vmware™ as a forensic tool

Brett Shavers
May 2006

Brett Shavers
bshavers@gmail.com

VMWare Workstation™ is one of the most up and coming software applications in both the corporate environment and in the computer forensic community. This paper will not detail the inner workings of the VMWare Workstation, but will attempt to describe instances of where this application can be of invaluable use to computer forensic examiners. The application has an intuitive interface and an easy to understand user manual. Several software applications are discussed in this paper for image restores, however, **X-Ways Forensics™** was chosen for demonstration due to the ease of operation of the application as well as the detailed information the program provides regarding forensic examinations.

VMWare Workstation allows computer users to operate additional operating systems as '**virtual machines**' from within their '**host'** operating system, in effect, it's analogous to running a computer within a computer. The virtual machines can be nearly any operating system to include Windows, Linux, NetWare, or Solaris x86. The host operating system can be either Windows or Linux. The user can operate several of these virtual machines at one time and even have several virtual machines networked together. Where mentioned in this paper, the **host** system is the operating system on which your computer is running. The **guest** or **virtual machine/operating system** is that which is running under the VMWare application.

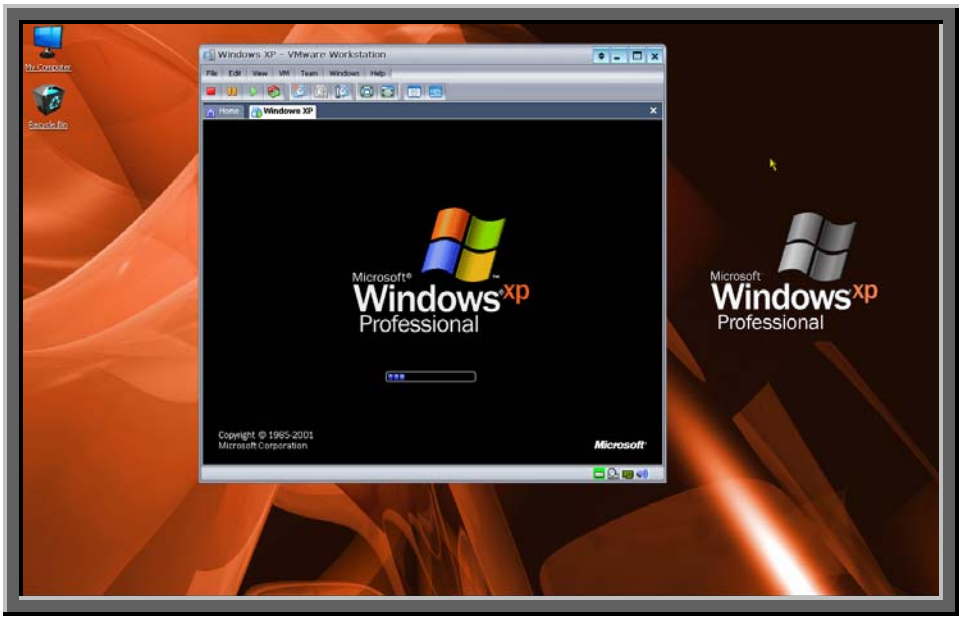

***Fig 1**: Windows XP Professional **Guest/Virtual Machine** operating within the VMWare Workstation which is running on the **host** Windows XP Professional operating system.*

Brett Shavers
bshavers@gmail.com

For convenience and perhaps necessity in some cases, an examiner running a virtual machine can **conduct an entire examination of a digital evidence image within a virtual machine**. Some of the benefits of using a virtual machine for conducting examinations include the storage of the virtual machine as part of the overall evidence. By having the examination virtual machine stored with the original evidence, it would be an easy task to keep a physical record of what operating system was used to include the updates and hotfixes, as well as the version of any forensic software used on the examination as well. By conducting examinations in the virtual machine, a cluttered hard drive on the host machine can be avoided. Some problems that may be encountered is the amount of RAM that is used, as since there is the host operating system and the virtual machine operating system running at the same time, the RAM is shared. Another nuance that may occur is the recognition of attached software application dongles and attached media. However, these are easily overcome and handled as they appear. The virtual machines seem to run best when set at full screen when conducting forensic examinations.

