

# **Methodologies for the use of VMware to boot cloned/mounted subject hard disk images**

Michael A. Penhallurick  
RMCS Forensic Computing MSc  
2002-2005  
Cranfield University

Network Investigator / Computer Forensic Analyst  
South Yorkshire Police  
Computer Forensics Unit

March 2005

Reproduced and distributed under licence and  
with permission of Cranfield University

## **Acknowledgements**

The author would like to express thanks to the following people who assisted in the proofing, testing and live demonstrations of the methods described above: -

### **South Yorkshire Police**

Andrew Smith  
David Swirles

### **The Centre for Forensic Computing**

Professor Tony Sammes  
Lindsey Gillies  
Helen Harmer

### **Customs and Excise**

The Hi-Tech Crime Team, especially  
Paul Birch  
Deepa Cole

**This area intentionally left blank**

## Abstract

This paper represents part of the work that was submitted for the RMCS Shrivenham / Cranfield University MSc in Forensic Computing in March 2005.

An investigation into the restoration of forensically acquired digital data to virtual hardware was undertaken. The objective of the investigation was to devise a methodology by which a subject operating system could be booted in a virtual environment. This would enable the investigator to experience the subject system in a controlled environment where file system changes could be discarded and the 'original' clone preserved for future, repeatable usage.

During the research and experimentation stages of this project, the following software was utilised: -

- Encase 3.22g was the primary forensic imaging tool.
- Mount Image Pro 1.05 was used to mount the forensic image files as a physical disk.
- Symantec Ghost 2003 was used to clone the physical disk to a new virtual disk.
- VMware 4.5.2 build-8848 was the virtual machine software used.  
*The underlying architecture of VMware is Intel based.*
- Microsoft Windows XP was used as the host examination system.  
*During the research phase of this project, the host examination machines utilised both Intel and VIA (AMD processor) architectures.*

It is anticipated that the reader will have some awareness and understanding of the use and functionality of the above applications. All trademarks and trade names of all software utilised are acknowledged. The systems researched and activated using the methods described below encompass Windows 95/98/ME & Windows NT/2000/XP.

The methods employed were found to be successful for Intel-to-Intel restorations. Anomalies were discovered when restoring Windows 2000/XP systems originally hosted on non-Intel architectures (i.e. VIA). Other anomalies were discovered when restoring Windows 95 systems onto fast AMD processors (>350MHz) and when installing the drivers for detected hardware on some Windows 98 systems. Discussion and resolution of these anomalies is covered in further detail below.

## Introduction

Forensic computing, albeit still a relatively new field of science, encompasses the retrieval and analysis of digital evidence. This retrieval is undertaken using accepted and proven concepts of digital image acquisition. Subsequent to acquisition, a number of 'forensic' tools can be used in order to reach conclusions based upon the facts of the examined (and sometimes recovered) data.

There are a great number of tools available to assist in the analysis of digital media, a list of which is beyond the scope of this paper. Whilst such tools provide a great depth of analysis, it is possible that the 'scene of crime' part of the examination process is often overlooked as an additional source of information. The actual environment that a user would experience whilst using the subject operating system(s) often remains unvisited during an examination and may provide valuable insight to the case.

The ACPO Good Practice Guide for Computer Based Evidence<sup>1</sup> defines four principles in relation to digital evidence examination (Figure 1 below). These principles underlie the methods used in forensic computer examinations and dictate the necessity of forensic imaging and any subsequent restoration.

When considering activating a suspect operating system, or in any other way directly accessing the data therein, it must be accepted that data *will* change on the drive. In dealing with restored/cloned subject data that has been 'laid out' and activated, the focus of investigation consequently needs to shift to Principle 3 of the ACPO Good Practice Guide. This addresses the ability to replicate boot processes, potentially multiple times, and consistently achieve the same results.

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Figure 1 - ACPO Guidelines for Computer Based Evidence

## Contents

This paper begins with an overview of the requirements and purpose of booting a restored machine. It continues with a discussion of the traditional method of physical restoration of data from a subject hard drive to 'new' forensically clean media and follows on with the restoration being directed to a virtual machine environment. Consideration is given to the inclusion of networking capabilities on restored systems and precautions to be taken when networking is required.

The importance and relevance of virtual machine snapshots is explored, along with detail in relation to the use of virtual disk drivers to gain read/write access to restored virtual disks.

Method 1 details direct access booting a virtual machine from either write-blocked subject media or mounted forensic images.

Method 2 describes processes that can be utilised to clone out the subject drive and make relevant modifications when direct booting using Method 1 fails.

A discussion follows on issues that have been encountered with restored Windows systems. These are the Win95 Fast Processor Issue; Win98 'Lost' CD-ROM Issue and the Win2k/XP Blue Screen Issue. In determining the resolution for the latter of these issues, a methodology for offline registry modification of a virtual system is explained, along with the potential of password extraction from a restored system. The initial Win9x issues are also explored and methods of resolution described. The paper concludes with details of a possible hardware solution and recommendations for future work.

## Rationale

The purpose of this paper is to discuss methods by which subject data can be examined in a virtual environment as if the original system were being used. Using this approach, an investigator can experience the system much as an original user would have. Benefits of employing these methods include time-efficient data restoration, repeatability of analysis and the potential of easier access to the passwords of the more secure Win2k and WinXP operating environments.

Due to the repeatable nature of the methods discussed, it is also possible to 'virtually' transport a restored system into almost any setting, such as a Court. Consequently, live demonstrations can be given of installed applications or other data that may be relevant to an investigation. Transportation can be undertaken on any machine capable of running the Virtual Machine software and with sufficient local storage to hold the restored system(s).

