware are to the three applications of VMware Player, Server, and Workstation

necessary confirm that the application was actually installed on that media. Several VM applications can be accessed and run from externally attached media, to include USB flashdrives or even run from a CD. These externally accessed devices are sometimes considered **'throwaway' or 'disposable' operating systems** due to the simplicity of use of having an extensive array of applications accessed virtually coupled with the ease of quickly throwing away the device to avoid detection or recovery as evidence. This use of a VM can be considered to be "anti-forensics" if intended by the user to avoid detection of computer use activity by forensic experts.

Collection and Recovery of Deleted or Encrypted Virtual Machines

Through data recovery/forensic means, many deleted files can be recovered, in part or whole, depending upon the severity of the fragmentation and method of deletion. Given a typical scenario whereby a user deletes a file to the recycle bin and empties the recycle bin, it is usually possible to recover those files in whole for review. Virtual machines, because of their typical sizes, may not have been sent to the recycle bin due to a file size limit of the Windows Recycle Bin. These files will be deleted directly by the system, but still may be recoverable for analysis. However, given a certain amount of fragmentation and inability to fully recover a VM, it may be impossible to examine the contents of that VM, at least to the extent of examining it as a physical system.

The encryption of a VM can be through several layers. The actual folder containing the VM can be encrypted by either basic Windows encryption (EFS[5], full disk encryption such as BitLocker[6], etc…), or a by a 3rd party encryption application. Bypassing this encryption ranges from possible to highly improbable depending upon the level of encryption. Additionally, the virtual operating system itself may be encrypted. As a virtual machine behaves as if it is a physical machine, it enjoys the same benefits of being able to be encrypted as an operating system, just as its host system can be encrypted. The access of encrypted files or the access of encrypted operating systems (virtual or otherwise) is a study beyond the focus of this paper. The encryption of the VM files is like any encrypted file and must be handled in the same manner.

Imaging and Cloning of Virtual Machines

Traditional acquisition of physical operating systems has generally involved abruptly interrupting power to the computer and cloning (imaging) the hard drive by use of hardware or software write blockers with software imaging applications. As the forensic imaging of a

[5] www.microsoft.com EFS- Encrypting File System
[6] www.microsoft.com BitLocker Drive Protection

physical hard drive includes all data on the hard drive, any VM that exists will be cloned in full, as it exists on that hard drive as well. In theory and practice, there could be more than one VM on a single hard drive, even to the extent that dozens of various types of VMs can exist on a single hard. In this type of scenario, the act of creating one image of a hard drive in fact may be creating one image containing dozens of (virtual) self contained operating systems.

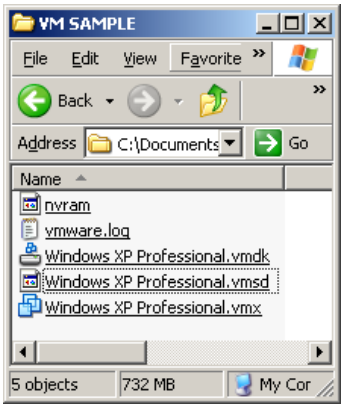


Figure 2 VMware Virtual Machine Files

Virtual machines of interest that exist on a physical media that is not of interest, can be acquired without the need to image the physical media by copying the files of the VM. This method, although workable in obtaining the VM files, may not be the preferred method in collecting best evidence, as additional data related to the VM existing on the physical media may be of vital importance to the examination. This additional evidence can be in the form of MACE dates and times of the actual files and VM application as well as files and activity that may have occurred between the host and virtual machine. It would be better evidence gained to forensically image the host media and export the VM files from the forensic image. As can be seen in Figure 2, there are several files associated with a virtual machine that are needed for the VM to function.

Basic copying of these files onto another media or folder should copy all that is needed to boot the VM. However, copying these files from original media may alter the MACE system metadata. It is advised that if the integrity of the VM is important to maintain, that forensic processes be followed to create qualified original copies of the VM files. The file extension of **vmdk** is the **Virtual Machine Disk/VMware Disk**, which contains the virtual machine, however it is not the only file needed to access the virtual machine. By not acquiring all the necessary files of a VM, it more than likely will not be bootable or accessible later. Not knowing where related files exist when conducting a simple copy may render your efforts useless. Virtual machines may also be linked together in teams or may require the existence of a folder on the host drive that contains files associated to the virtual machine. It is vital to capture the entire host if possible to avoid missing files necessary for a VM to operate as well as miss shared folders that may exist.

Additionally, a VM may have a shared folder on the host machine. Copying the VM by itself from the host will not copy any shared folders on the host machine. Valuable evidence may be missed by not capturing the host media in its entirety. Virtual machines using different applications than VMware will have different file extensions than shown in Figure 2. In the context of VMware, unless otherwise noted, it is intended that VMware refers to the applications related to this paper to include VMware Workstation, VMware Player, and VMware

Server. Although not an intended function of these programs, each of these three applications is well suited for forensic examinations.

As a virtual machine is simply a collection of files that when opened by its associated program, will behave as an operating system within its host, the files should be able to be easily copied by nearly any means for examination. The examination of these native VM files cannot be merely examined with forensic tools, at least if the intent of examination is the analysis of the VM files as an operating system and the user data contained within. The virtual operating system files need to be exported or the VM must be mounted as a drive as if it were a physical operating system for examination. These methods are necessary in order to examine the contents of a VM's internal data.

With the skills, technology, and knowledge available today, '**live acquisition'** has started to become a consideration when a computer system to be imaged is encountered during a running (i.e. *live*) state. The practice of acquiring a live system differs than that of the method of pulling the plug, in that software applications may have to be run on the suspect machine to acquire the image and system memory. It is possible that encountering a live system to be acquired in a live state, may involve a virtual system running as well. Acquiring the host system will also acquire the running VM, however, a consideration would be acquiring the VM in its live state as well, in effect, creating two separate images from one physical machine. Running processes and the virtual system's memory may just as important, or maybe even more so, than its host.

One method of exporting a virtual machine is to use the virtual machine's associated program. As a virtual machine boots into its own actual operating system, it can be **booted in a forensic environment** using a forensic boot media, such as a forensic floppy or compact disk. This method differs only slightly than imaging an actual physical media, but in concept, it is the same. This method requires adding an attached media as the destination drive for the forensic image. With VMware, a physical or virtual external device can be added as the image destination drive. It is comparable to 'plugging in an USB drive' physically; however with a virtual application it is done by selecting the options to create a virtual drive (basically a folder, partition, or physical media) to be attached/linked the virtual machine application. Once connected to the virtual machine, the virtual machine's BIOS boot order must be configured to boot from the forensic media and not to the virtual operating system.