One of the most basic and important rules in digital forensic examinations is '**do no harm**', in that the original evidence should not be altered. However, there are instances where the suspect hard drive may need to be examined in its native operating state. This paper does not advocate altering any original evidence, but rather, suggests that restored images of suspect drives be used to visually exam the suspect system. By using a restored image of the suspect drive, the examiner does not need to risk altering the data on the original.

An example where the suspect hard drive may need to be restored and viewed in a virtual machine is where data exists on the suspect system that cannot be viewed without the **proprietary software** that is on the suspect system. It is not common, but does occur, that individuals or businesses create programs for specific purposes and that these programs are not commercially available. Should the programmer be the suspect, gaining cooperation may not be possible. By restoring the suspect hard drive, the examiner will be able to use the suspect's unique software to view data created by that unique software which is considered evidence. There are also instances where specific versions of outdated software may be required to view evidence files as well. Depending up the popularity of that software, it may or may not be available anymore. A working, restored suspect drive allows for these items of evidence to be seen in the exact version of software that they may have been created in by the suspect(s).

Of all aspects of computer forensic investigations, **the most important is conveying the findings of the examination** to those groups of persons that need to understand it. No matter how well an examination was conducted and no matter the training and experience of the examiner, if the results of the examination are not clearly and simply explained, the work may be all for naught. Prosecutors, defense attorneys, judges, jurors, supervisors, and clients need to be able to understand what was on the suspect evidence, how it got there, and

what it looks like. Spreadsheets with names, dates, and times are not easy to explain, especially if there are hundreds of items listed. Check sums, unallocated space, encrypted files, and other 'intangibles' may only confuse those that need to understand the most.

Attempting to describe how the suspect used their computer or how the suspect set up the computer to the average computer user is not an easy task. However, by **viewing the suspect operating system in its native environment**, it is a simple demonstration to 'point and click' through that system, showing those important aspects of the findings, opinions, and conclusions of the forensic examination. Nearly every adult (and teenager) on the planet has seen at least one version of Windows. Most persons probably have one version of the Windows operating system on their home, school, or work computers, and by showing the suspect's running operating system, the task of explaining has been made much simpler as they now have something that can be seen for comparison to what they already know.

In a networked computer system, in which the suspect computer had access to other computers in the workplace or in a residence, VMWare can be used to **replicate a network using multiple virtual machines**. By replicating the network in VMWare, the access rights to files and other computers on the suspect operating system can easily be seen and described. VMWare allows for 'snapshots' to be taken of the virtual machines at any point by the user. These snapshots allow for the virtual machine to be started (booted) at the same point as many times as needed. This is an excellent benefit to the investigator/examiner as the virtual machine can be tested for alleged Trojans/viruses to help prove or disprove the allegations.

Having digital evidence files in hand, whether they are dd images, Encase images, or a cloned suspect hard drive, **each item of digital evidence can be restored into virtual machines** for further examination. A major problem of restoring the Windows XP operating system occurs during the booting of the restored virtual machine. As there will be numerous hardware changes to the restored suspect virtual machine, the examiner will need to repair the Windows installation using techniques of basic service repair. These steps of repair are documented in many A+ study guides and through various internet websites. During a repair install, the system files will be replaced, however, the evidence files, i.e. those individual files created by the suspect, will remain unchanged and can be verified with checksums. Risks remain that the suspect may have set the boot process with self destruct programs that may wipe evidence from the virtual machine; however, the original evidence is still untouched in the original images.

The simplest of restores into a virtual machine is using the **cloned suspect hard drive**. If the clone resides on a hard drive, then by physically connecting the suspect hard drive to the examination machine, VMWare can be configured to boot that clone into a virtual machine. The act of **removing a hard drive through VMWare does not delete that hard drive;** it only removes it from that particular virtual machine.

Therefore, a hard drive naming procedure should be developed by the examiner to keep track of the numerous hard drives created, added, and removed in the restoration process.

The steps to add a physical disk with VMWare are;

(1) Edit virtual machine settings,

(2) Add hard disk,

(3) Use a physical disk as seen below.