### **Booting Restored Systems**

In order to experience and understand the operating environment of any particular system, and indeed to analyse applications and data that have been installed and used therein, it is beneficial to restore the data from the original hard disk(s) or forensic image(s) and to then boot the system from the resultant 'clone'.

To achieve successful activation of a restored system, the 'live file' data is normally all that is required. This includes files present within the Recycle Bin/Recycler, any System Restore points (where applicable) and hidden/system files. Generally, it will be possible to disregard data that resides in the unallocated/user inaccessible areas of the disk. There may be instances when regard *must* be given to data that resides in such areas of the disk, however it is anticipated that this will be the exception rather than the rule. An example of when access to the unallocated/user inaccessible areas would be required, as opposed to simply accessing the 'live file' data alone, would be the investigation of a suspicious application that utilises 'hidden' data. Given the ability to secrete data in boot sectors or otherwise unused/user inaccessible disk areas, it would then be necessary to undertake a full sector-by-sector restore of the subject drive to ensure that *all* relevant data areas are available in the cloned system. Only in this way will it be possible to observe the behaviour of an application that utilises data resident in these areas.

A number of different methods have been researched, from a straightforward 'live file' copy through to a full forensic sector-by-sector restore. Detailed below are two methods that have successfully been used to clone out and repeatedly activate subject operating systems.

### **Physical Restoration**

The traditional method employed in order to facilitate booting the original machine is to restore a subject hard drive to a new forensically clean hard disk. This process can be time consuming and may require some degree of repetition in order to boot more than once from the same forensically restored image. If multiple disks are involved, the restoration process will take even longer.

Physical restoration of digital data requires the use of a hard disk drive of at least the same or greater capacity as the original media. There may be occasions when locating a suitably sized physical hard drive is in itself problematic. Hard disk drive sizes are continuously increasing and as time progresses it will become more difficult to obtain smaller hard drives. If the difference in capacity of the 'new' drive to the subject media is too great, drive translation issues *may* affect the restored image. The ideal is to restore the relevant data to a drive with exactly the same number of sectors. This in itself may cause restoration issues dependent upon the underlying operating system of the examination machine. Specifically, when restoring a forensic image to a target drive with exactly the same number of sectors as the original subject drive, it was found that disk access issues precluded the use of forensic restoration tools in a Win2K/XP environment. The restoration process has subsequently had to be undertaken within the older Win98 environment or with an alternative operating system such as Linux.

## Virtual Restoration

With the advent of virtual machine software, entire systems that run in a purely emulated environment can be produced. VMware<sup>4</sup> and Microsoft VirtualPC<sup>5</sup> are two such products. Virtual hard disk drives can be created and accessed as though they were actual physical devices connected to either the host machine or the virtual machine. The user of the host system wholly controls the size and mode of access to these virtual drives. Virtual hard disk size is limited only by the amount of space available on the host system.

It is possible to undertake the activation and examination of forensically acquired data in an entirely emulated environment using VMware virtual machine software. With any restored systems, the internal clock (of the virtual machine) should be set to the date/time of seizure. This will ensure that time limited software is not adversely affected, particularly if some considerable time has elapsed between seizure and examination.

## Networking Capabilities

In the vast majority of emulations, networking should *not* be added. Not only will this ensure that the host (examination) machine remains isolated from the guest (subject) machine, it will mean minimal changes to any network settings already present in the subject system.

If the systems being emulated are part of a network, or if network activity requires closer examination, then networking capabilities *can* be added to the virtual machine. Additional steps, such as a local firewall on the host machine and regularly updated antivirus software, should be installed on the host system to ensure continued isolation between the host and any activated subject system(s).

## Image Mounting Tools

As of November 2004, there are two primary tools available, the Encase Physical Drive Emulator (PDE)<sup>2</sup> and GetData's Mount Image Pro (MIP)<sup>3</sup>, which both enable the 'mounting' of Encase and Linux dd images in a Windows environment. Dependent on which tool is used, additional forensic image formats or virtual file systems such as VMware can also be mounted. The mounted disk is subsequently available to the host system as either a physical drive or a series of logical drives.

The Physical Drive Emulator (PDE) has been available as a module to Encase since Version 4.18 (March 2004). This module enables an investigator to mount an acquired image and parse this into VMware. Once added to a virtual machine, the subject operating system can be booted and examined, as a user of the original hardware/system would have seen it.

The Encase PDE is currently only able to emulate a single drive at any one time. This could prove to be a severe drawback should it be necessary to examine a system comprising more than one drive or with multiple RAID sets.

Full documentation relating to the Encase PDE is only available to registered users of Encase and can be found at the Guidance Software website<sup>2</sup>.

The second tool to perform the same function is GetData's Mount Image Pro (MIP). With MIP, the underlying forensic software is not required and multiple image files can be mounted simultaneously. The number of available drive letters on a system dictates the number of drives that can be mounted at one time. This could be up to 23 additional drives on the host machine, albeit for the vast majority of investigations it is unlikely that any more than 2 or 3 drives will be required.

## Virtual Disks and VMware Snapshots

When dealing with virtual machinery the perception of hardware changes from the tangible to the emulated. When considering storage devices, virtual disks simply become a series of files as opposed to a *physical* disk of fixed capacity.

The size of a VMware virtual disk is limited primarily by the amount of storage available on the host system. These virtual disks are stored by default as a series of 2GB files but can also be stored as a single large file. The option exists to allocate all virtual disk space immediately, which will naturally require considerable host disk space for larger drives but may improve overall performance. Alternatively, the default option is to allocate disk space only as required. This creates the same number of files but only uses the host machine disk space as and when data is added to the virtual disk.