With a VMware virtual machine, the forensic media can be ISO images or actual physical media such as a floppy or compact disk. This option may not be available with other virtual applications. After the configuration of the BIOS boot order and addition of destination media, the VM can be booted to the forensic environment for imaging as if it were a physical machine.

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

The forensic boot environment, whether it is DOS or Linux, will allow for the virtual operating system to be forensic imaged to the previously attached destination media. The VM operating system never needs to be booted for imaging in order to avoid any changes to the original VM. The resulting forensic image is a complete bit stream clone of the virtual machine as if it were imaged from actual physical media.

If the evidence VM is a VMware virtual machine, **FTK Imager**[7] provides perhaps the fastest and most error free method of imaging. Using FTK Imager, a VMware virtual machine can be added as an evidence item simply by opening it as an image file. FTK Imager can then preview the VM as if it were a physical drive as well as creating a forensic image of the VM to a destination location. This is perhaps the single best method to create forensic images of a VMware virtual machine.

Virtual machines may also be **mounted as physical drives** through various commercial software applications. When mounted as a physical drive, the virtual machine can be imaged, copied, or examined as such.

An obstacle to the collection of a VM may be in the location of a VM existing on a virtualized network system. Many organizations have become 'virtualized' in which entire networks are virtual systems. These systems can consist of a single 20 terabyte virtual machine, on which, numerous client machines (also virtual machines) are connected. Imaging a 20 terabyte virtual machine may not be practical with technology currently available. The collection of a client virtual machine on a virtual network will require additional steps to ensure best evidence collection.

As organizations move to virtualized networks where virtual clients can be pushed out on a regular basis, it is highly probable that a virtual machine on a client computer may not exist today as it did last week due to the virtual client being replaced with either a newly configured VM or a VM common to the organization. Although this concept is the same that is currently accomplished by IT staff by physically pushing out images to hard drives, the virtual method is much faster, easier, cheaper, and therefore, may be done more often. Given a time frame of activity in question that needs to be captured and examined, if client virtual machines are replaced on a frequent basis, the only copy of that suspect machine may exist on a backup system that may need to be restored prior to capture.

After a virtual machine has been imaged through any of these means, the image can be examined fully as if it were an image of an actual system using nearly any forensic applications available. As can be imagined, a single hard drive containing one (or more if it's a dual boot)

[7] FTK Imager: www.accessdata.com

operating system can practically contain many virtual operating systems that are essentially complete computer systems. For examination purposes, this scenario can drain forensic resources as one computer hard drive may actually be dozens of independent systems to examine.

Examination of Virtual Machines

Examination of an imaged/mounted virtual machine is nearly identical, if not completely identical, to that of an imaged physical computer system or actual media. Once the virtual machine is accessible through the means discussed thus far, the forensic tools and processes do not differ from traditional forensics. Virtual machine forensics does incur an additional analysis related to the virtual machine files associated with the host machine. The system metadata associated with the virtual files and the virtual application as they reside on the host machine may give additional information that may be of importance. This data, whether it is MACE metadata or information of the host computer user accounts logged in at time at virtual machine access, can give inferences as to the actual computer user, or at a minimum, the computer user account logged in.

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

The Virtual Machine as Your Forensic Tool

Restoration of Forensic Images into Virtual Machines

Not long ago, restoration of a forensic image meant several hours, if not an entire day, of restoring an image back to disk, to be placed into a physical computer and booted. Often times, this meant numerous attempts to configure a restored drive to recognize different hardware if the original physical computer was not used. The process involved setting up a complete computer system in hopes of emulating the original system as it looked originally prior to be imaged.

With virtual machine applications, a VM can be booted directly into an environment on the forensic machine, in a window, with only a few mouse clicks. The majority of hardware issues are configured automatically and sometimes the only issue is the activation of Windows or repairing Windows given a 'blue screen' upon booting. These two issues are the same issues to overcome whether the restore is an actual physical restore to a complete computer system or a restore to a virtual environment. However, the time spent in the restore is dramatically reduced when using the virtual applications.

The reasons for booting a virtual machine can be many. Often times, it may be for the benefit of non-examiners, such as court officers and jury to demonstrate a suspect computer seen as it was seen by the suspect prior to seizure. Forensic analysis reports may be difficult for the lay person to understand, but showing a computer screen with an operating system running is not. A restored system can be used to visually show how folders have been created and named as well as how automated processes were configured. Other reasons to boot a restored image may be to test theories, either to prove or disprove claims of 'Trojan horses' or other malicious software. These tests can be made with the results captured using snapshots in time.

Booting a virtual machine directly or booting the image of the virtual machine will achieve the same effects as both will behave identically. For best evidence, booting the forensic image may be the better option instead of booting the actual virtual machine. One of the benefits of booting the forensic image is that of validation. Forensic images will typically contain metadata validating the image as an original copy by hash value. The image can also be shared with other examiners to be booted for examination and demonstration and rebooted on

multiple occasions without altering the forensic image. Booting a virtual machine will incur numerous changes to the VM files and virtual system.

Booting a forensic image requires certain steps prior to booting. Depending upon the format of the image, it may be bootable without several software applications. DD images can be booted directly with some VM configuration files whereas Encase[8] images (Expert Witness Format) require mounting before making configuration files to be bootable. Using a combination of freeware, open source, and commercial software applications, forensic images can be quickly booted directly into a virtual environment regardless of their original format.

Booting the original disk is not a forensically sound process as there will be irreversible changes to the original media. In cases where the original disk is to be booted for analysis, booting the disk into a virtual environment can prevent those changes from occurring. By using a write protection device to connect to original evidence, VM configuration files can be created in which the original evidence drive can be booted into a virtual machine without changing the contents of the evidence. Although not best practices, this may be a necessity in cases where time is of the essence to obtain electronic evidence while maintaining the original evidence state.

As VMware has many options to configure a virtual machine that mimic a physical computer, an important feature to **not use is the bridged networking** function unless you desire your VM to have access to network resources such as the internet. At times, it is the sole reason to boot into a virtual environment in order to have the ability to document interactions with the internet as well as configuring several virtual machines to interact with each other on a virtual network.