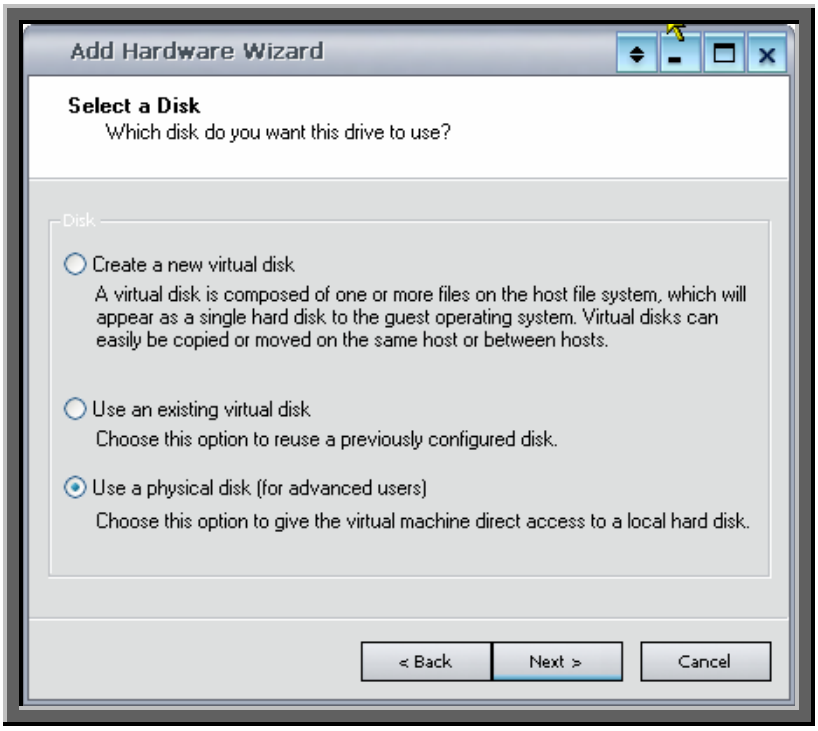

Fig 2: *Adding a hard disk using a* ***physical disk*** *in VMWare Workstation*

The virtual machine, when started, will boot to the attached physical disk. The restoration of image files requires a bit more in depth explanation than simply connecting a cloned physical disk. **Several different programs can be used to restore images into a virtual machine**. The steps outlined below were chosen for restoration processes primarily for the simplicity and time saving factor of using specific software applications. Although there exists other methods, time is usually (if not always) a factor in forensic examinations due to cost and deadlines.

Some of these programs include; ***X-Ways' Forensics, Guidance Software's Encase,*** and ***ILook IXimager***. The procedure for using Encase and X-Ways Forensics are similar, however, for this example, X-Ways Forensics will be demonstrated. ILook IXimager and other bootable media are in themselves similar to each other as well. ILook's IXimager is a law enforcement restricted software, but in function, there are several other Linux based bootable CD's that offer the ability to restore images available to non-law enforcement.

The differences lie in that with Windows based software, the restoration must take place in an operating virtual machine. With a DOS or Linux based bootable software, the restoration takes place after booting into Linux/DOS from a boot CD or floppy disk. In concept, with any of the software applications used, the process is basically the reverse of making an image of a suspect hard drive. Image restores can be completed using several different methods, some more manual than others, some utilizing specific software designed to restore into virtual machines, however, this topic in this paper will detail two selected methods.

Starting a **restoration by using a bootable Linux CD or bootable DOS floppy** will be the easiest to describe in that there are fewer steps than using a Windows based application. Using a physical hard disk that contains the image of a suspect hard drive will be the sample in this explanation. The process includes;

(1) Set up the virtual machine without networking;

a. Do not install any operating system as this machine will not be needed to be bootable
b. Do create a virtual hard disk that will be used for the bootable media.

(2) Add the physical hard drive that contains the suspect image;

a. Edit Virtual Machine Settings
b. Add Hard Disk
c. Use a Physical Disk
d. Select Device (choose the hard disk that contains the suspect image)

(3) Create a virtual drive (this virtual drive will be the 'target' of the restoration);

a. Edit Virtual Machine Settings
b. Add Hard Disk
c. Create a New Virtual Disk
d. Choose disk size (same or at most, a little larger than the suspect hard drive)
e. To keep track of virtual and physical drives, name the target drive to something other than the default.