VMware Workstation 4 introduced the ability to take a snapshot of a system at a specific time. This facility enables the investigator to return the system to an earlier state, a feature similar to the System Restore function within Windows XP.

The process of taking a snapshot in VMware will cause the creation of a series of REDO virtual disk files. VMware uses these to monitor and apply changes to the underlying virtual disk that is in use. The REDO files are generated when the machine is first started after a snapshot has been taken. Mounting and modifying via the REDO files will leave the original cloned image unaltered.

When a snapshot is taken of an installed guest operating system, (in these circumstances, a cloned subject hard drive is the guest OS), any subsequent disk interactions are intercepted and stored in these REDO files. These changes are only merged into the original system when a subsequent snapshot is taken which supersedes the existing one. At the point of this new snapshot, the contents of the REDO files are permanently merged with the original disk contents. Until this latter snapshot is taken, the integrity of the original cloned (or restored) disk is maintained and the REDO files can simply be discarded by using the 'revert to snapshot' option.

If booting a mounted/cloned disk image results in an INACCESSIBLE\_BOOT\_DEVICE error, it should be possible to start the machine by employing the steps detailed in Method 2 below.

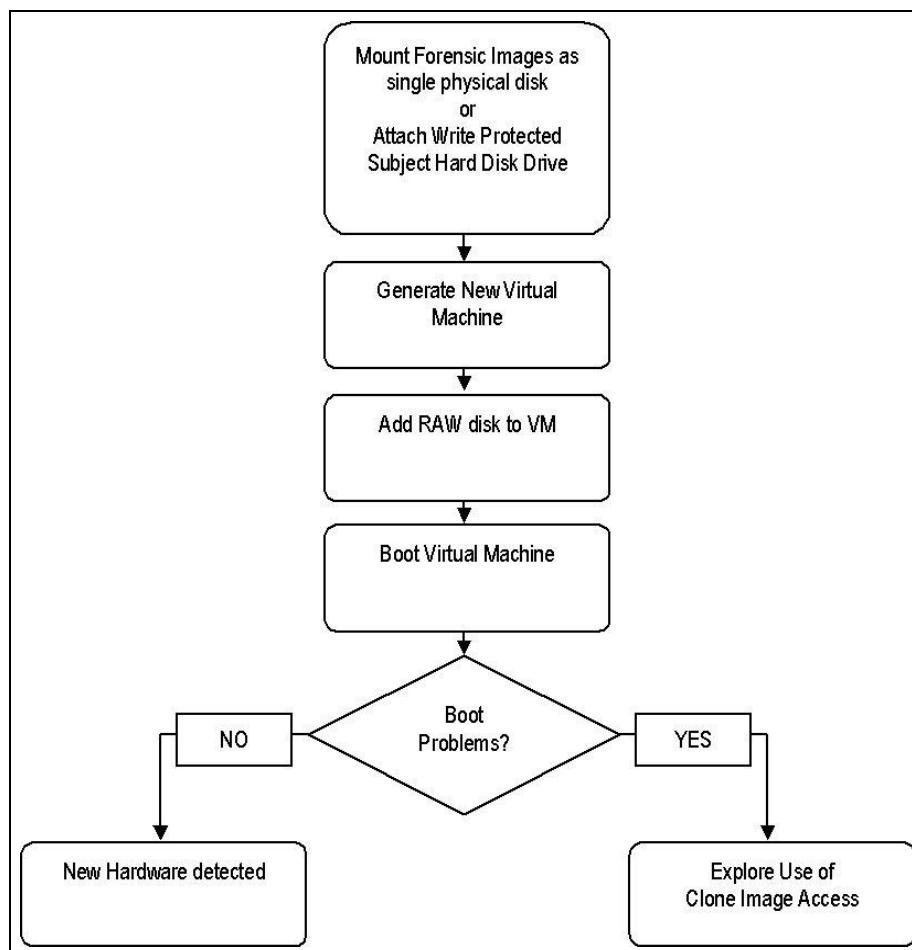
*NB Experimentation using Mount Image Pro and REDO files indicates that this method will only work if the mounted image is ghosted/cloned to a virtual disk drive and hence has full read/write access. Attempts at modifying read-only MIP mounted raw disks with read/write access via REDO files failed to produce the anticipated results and actually caused the host system to reboot.*

## Boot Methodologies

In all subsequent tests, Mount Image Pro was used to mount the forensically acquired images as emulated physical disks. During the research stage of this paper, Encase PDE was unavailable to the author although it is anticipated that use of this product will yield similar results. The host operating system used was Windows XP and the virtual machine software was VMware workstation 4.5.2 build-8848. The restored systems originated from image files acquired from single disk installations.

## Method 1 - Directly using a mounted image

The flowchart below (Figure 2) illustrates the processes involved in activating a system through a virtual machine. This method has been found to be successful for Win9x/NT systems and Intel based Win2k/XP systems.



**Figure 2 - Virtual Boot Process Using Direct Image Access**

Either a write-blocked disk or the acquired image files can be used as a raw (physical) disk source for the virtual machine. In either case, the drive, whether physical and write-blocked through hardware, or mounted and write-blocked through software, must be available to the host system *before* the virtual machine software is started. If this is not done, then the virtual machine software will not detect the availability of the drive(s) and will need to be re-started in order to detect the presence of the new 'hardware'.

The individual steps required to boot a machine with direct image access are detailed in Figure 3.