[8] Encase images www.guidancesoftware.com

The Virtual Machine as Your Forensic OS

Using a Virtual Machine as your Forensic Operating System

A Clean OS Every Time

In certain cases, an examiner may be choose to maintain the original or imaged hard drive of a forensic machine after the conclusion of an examination for evidentiary purposes. This could be due to preparation of substantial criminal charges that may require an examination of the forensic machine to determine the validity of the forensic software applications used. Although this may be rare, if it is a possibility or reality, then perhaps conducting the forensic analysis in a virtual environment may be the most feasible option.

Using a virtual machine for forensic analysis has drawbacks. These include the recognition of software protection devices (dongles) that are placed into the physical machine, but not seen by the virtual machine, or unexpectedly being removed (virtually) during analysis. This situation is sometimes overcome by ensuring the virtual machine is maximized on the computer, or by reinstalling the software protection device(s). Other issues are reduced computer performance as the virtual machine shares resources with the host machine. Additionally, virtual machines may not always have the fastest connections available for use, such as Firewire. The forensic image to be examined could be placed within a folder on the C:\ drive of the virtual machine. Direct access in this manner will give the best performance. Additionally, since the entire virtual machine containing the forensic image can be maintained together, it makes for a more secure storage environment.

A virtual machine can also be used as forensic operating system as a convenience. Due to the ease of virtual machine replication, either from simple file copying of the virtual machine or through cloning, a complete forensic virtual machine can be created and reused by reverting to the original virtual system. This ensures a 'clean start' for each forensic examination. A complete "forensic operating system" can also be carried with an examiner offsite, whereby all forensic applications will be available within a virtual environment, if needed for use on other computer systems.

The Virtual Machine Used as “Anti-Forensics

Using a good tool for bad things

Disposable Operating Systems

Virtual machines can be a valuable tool in forensic investigations and can also be used to thwart forensics investigations just as easily. As a virtual machine is only a file or set of files, it can be carried on removable media and accessed on nearly any computer. Several types of virtual machines require an associated program in order to boot the VM. As an example, a VMware VM requires one of its associated programs (Workstation, Player, or Server) to be installed on the host machine in order to run. Other virtual machines may be able to run from an external device without having an associated program installed on the host machine.

Virtual machines that exist on removable media can be disposed easily after use or the media can be encrypted with various encryption schemes to prevent access if discovered. It is possible to use portable virtual machines to access data on host machines for illegal purposes. Cybercrime activities, such as intellectual property theft or other high tech related criminal activities can be conducted on a host machine with all user activity occurring within the virtual machine. An analysis of the host machine will show some activity, however, the virtual machine, which may not be available, will have the evidence needed to show specific user activity. With the ease of duplication of virtual machines, several virtual machines can be saved to individual external devices and discarded after each use.

Within the corporate environment, employees with administrative rights access can run virtual machines to conduct activities against policies or commit illegal acts within a virtual machine. Network logs may show internet/intranet activity; however, for specific activity within the virtual system as it relates to the host machine, evidence will remain only within the virtual machine. Through plausible denials (“That’s not my thumbdrive.”) and encrypted folders containing virtual machines that may be improbable to access, the use of virtual machines as an anti-forensics tool greatly hinders any investigation.

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

How to…

Brief descriptions of "How to" scenarios concerning virtual machines

There are a multitude of benefits to forensic investigations related to virtual machines. The following pages are some of the methods and processes that can be followed to benefit an analysis. Many of the suggestions are geared toward the VMware virtual machines as VMware offers benefits in a wide range of configuration options, ease of use, and cost, ranging from free to moderate cost.

Different virtual machine applications may be processed in similar manners as detailed herein, however, it is up to the examiner to validate findings, processes, and procedures. As technology continues to improve, the steps described may change, typically to be easier and quicker. With the introduction of LiveView[9], as an example, several steps of configuring an image to be booted into VMware have been eliminated.

Clones of virtual machines may also be created from within their respective application. VMware Workstation has the ability to create a clone of an existing virtual machine that can be used as a backup or copy for examination and testing. These clones will operate and will be similar to the original, however, there are differences. A clone's created with VMware will have a MAC address and UUID that are different from those of the parent virtual machine. The cloning feature of VMware should be considered to have the same meaning as a forensic clone, as it is not the same. The imaging methods in this paper detail means to acquire true forensic clones.

The Programs and Methods

An overview and description of the programs discussed is in order. Some of these programs are freely available while others are commercially available with free trials (15-30 days). Given an infrequent use of restoring images for booting into virtual environments, it is entirely feasible to use the freely available and trial applications on an as needed basis. However, for regular use, the purchase of full versions may be best in order to have full feature sets and technical support.

BSOD *(Blue Screen of Death and other headaches)*

Just as booting any computer can give you problems with blue screens and missing vital boot files, a virtual system will give the same. Some of the problems faced are **activation**

[9] www.liveview.sourceforge.net

issues with Windows XP and Vista. The restoration of any drive to an actual drive or virtual environment will create the same problems if there are substantial hardware changes. Virtually, this may be an issue on many occasions.

The solutions to these issues are the same as if it were a physical computer. If the original OS installation CD/DVD is available, it may require repairing the OS boot files. Basic A+ skills are required regardless of the environment (physical or virtual).

The Steps to Boot a Forensic Image to a Virtual Machine

In general, to boot a forensic image into VMware, configuration files are created for an image (or physical disk), which are then loaded into VMware for booting virtually. To protect physical disks (not forensic images) from changes during booting, use a write protection device such as a hardware write blocker.