(4) Boot using a bootable Linux CD or DOS floppy (change the VMWare settings to boot to the CD/floppy);

(5) Restore the image from the physical hard disk into the target virtual drive;

a. Boot into the Linux/DOS software of your choice
b. Typically, the programs offer an option to **restore image**, if not, then that application will not be able to work in this fashion for a restore.
c. Choose the source of image (which should be residing on the attached and added physical hard drive)
d. Restore the source to the virtual target drive that was created and renamed.

(6) Shutdown the virtual machine;

(7) Remove the physical hard disk that contains the image from VMWare;

a. This removal of the physical hard disk is done through the VMWare application,

b. Edit Virtual Machine Settings – Remove Hard Disk

(8) Boot to the restored suspect virtual machine.

A **restoration using Windows based software** requires additional steps. This is due to the tools requiring a running Windows operating system to function. The process includes;

(1) Set up the virtual machine without networking to include a Windows operating system; This operating system must contain the restoration software (Encase, Winhex, etc…),

(2) Add the physical hard drive that contains the suspect image;

(3) Create a 'target' virtual drive;

(4) Boot to the Windows operating system virtual machine that contains the forensic software;

(5) Use the Windows based forensic software to restore the image from the physical hard drive onto the target virtual drive; (example; Choose "**Restore Drive**" in Encase and follow directions to restore the suspect evidence file to the target virtual drive); The following screen shots are taken by using X-Ways Forensics as an example:

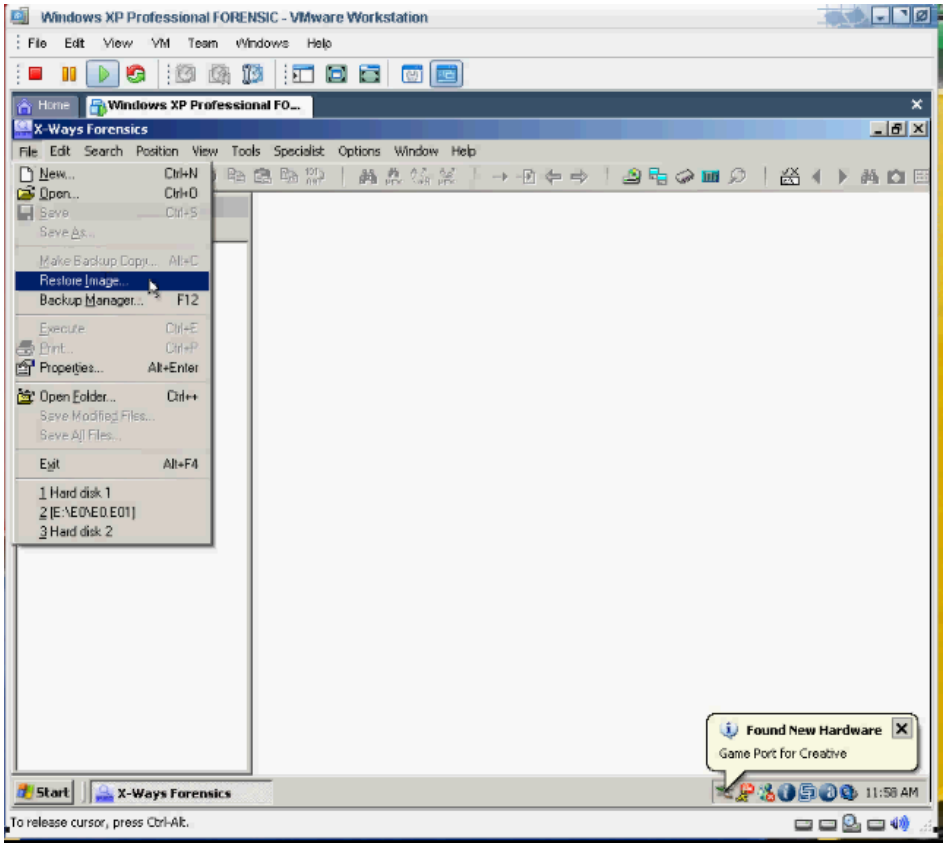

Fig 3: Using X-Ways Forensics, choose **File-Restore Image** to begin the restoration