## Method 1

*This method has been used to successfully boot pre-Win2k systems and Win2k/XP systems originally installed on Intel architectures.*

1. Mount the image as a single physical disk  
Use Mount Image Pro, Encase PDE or direct physical disk access via a write-blocking hardware device to enable the host system to recognise the subject disk.
2. Start VMware
3. Create a new custom Virtual Machine that corresponds to the operating system under investigation
4. Add the mounted disk image as a (raw) physical disk  
The mounted disk will be the last physical drive available to VMware
5. Do **not** add any networking capability  
If networking is required, ensure adequate measures are in place on the host system to retain isolation between host and subject.
6. Take a **snapshot** of the system
7. Boot the new Virtual Machine  
Consideration should be given at this point to ensure that the virtual machine date/time is set back to the date of seizure using the virtual BIOS of the virtual machine.
8. Disregard warnings relating to SCSI devices  
Using MIP, the mounted disk will appear to the virtual machine as a SCSI device. With some operating systems, VMware will alert the investigator that this may cause problems. During testing, these warnings have been ignored with no apparent adverse effect on the resultant system.
9. New hardware will be detected  
With Win9x/NT/2k systems, it has been found that new hardware will be detected *before* the user login screen appears. With WinXP systems, it has been found that new hardware is detected *after* a user has logged in.
10. VMtools can be installed to facilitate adjustment of screen resolution  
VMtools includes an SVGA driver that is required to facilitate screen resolutions greater than 640x480 with 256 colours. This driver is required in order to accurately adjust screen settings to that of the original system. When VMtools is installed, it is important to ensure that time synchronisation between the host and subject is *not* enabled.

**Figure 3 - Details of Virtual Boot Process Using Direct Image Access**

The steps detailed in Method 1 provide a straightforward process that enables booting and accessing a subject operating system with relatively minimal effort. There will however be occasions when this procedure does not immediately work; most notably this has been encountered with blue screen failures on Win2k/XP systems and workarounds have been required to successfully boot Win9x systems.

With Win2k/XP systems that have originally been hosted on non-Intel architectures, it is necessary to modify the registry of the subject system and add a disk driver file. With Win98 systems, it may be necessary to boot from a floppy disk that the investigator has crafted to force inclusion of a CD-ROM driver. With Win95 systems on fast processors, it may be necessary to install a patch before the system will boot properly. These issues are described in further detail below.

## Method 2 - Using a cloned image with modification as required

When Method 1 results in boot failure, it may necessary to clone out the original media, whether actual write-blocked drive or mounted image files. The cloning process can be undertaken using Ghost or a similar utility. An overview of the process involved is shown in Figure 4 below, with further detail described in Figure 6.

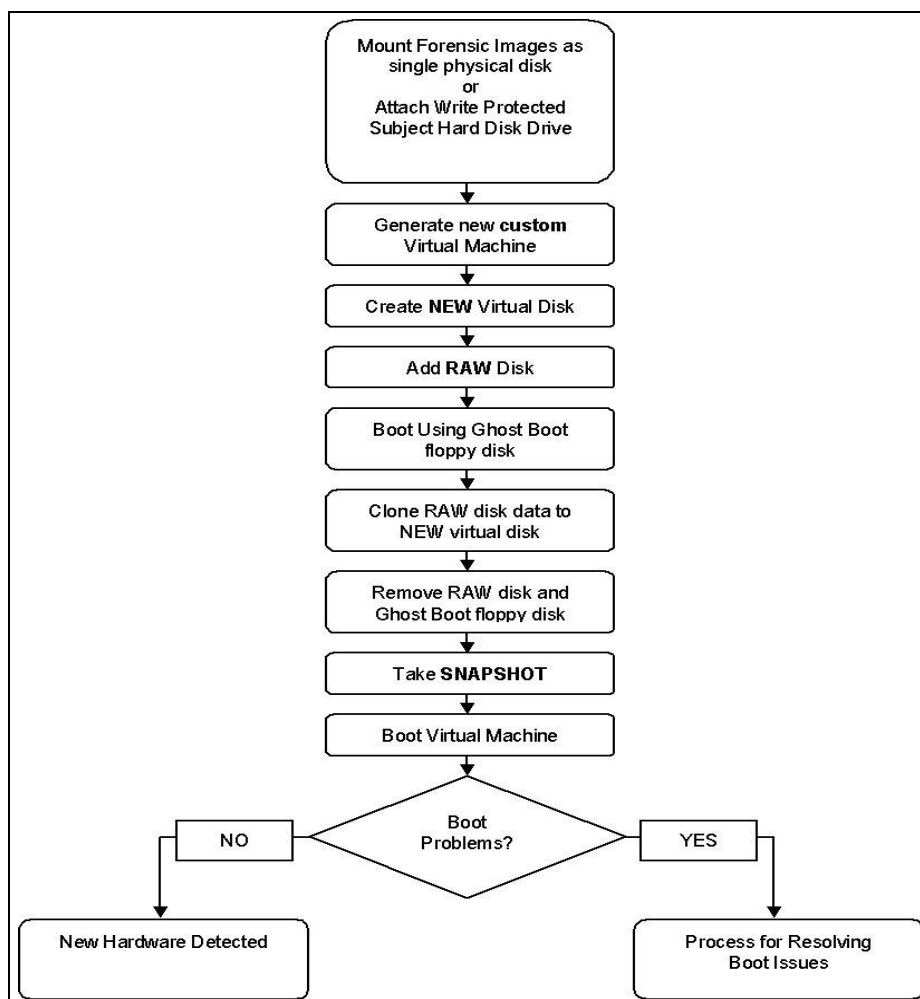


Figure 4 - Cloned Image Access

## Cloning with Ghost 2003

The default copy mode for Ghost will clone out the 'live file' data in each partition as described above. With the use of the command line switches '-IA' or '-ID', a sector-by-sector forensic restore can be undertaken, ensuring that, where applicable and necessary, *all* disk data is copied including that in unallocated space. Full details of Ghost command line parameters can be accessed by starting Ghost with the '-?' switch, as shown in Figure 5.