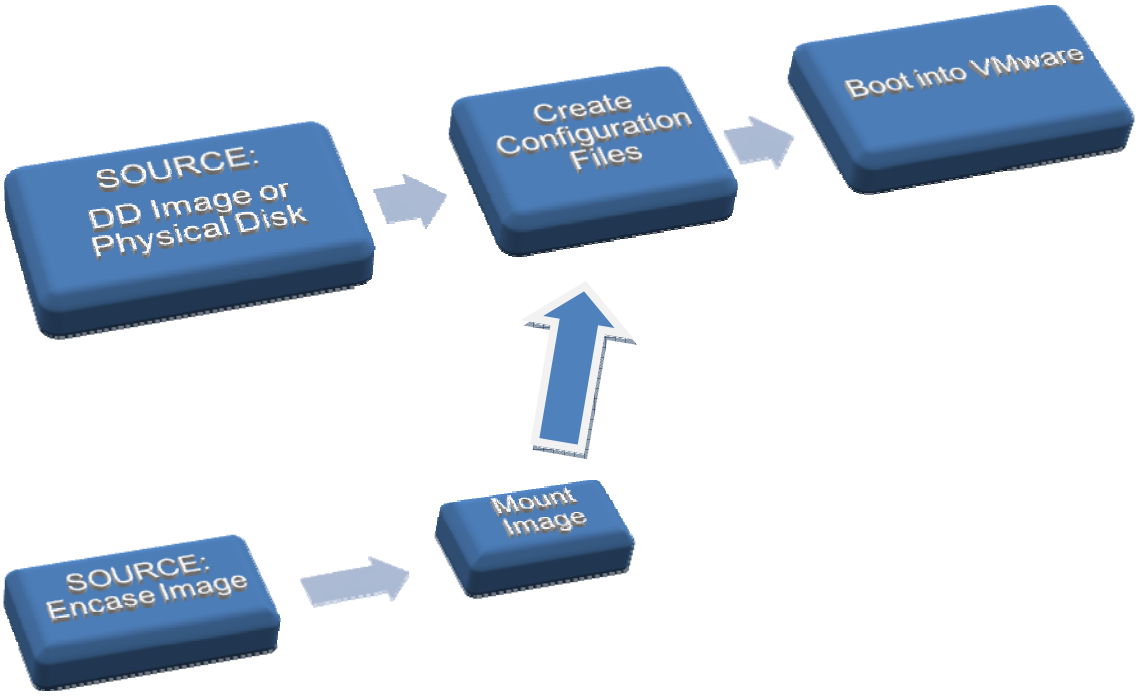
To boot a forensic image into VMware, several software applications are required, listed below:

- VMware Player, VMware Server, or VMware Workstation, **and;**
- VMware DiskMount Utility[10], **and (*suggested*);**
- An application to configure the VM files (such as LiveView, Virtual Forensics Computing[11], or ProDiscover[12]), **and;**
- An application to mount an Encase image (Mount Image Pro[13], Paraben P2 Explorer[14], Encase Physical Disk Emulator[15]) **or;**
- An application to convert an Encase image to DD to avoid having to mount an image

With these installed applications, the steps shown on the following page can be made to boot a forensic image or physical disk into VMware. The number of steps required will depend upon the type of image and whether or not the image needs to be converted to DD and/or mounted as a disk for configuration of the VM files.

[10] www.vmware.com
[11] www.mountimagepro.com
[12] www.techpathways.com
[13] www.mountimagepro.com
[14] www.paraben-forensics.com
[15] www.guidancesoftware.com

Steps to Boot Virtually (from an image or physical disk)



Brett Shavers *Virtual Forensics © 2008*
bshavers@gmail.com

Disk Image Mounting

Forensic (non-DD) images will need to be mounted as disks for booting into the virtual machine environment. Automated software is typically the most efficient method to mount images as disks. If the forensic image is a DD image, disk mounting is not necessary as configuration files can be made specifically for DD image booting into VMware using the aforementioned programs.

- **Mount Image Pro**

http://www.mountimage.com/

Mount Image Pro is a commercially available product that has a 30 day trial and is capable of mounting Encase images, DD images, and SMART images as drive letters.

- **Paraben P2 Explorer**

http://www.paraben-forensics.com/

P2Explorer from Paraben Forensics is capable of mounting forensic images (to include Encase, DD, Safeback)

- **Encase Forensics Physical Disk Emulator**

http://www.guidancesoftware.com

Guidance Software's Encase (Physical Disk Emulator) is capable of mounting Encase images as a drive letter.

- **SmartMount**[16]

http://www.asrdata.com/

ASR's SmartMount is capable of mounting Encase, SMART, DD, and **VMware Disk Files (.vmdk).**

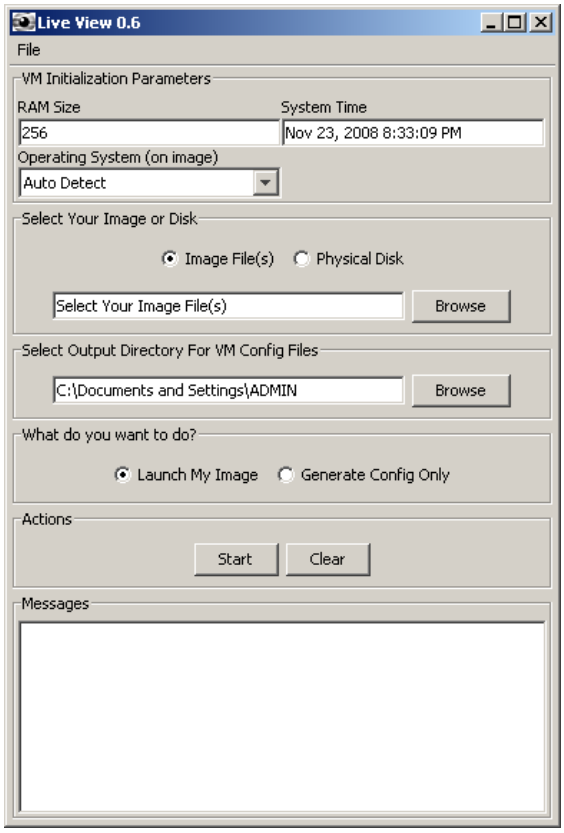
[16] SmartMount ASR Data

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

Configuring the Virtual Machine Files

It is possible, though time consuming, to manually create the virtual machine configuration files for booting; however, there are automated processes that can be used that are more efficient. Some of these tools and methods available include:

- **LiveView** (http://liveview.sourceforge.net/)
    - LiveView is a **freely available** application designed for booting disk images into a virtual environment. Used alone, it can create the configuration files to boot DD images and when used along with disk image mounting applications, it can also be used to boot Encase images as well.



    - An image file (DD) or physical disk (either an actual physical disk or an image file that has been mounted as a disk) can be configured to boot into VMware using LiveView.

Brett Shavers *Virtual Forensics © 2008*
bshavers@gmail.com

- **ProDiscover Basic** (http://www.techpathways.com)
    - ProDiscover Basic is **freely available** forensic application that has many features in addition to being able to create VM configuration files. Actually, the ability to create the VM configuration files is a small feature of this application as it does so much more.
    - With ProDiscover Basic, simply choose your evidence file (DD image) and the VM configuration files will be created.