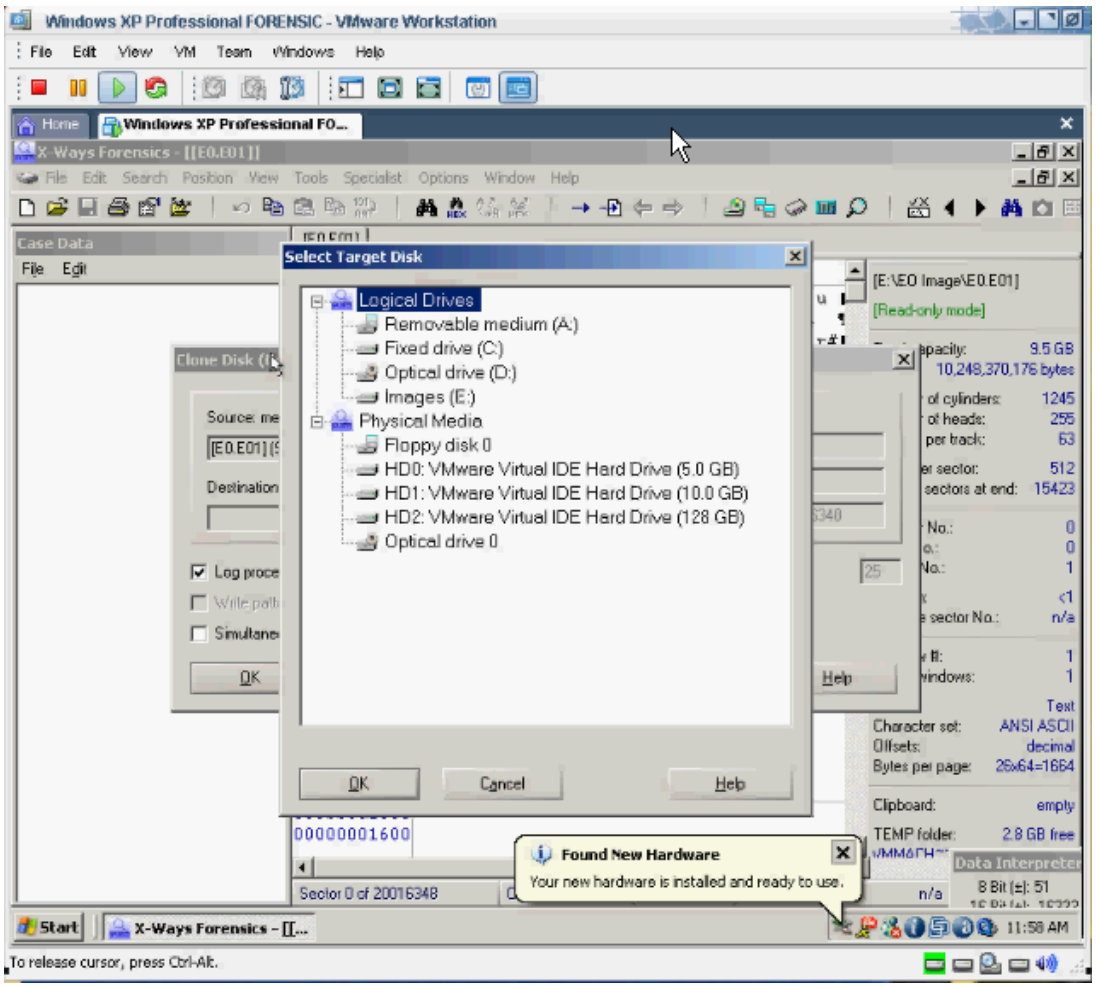

Fig 4: After selecting the image, select the target Physical Media. With this method, you should see 3 virtual drives (**one** for the Windows operating system you are running, the **second** for the virtual drive that will be used to restore the image to, and finally, a **third** virtual drive that contains the image(s). In the above screen shot, the 5GB is our running virtual system, the 10GB is the empty target for restoration, and the 128GB is the physical drive containing the image to be restored.