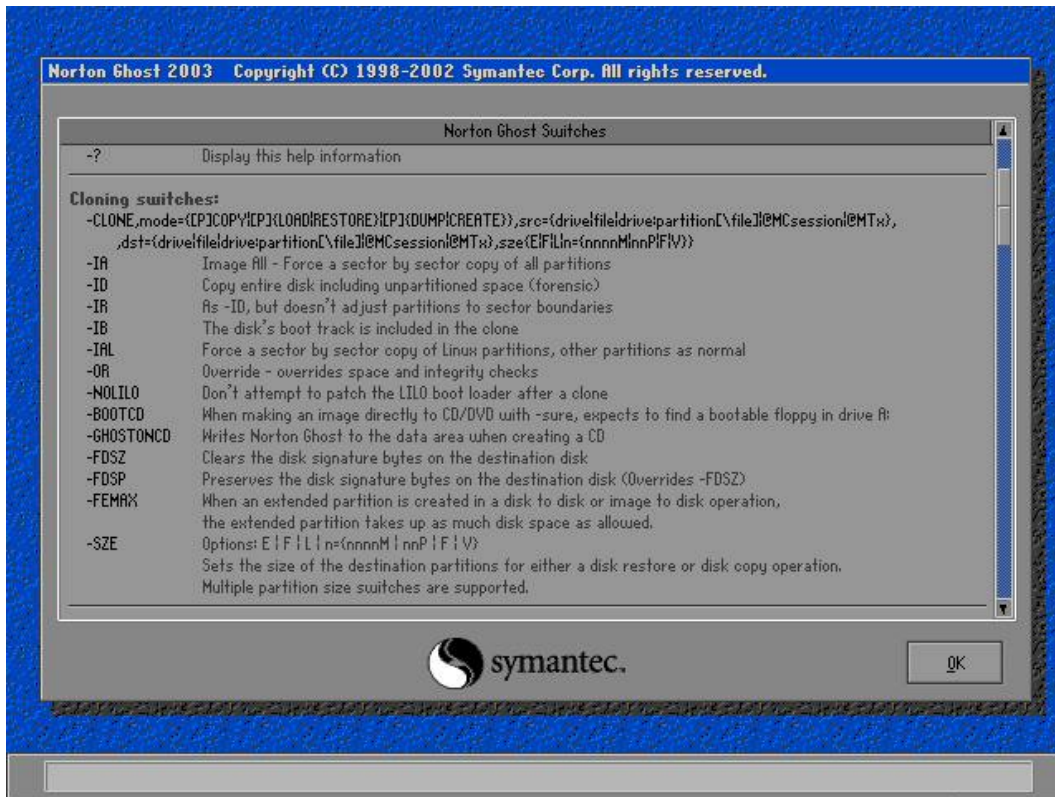


Figure 5 - Ghost command line cloning switches

When the process described in Method 1 is unsuccessful, the cloning element of Method 2 provides the opportunity for an investigator to make essential modifications to the operating system under investigation. Directly booting from read-only devices such as mounted images or write-blocked media means that this functionality is not available. The key feature of Method 2 is the repeatable nature of the process that is afforded by the use of snapshots. Utilising the snapshot feature and manipulating the file system via REDO files leave the integrity of the original cloned data left intact. This integrity can be verified by running an MD5 hash of the drive data immediately after cloning, taking a snapshot, modifying the disk (by booting the system), reverting to the snapshot and again hashing the drive. The resultant MD5 hashes will be the same.

Figure 6 details the steps required to clone data from a write-blocked hard drive or mounted forensic images to a virtual disk. Figure 7 depicts the processes that can be applied in order to resolve anomalies that have been encountered with restored systems. It should be noted that in order to resolve the issues encountered with Win9x systems, the relevant process could be applied without the need for cloning out the drive.

## Method 2

*This method has been used to facilitate read/write access to cloned Win2k/XP systems that have required registry/file system modification in order to successfully boot. Explanations of steps common to both methods are as detailed in Method 1.*

1. Mount the image as a single physical disk
2. Start VMware
3. Create a new custom Virtual Machine that corresponds to the operating system under investigation
4. Add a new virtual disk of the appropriate size (plus 0.1/0.2GB)  

VMware virtual disks are created based on the calculations for binary kilobytes (1024 bytes) as opposed to decimal kilobytes (1000 bytes).

E.g. A 20GB drive (20,000,000,000 bytes) equates to a 18.63GB virtual disk (18,626,451,492 bytes). It has been found that an additional 0.1/0.2GB is required to ensure sufficient LBA sectors are available for the clone.
5. Add the mounted disk image as a (raw) physical disk
6. Do **not** add any networking capability  

If networking is required, ensure adequate measures are in place on the host system to retain isolation between host and subject.
7. Boot the new virtual machine with a Ghost boot floppy disk  

If a full sector-by-sector copy is required, utilise command line switches as detailed in Figure 5.
8. Clone the raw disk to the new virtual disk  

If the new virtual disk is the same size as the original, there should be no change to any partition sizes during the cloning process. If the new virtual disk size is greater in capacity, it may be necessary to adjust the partition allocations to ensure they mirror the original.
9. When completed shut down the virtual machine and remove both the raw disk and the ghost floppy disk
10. Take a **snapshot** of the system
11. Boot the new Virtual Machine  

Consideration should be given at this point to ensure that the virtual machine date/time is set back to the date of seizure.
12. Disregard warnings relating to SCSI devices
13. New hardware will be detected
14. VMtools can be installed to facilitate adjustment of screen resolution

**Figure 6 - Details of Virtual Boot Process Using Cloned Image Access**

## Resolution of Boot Problems with Restored Systems

When a virtual machine has been created from existing subject data as described using either Method 1 or Method 2 above, it is likely that the investigator may encounter problems in successfully activating the resultant system. Processes for resolving these issues are outlined in the flowchart below.