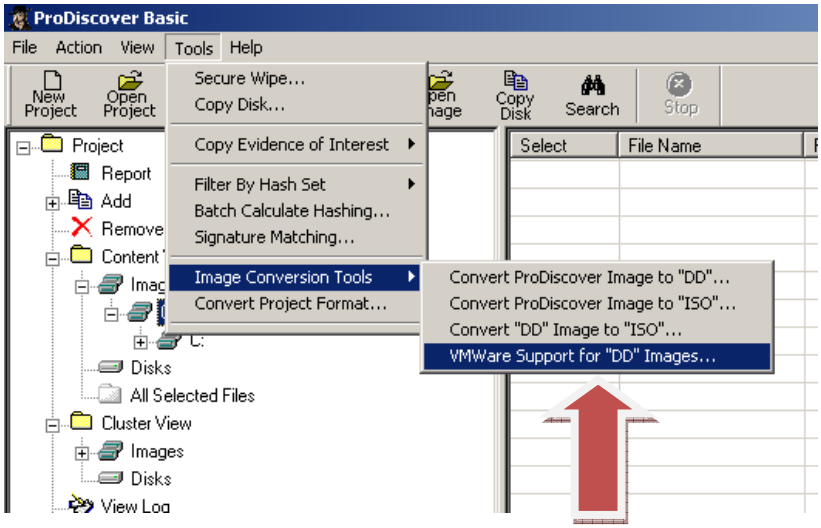


Figure 4 VMware Support with ProDiscover Basic

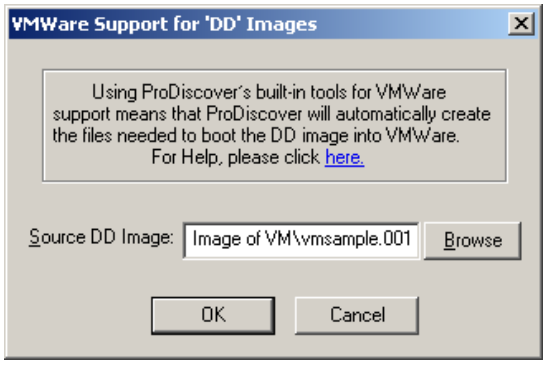


Figure 3 Autoconfiguration with ProDiscover Basic

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

- **Virtual Forensics Computing** (http://www.mountimage.com/)
    - Virtual Forensics Computer (VFC) is a commercially available product that also has a 15 day trial period. Used alone, it can create the configuration files to boot DD images and when used along with disk image mounting applications, it can be used to boot Encase images as well.
    - Given an image which other methods of creating configuration files may not be working, VFC seems to have a higher success rate to create a bootable image.

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

VMDK (VMware Disk) Mounting

The mounting of VMware VMDK files is possible through command lines and automated tools. By mounting a VMDK file, it is not necessary to have any VMware Application installed (Workstation/Player/Server) other than the VMware Disk Mount Utility. By mounting a VMDK (VMware Virtual Machine), access to the VM as a drive letter is achievable, allowing for file transfer (read-write) as well as having access to perform analysis as a mounted drive.

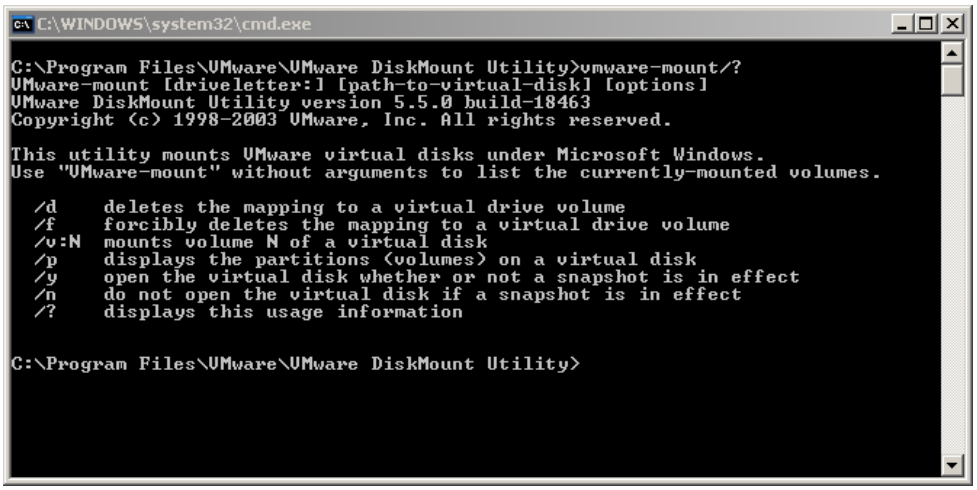
Mounting a VM as a drive letter, in which changes are made, are not in the best interests of forensic processes. As an option, a VM can be mounted on a write protected external media protecting the VM against unintended changes.

- **SmartMount** (http://www.asrdata.com/)

ASR's SmartMount is capable of mounting VMware Disk Files (.vmdk) directly.

- **VMware DiskMount** (http://www.vmware.com/)

VMware's DiskMount Utility is capable of mounting VMware Disk Files through the command line. Once installed, entering the command of **"vmware-mount /?"** in a DOS shell, a list of command line options will be shown for mounting the VM.



From the command line, typing in a command as below mounts the VM to a drive letter of your choice:

vmware-mount **j**: "C:\Documents and Settings\user\My Documents\My Virtual Machines\Windows XP Professional\Windows XP Professional.vmdk"

- **Other Utilities**

A set of utilities are available from http://petruska.stardock.net/Software/VMware.html, in which a GUI version of the above command lines can be used.

Ken Kato (http://chitchat.at.infoseek.co.jp/) also provides several VMware utilities including those that are useful for mounting VMDK files.

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

Imaging Virtual Machines

It's Kinda Like a Real Hard Drive, but Not Totally…

Why Image a VM?

Possessing a VM to examine is not any different than possessing a hard drive to examine. The main difference is that to effectively examine a virtual machine using the same tools and processes that are common to computer forensic investigations, it is best to export (image) the virtual machine into a common forensic format. Whether the format is DD, SMART, Encase, or Safeback[17], having a forensic image that can be validated and verified has all the benefits of conducting a professional forensic examination.

Creating a forensic image of a virtual machine will also allow for the booting of that image almost as easy as booting the original virtual machine without the risk of making inadvertent changes to the original evidence. The concept of creating a forensic image of a virtual machine is no different than that of creating a forensic image of a hard drive. Safeguard the original against changes. Verify and validate the image. Work on the image, not the original.