(6) Shutdown the virtual machine;

(7) Remove the physical hard disk and the virtual machine containing the forensic software from VMWare;

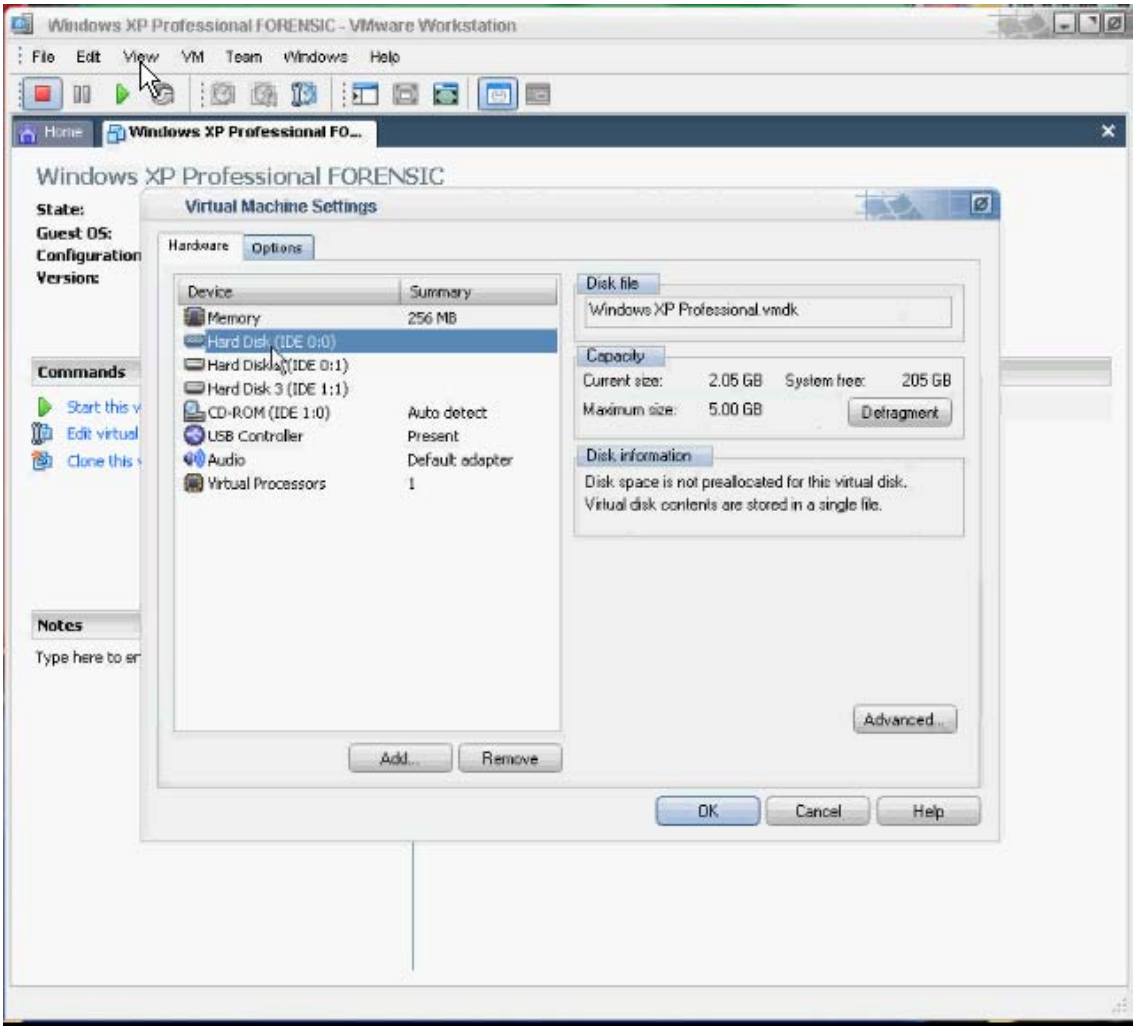

Fig 5: **A**gain in this case, there are three hard disks (virtual drives), two of which will be removed. The Windows virtual drive containing the software (IDE 0:0) and the physical disk (IDE 1:1). The remaining virtual drive will be the drive used as the target of the restoration. It may be necessary to change the remaining virtual drive to IDE 0:0 to make it the primary master (bootable) using the **Advanced** tab.

(9) Boot to the restored suspect virtual machine.