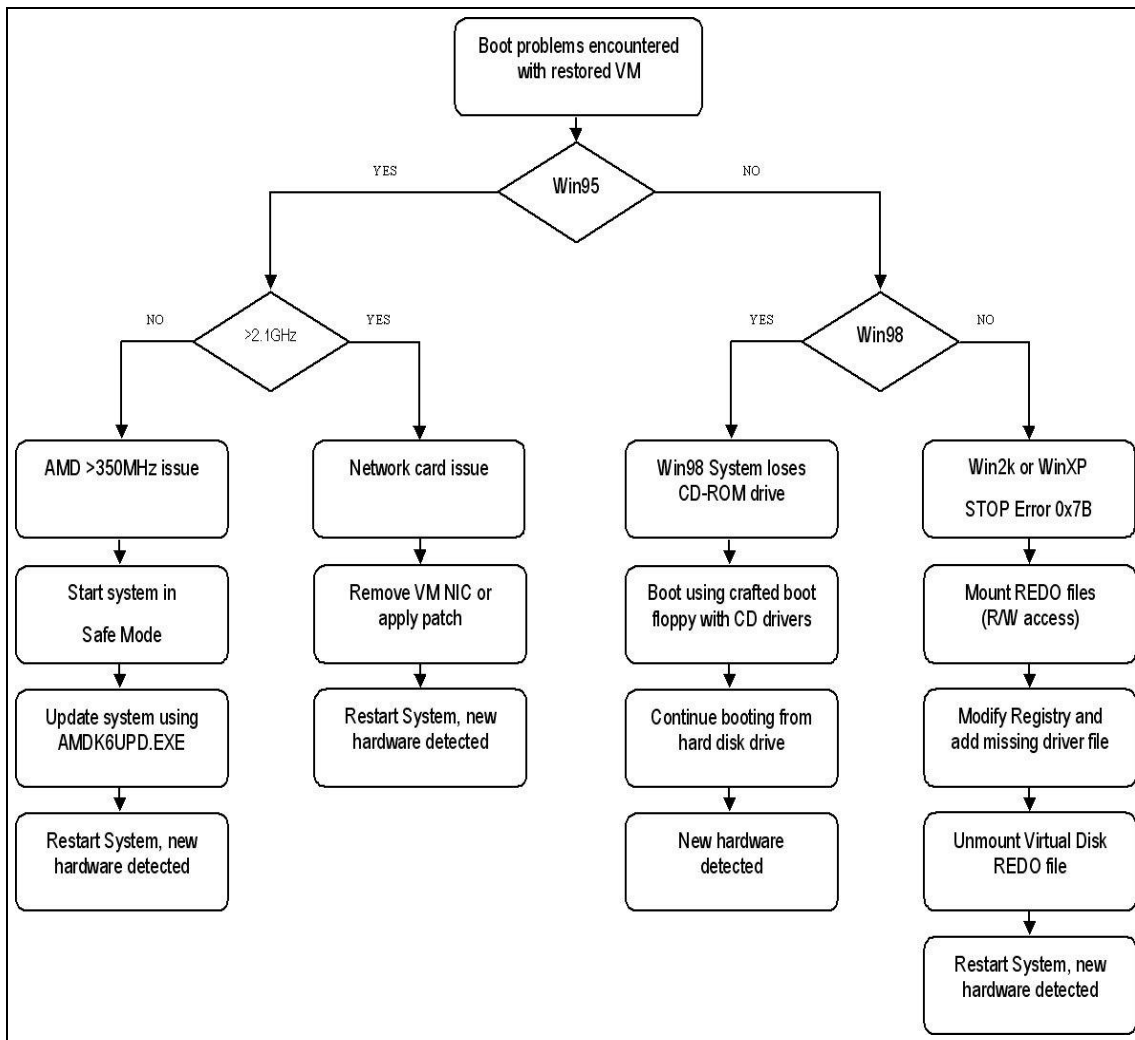


Figure 7 - Process for resolving boot issues

This area intentionally left blank

## Win95 Fast Processor Issue

With Windows 95, there are two known issues relating to fast processor speeds.

If the restored system is Windows 95 OSR2, OSR2.1, or OSR2.5 and the host system has an AMD processor running at speeds of 350 MHz or above, you may receive the following error message:

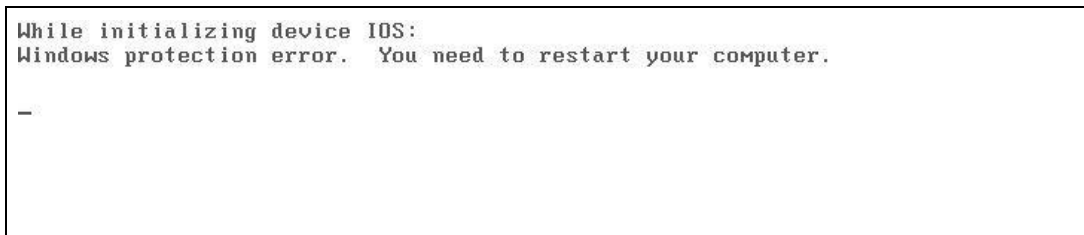


Figure 8 - Windows 95 device IOS: error

Microsoft has a documented resolution to this issue that involves the application of a patch containing modified system files<sup>9</sup>. This patch file, 'amdk6upd.exe' (284KB) is intended for the anomaly occurring on systems using an AMD-K6 processor. If the restored Win95 system freezes with the above message, start the system in safe mode and apply the patch.