The following methods of creating forensic images can be conducted on VMware virtual machines as well as some of the methods being able to work on other virtual applications too. As with any forensic process and procedure, it is up to the examiner to validate the processes with multiple tools.

FTK Imager

FTK Imager is the first choice of many examiners for acquiring evidence from physical hard drives. Few examiners have been aware of FTK Imager's ability to just as easily image a VMware virtual machine into a forensic image as if it were a physical hard disk.

FTK Imager, through no more than "pointing and clicking", can open a VMware machine for preview or creating a forensic disk image of the VM.

In FTK Imager, through the selection of the following commands:

1. Create Disk Image
2. Select "Image File"
3. Browse to the "VMDK Virtual Drive" file

[17] www.forensics-intl.com

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

4. “Add” destination and image type (choose E01, DD, or SMART)

5. Choose destination folder and name the image

Another feature of FTK Imager well suited for virtual forensics is that of image conversion (or more accurately stated it is the creation of a new image from one format to another). Given an Encase or SMART image, FTK Imager can create a DD image, thereby negating the requirement of having to mount the image for booting into a virtual environment. This method of creating a new image would be based upon not having the software application to mount an Encase or SMART image as the time to create a new image would be longer than simply mounting the image directly.

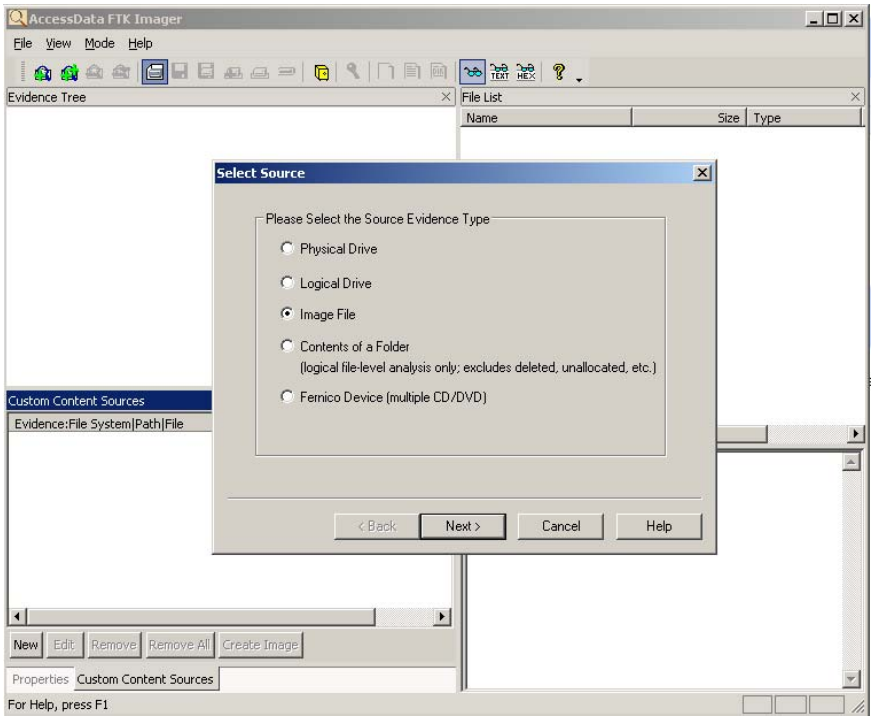


Figure 5 FTK Imager

Booting into a Virtual Forensic OS to Image

With the most common virtual applications, users can configure the boot order of the VM through the BIOS of the VM before having to boot into the VM operating system. As with a physical computer, a virtual machine be booted to a floppy or CD drive which can contain a forensic boot media (DOS or Linux as an example). In this pre-boot state, forensic imaging tools can be run within the forensic operating system which can create a forensic image of the VM onto external media.

The steps involved for creating a forensic image of a VM are the same as creating a forensic image of a hard drive of a suspect computer, ***only easier and faster***.

1. Prior to booting the VM, "Add" your external media/destination drive
    a. Depending upon the virtual application, this can be as simple as choosing "Add Device".
    b. Choose the device, which can be a physical external drive or a folder/partition on a drive.

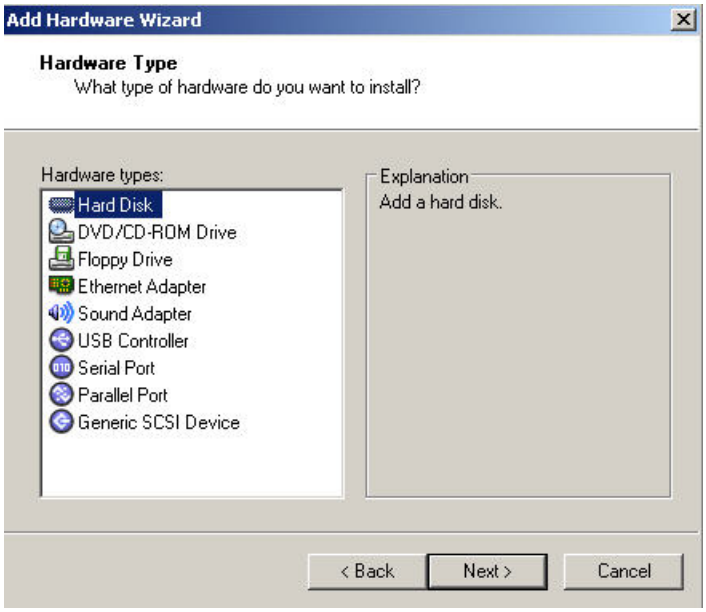


Figure 6 VMware Add Hardware Wizard

2. Add your forensic boot media

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

a. Depending upon the virtual application, a hardware device may be added. This can be either a floppy disk drive or a CD Rom drive.

b. With VMware, the floppy and CD Rom can be configured to boot to an ISO image. In this manner, a forensic boot floppy or CD can be made, configured to the VM, and used for booting into a forensic environment without having to use a physical floppy drive or CD Rom.

c. Configuring the floppy/CD to boot from an ISO image is a convenient and consistent method of booting to a forensic environment without having to have physical access to a floppy or CD drive.