As with any **restoration process**, there may be several nuances that occur which must be dealt with on a case by case basis. With the same principle, dd images can be restored into a virtual machine, with the listed steps in this paper. Problems upon booting are handled as with any basic trouble shooting methods, to include repair CD's and operating system installation CD's, which goes beyond the scope of this paper. An important point to remember is that if an installation repair is done on the restored image, **only the system files are being changed**, not the evidence files (graphics, email, etc…) during the repair. Obviously, once restored, a checksum of the restored image will not match against the original image. This is not an issue in regards to individual evidence files as the original evidence will remain unchanged and can be checked against any restored image files.

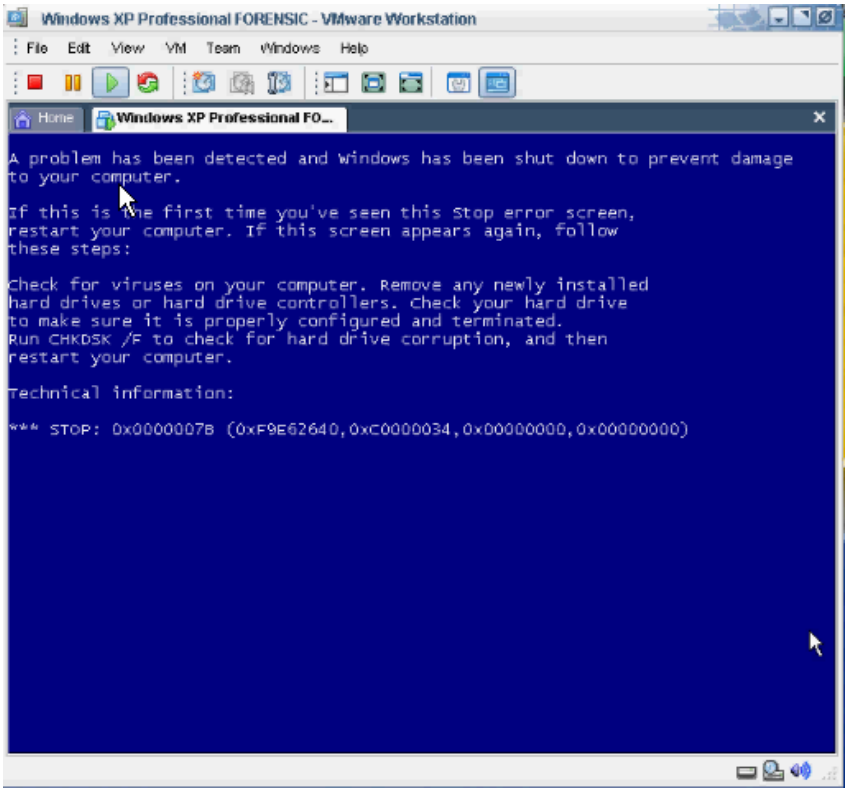

Fig 6: The blue screen is dealt with as any blue screen, using recovery CD's or a repair installation of Windows.

Typically, restoring images of hard disks are not undertaken as there is not a strong need for it in every investigation. The time required to complete the restore can be very expensive depending upon the size of the image and other factors, such as large RAID setups or perhaps imaged networks. However, when it is necessary, the visual impact of observing how the running suspect operating system behaves can be the pivotal decision maker in a criminal or civil proceeding. The primary goal of restoring suspect images into a virtual machine is to be able to boot into the operating system in order to visually inspect, instruct, or explain that particular system and setup as the suspect saw it. A picture may be worth a thousand words, but an operating system that is fully functional, that visually shows individual folders created by the suspect, and that clearly contain the suspected evidential data, well, that may be worth a lot more than a thousand words.

Trademarks and Copyrights:

VMWare Workstation and **VMWare** are registered trademarks of **VMWare Inc.**
www.vmware.com

WinHex and **Replica** are registered trademarks of **X-Ways**, **Inc**.
www.x-ways.net

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

ILook and **IXimager** are registered trademarks of the IRS Criminal Investigation Electronic Crimes Program and Elliot Spencer.
http://www.ilook-forensics.org/homepage.html

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

A+ is a registered trademark of **CompTia**
www.comptia.org