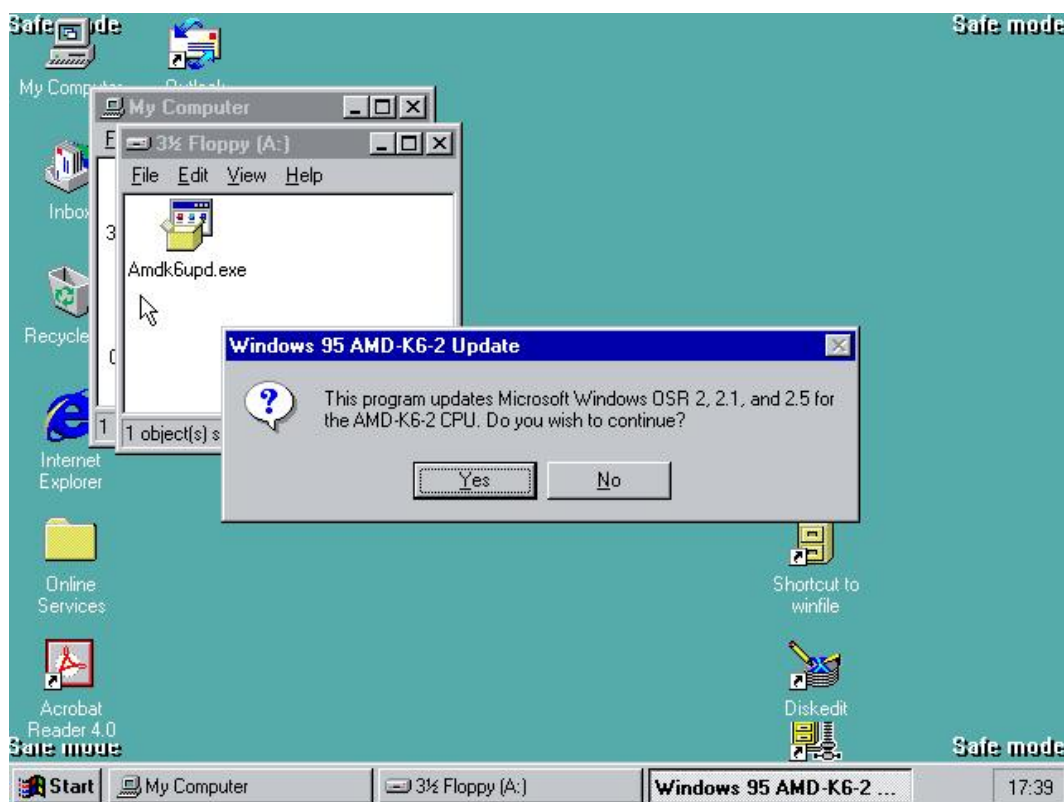


Figure 9 - AMD K6-2 > 350Mhz issue

Once installed the system needs to be re-started, at which point it will continue with a full boot, including detection of new hardware.

If the system is running at 2.2GHz or above and has a network card installed, you may receive the error message:

While initializing device NDIS.  
Windows Protection Error.  
You need to restart your computer

This problem may also affect Windows 98 systems. The resolution to this issue is documented by Microsoft and can be accessed from their support web site<sup>10</sup>. An alternative resolution is the complete removal of network capability, as discussed previously, although this may not be appropriate if the original system was part of a network and subsequent networking *is* required. It should be borne in mind that any existing registry artefacts relating to networking *will* be affected by the addition of virtual networking cards – *not* including networking will leave these artefacts unchanged and may provide additional information to the examiner in the original environment.

**This area intentionally left blank**

## Win98 'Lost' CD-ROM Issue

During the installation of Windows 98 from CD, it has been the author's experience that Windows will 'lose' the CD-ROM drive and will be unable to complete the installation. The same holds true for the detection of new hardware when a Windows 98 system is relocated to new hardware. The result is that required driver and cabinet files that are not on the local disk cannot be loaded from the CD.

Under normal installation conditions, it is common to find all of the relevant cabinet files on the local disk. OEM installations commonly use an OPTIONS\CABS\ folder within the Windows folder. If these files are not available on the local disk when dealing with restored subject drives, having to copy the relevant files to the subject disk is less than desirable, as this will dramatically change the contents of the system. The ultimate goal is to boot the subject system with minimal interference to the existing installation.

The resolution to the issue of the 'lost' CD-ROM is to ensure that an underlying DOS level CD-ROM driver (MSCDEX) is loaded at boot time so that any subsequent requests for CD access do not rely on the Windows level driver.