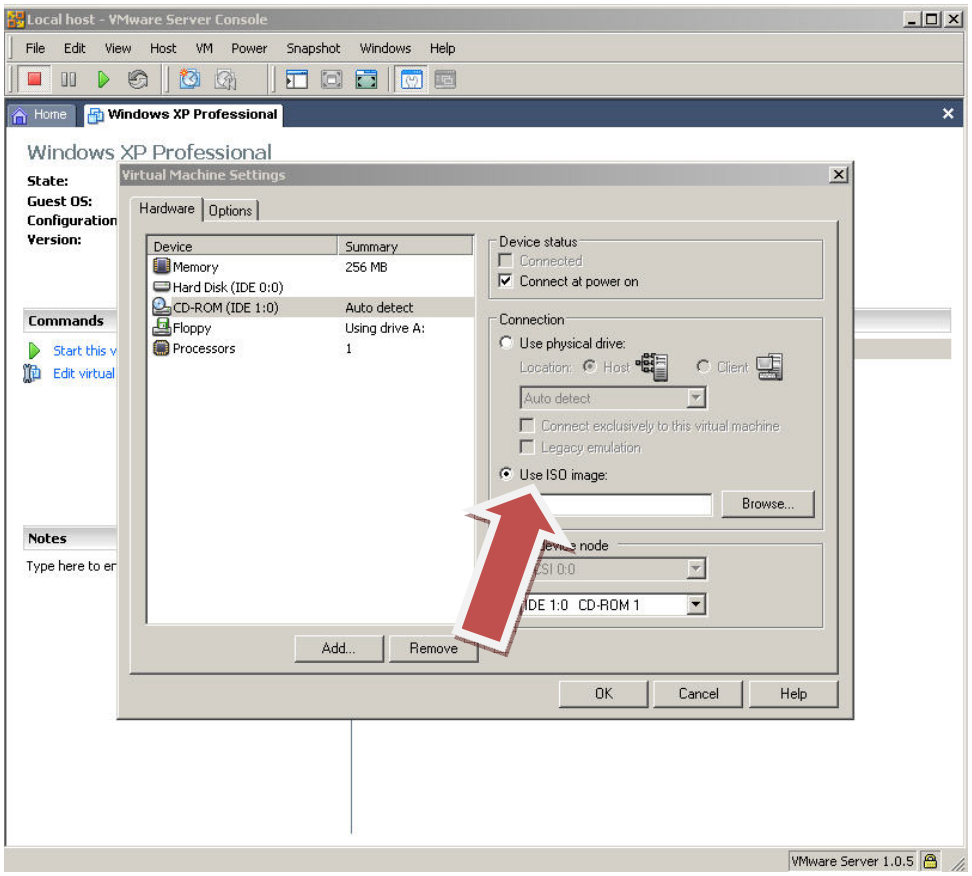


Figure 7 VMware Add Boot Media

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

3. Boot to the virtual machine's BIOS to change the boot order

a. Change the boot order to the forensic floppy/CD Rom instead of the virtual hard drive. Another method is to press the "ESC" key when booting. VMware will give a choice of media from which to boot for that session only.

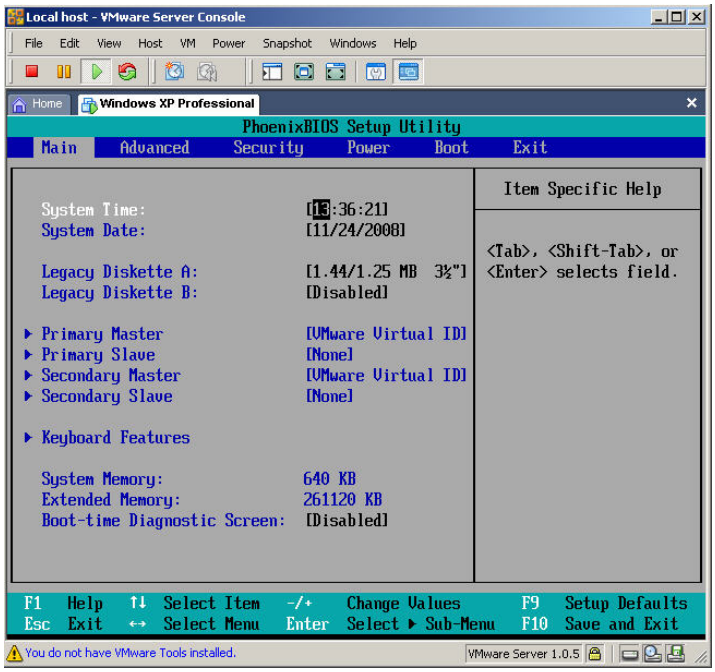


Figure 8 VM BIOS

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

4. Use the imaging program located on your boot media/ISO to create a forensic image to your external media

    a. Any forensic imaging application that will run in your forensic environment will now be able to create a forensic image of your virtual machine onto your external media. This can be DOS, Linux, or any OS configured to make no changes to the virtual machine. Booting to DOS or Linux through an ISO can be replicated across many virtual machines in an easy and quick process.

    b. The imaging speed will be slower than imaging through the host computer as the VM application will be sharing resources with the host.

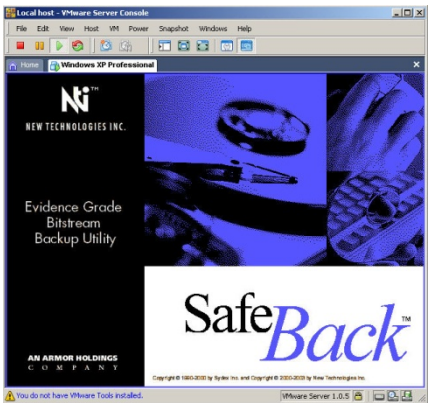


Figure 10 Safeback (www.forensics-intl.com)

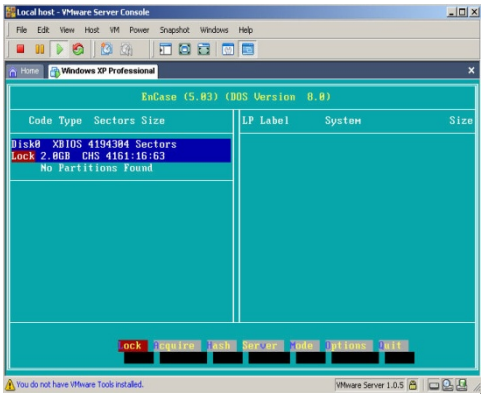


Figure 11 Encase (www.guidancesoftware.com)

Figure 9 Helix (www.e-fense.com)

Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

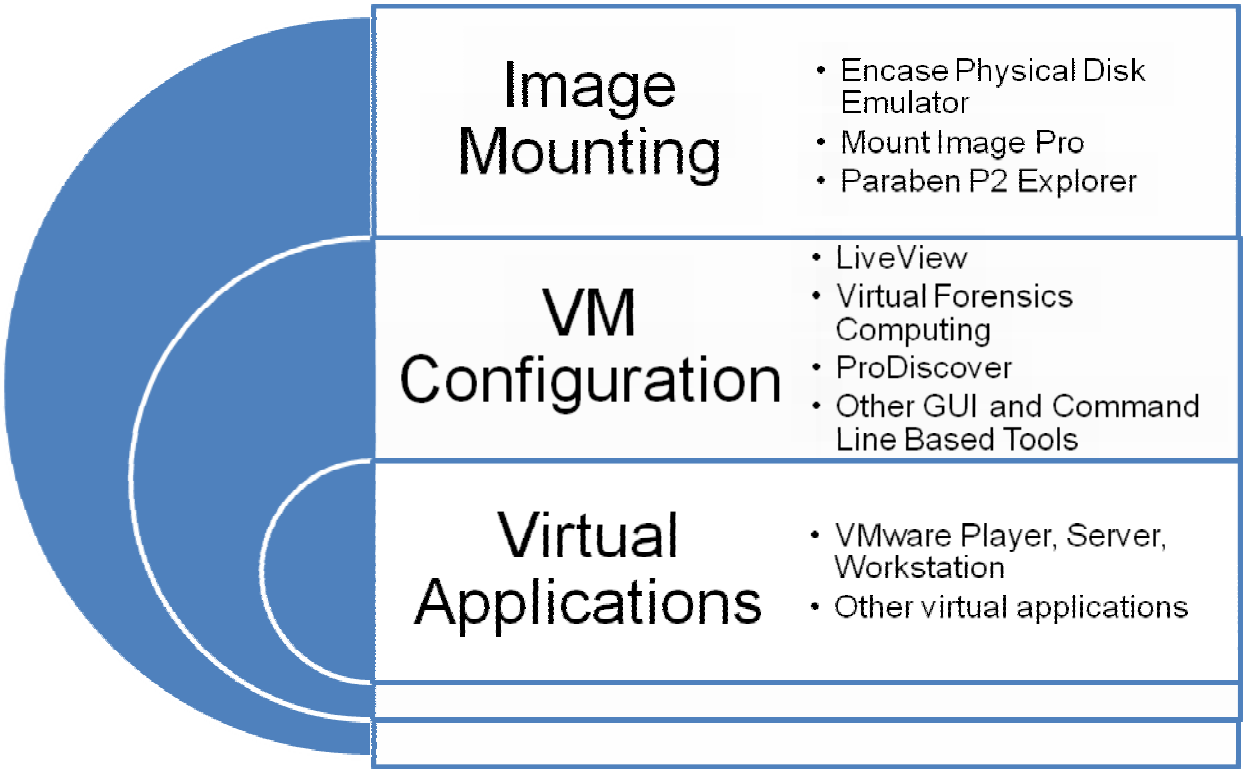
Summary

The time of virtual machines has come and will only become more commonplace. Although a virtual machine is nearly identical to an actual computer system, there are differences that need examiners should be aware. Given the capabilities that are inherent in booting forensic images into a virtual environment, this should be the first choice in the restoration of any forensic image as it not only saves time in the restoration process, but it can be repeated as many times as needed, quickly and easily.

One of the most glaring obvious benefits of the use of booting a forensic image to a virtual environment is that nearly every person in the industrial world has seen a computer screen with an operating system. Few have seen or want to ever see things like, “filepaths” or “lnk files”. Being able to show a courtroom or client the location of a specific file or folder by using a virtual machine will get the point across much faster and clearer. These are the moments where “**Eureka! Now I understand what you are telling me**!” are needed. Blank stares are disastrous in the courtroom, confusing to the client, and a failure for the examiner.

Software Application Listings:

Possessing the following set of tools will allow a forensic examiner to conduct nearly every investigative method mentioned in this paper. The creation of the initial forensic images can be made using commonly available commercial software and freeware or open source software.



Brett Shavers Virtual Forensics © 2008
bshavers@gmail.com

References

Using Linux VMware and SMART To Create a Virtual Computer to Recreate a Suspect's Computer
Senior Special Agent Ernest Baca United States Customs Service Office of Investigations Resident Agent in Charge
3010 North 2nd Street, Suite 201, Phoenix, Arizona
http://www.infosecwriters.com/text_resources/andrewrosen/SMARTForensics.pdf

Analysis of USB Flash Drives in a Virtual Environment
Derek Bem and Ewa Huebner
Small Scale Digital Forensics Journal, VOL. 1, NO. 1, JUNE 2007
http://www.ssddfj.org/papers/SSDDFJ_V1_1_Bem_Huebner.pdf

Computer Forensic Analysis in a Virtual Environment: University of Western Sydney
D. Bem and E. Huebner, University of Western Sydney, 2007.
http://www.utica.edu/academic/institutes/ecii/publications/articles/1C349F35-C73B-DB8A-926F9F46623A1842.pdf

VM Back
http://chitchat.at.infoseek.co.jp/vmware/vdk.html

VMware Utilities
http://petruska.stardock.net/Software/VMware.html

Penguin Sleuth Kit Virtual Computer Forensics and Security Platform
http://www.vmware.com/appliances/directory/249

Honeypotting with VMware Basics
Kurt Seifried
http://seifried.org/security/ids/20020107-honeypot-vmware-basics.html

Time Keeping in VMware Virtual Machines, 2008
http://www.vmware.com/pdf/vmware_timekeeping.pdf

Trademarks and Copyrights

VMware Workstation, Server, Player and **VMware** are registered trademarks of **VMware Inc.**
www.vmware.com

Encase is the registered trademark of **Guidance Software**, **Inc**.
www.guidancesoftware.com

FTK Imager is the registered trademark of **Accessdata**.
www.accessdata.com

ProDiscover is the registered trademark of **TechPathWays, Inc**
www.techpathways.com

Mount Image Pro is the registered trademark of **GetData Software Company**
http://www.mountimage.com/

Virtual Forensics Computer is the registered trademark of **GetData Software Company**
http://www.mountimage.com/

SafeBack is the registered trademark of **New Technologies Inc.**
http://www.forensics-intl.com

Helix is the registered trademark of **e-Fense**
http://www.e-fense.com

SmartMount is the registered trademark of **ASR Data**
http://www.asrdata.com

Windows and **Windows XP** are the registered trademarks of **Microsoft, Inc.**
www.microsoft.com