The Windows 98 startup disk contains generic CD-ROM drivers that can facilitate access to the CD-ROM drive throughout the hardware detection phase. By copying the MSDOS.SYS file from the subject drive onto a copy of a Windows 98 startup disk and modifying the AUTOEXEC.BAT file to point to the boot drive (by default, the C: drive), the system will load the relevant drivers and continue booting the system from the hard drive. Examples of the required entries for a modified AUTOEXEC.BAT file and the MSDOS.SYS file can be seen in Figure 10 & Figure 11 below. Once all necessary modifications are made to the restored system, the crafted boot disk can be removed and the system can be started normally.

```
path=a:;\;%CDROM%:\;c:\windows;c:\windows\command
set comspec=c:\windows\command.com
set tmp=c:\windows\temp
set temp=c:\windows\temp
```

Figure 10 - A:\AUTOEXEC.BAT required entries

```
[Paths]
WinDir=C:\WINDOWS
WinBootDir=C:\WINDOWS
HostWinBootDrv=C

[Options]
BootMulti=1
BootGUI=1
Logo=0
DoubleBuffer=1
AutoScan=1
WinVer=4.10.2222
BootDelay=2
BootMenu=1
```

Figure 11 - A:\MSDOS.SYS required entries

## Win2k/XP Blue Screen Issue

The largest obstacle that the author encountered when dealing with restored machines was related primarily to changes involving the underlying architecture. VMware virtual machines are based upon the Intel BX440 motherboard (full details of which are available from within the VMware documentation). It was discovered that attempting to boot a disk image originally installed on a non-Intel system would result in a blue screen error 0x7B INACCESSIBLE\_BOOT\_DEVICE. The problem stems from the absence of Intel specific entries within the critical device database section of the registry and an associated missing driver file, intelide.sys.

There are a number of workarounds for this problem, a VMware specific solution is documented within the support section of the VMware web site<sup>7</sup>. A Microsoft solution is documented within their Knowledgebase<sup>8</sup>. Both methods rely on being able to access the original hardware. Concerning forensic images that are mounted or cloned into a new environment, access to original hardware may not always be possible. It *can* be achieved by first physically restoring to new media, placing the restored image into the original machine, undertaking the necessary changes and then re-imaging. However, this is a time consuming process and is not easily repeatable.

*The remainder of this paper deals with Method 2 - Restored Image Access.*

In order to resolve the blue screen issue, the snapshot feature of VMware 4 can be utilised.

The following steps use the virtual disk driver developed by Ken Kato (VMware's Back)<sup>6</sup> in order to mount the VMware virtual disk image. A similar unsupported disk mount utility is available from VMware<sup>12</sup>. Both tools allow read/write access to mounted virtual disks, either directly or via REDO files. In this way, modification can be made to the registry and the appropriate driver file can be added to the operating system. Obviously, these changes *will* affect the overall 'forensic' image. However, the entire process is designed to be able to boot, a process that will naturally cause changes to disk data. The changes that are imposed using the method below are specific to this issue and minimal. It is the snapshot feature of VMware that makes the entire process entirely repeatable and forensically sound.

**This area intentionally left blank**

## Installation of the Virtual Disk Driver

The virtual disk driver consists of two files, vdk.exe and vdk.sys. These are available as a zip archive from VMware's Back<sup>6</sup>. The simplest method of installation is to extract the vdk.exe & vdk.sys files and copy both files into either the WINDOWS\system32 or WINNT\system32 folder dependent upon whether the host machine is Windows XP or Windows 2000 based. Once copied into the relevant location, they are installed and activated as a service as described below, the full details of which are described in the readme.txt file provided within the vdk.zip archive.

Installation and subsequent disk mount instructions are issued from the command prompt.

```
Install the Virtual Disk Driver.

SYNTAX:
  VDK.EXE INSTALL [driver] [/AUTO]

OPTIONS:
  driver  Specifies the path to the Virtual Disk Driver file (VDK.SYS).
          Default is VDK.SYS in the same directory as VDK.EXE.
          (Note: *NOT* current working directory.)

  /AUTO  Configures the driver to start at the system startup.
          (Note: this option does not start the driver after
          installation is completed.)
          By default the driver has to be started manually.

Device drivers cannot be started from network drives.
Make sure to place VDK.SYS on a local drive.
```

**Figure 12 – Installation details from vdk.zip: readme.txt**

*If the files are installed and started from the system32 folder, they will subsequently be accessible from anywhere within the host system. In this way, the relevant image files can be more efficiently opened directly from the folder they reside in.*

**This area intentionally left blank**

## Use of the Virtual Disk Driver

When a snapshot is taken of a virtual machine, a series of REDO files are generated upon the first use of that machine post snapshot. These REDO files track any changes that are directed towards the virtual disk and are applied or discarded at the discretion of the investigator. By using the virtual disk driver to mount these REDO files, read write access can be facilitated to the cloned disk whilst always preserving the integrity of the original cloned image.

```
The command to mount the relevant virtual disk file will be: -  
  
C:\[path to subject virtual machines] > vdk open <drivenumber> <virtual disk REDO  
file> /rw  
  
e.g.  
E:\VMClones\Win2k\ > vdk open 0 "Windows 2000  
Professional.vmdk.REDO_a03380" /rw  
  
The /rw switch provides read/write access to the REDO files and hence all  
of the data within the underlying disk. Any changes can be latterly  
discarded simply by reverting to the snapshot.  
  
To close a mounted image, simply use the command: -  
  
C:\[path to subject virtual machines] > vdk close <drivenumber>  
  
NB To successfully close a mounted image, all access to the mounted  
drive must also be closed, including explorer windows and applications  
such as regedit where applicable.
```

Figure 13 - Using the virtual disk driver

**This area intentionally left blank**

## Registry Modifications

In order to perform modification to the subject registry, it is first necessary to determine which control set is active on that system.

The CurrentControlSet determines configuration data for the system and is where 'last known good configuration' data is loaded from when required. Examining the registry and looking at the value stored in HKEY\_LOCAL\_MACHINE\System\Select can ascertain this, as shown in Figure 14 below.

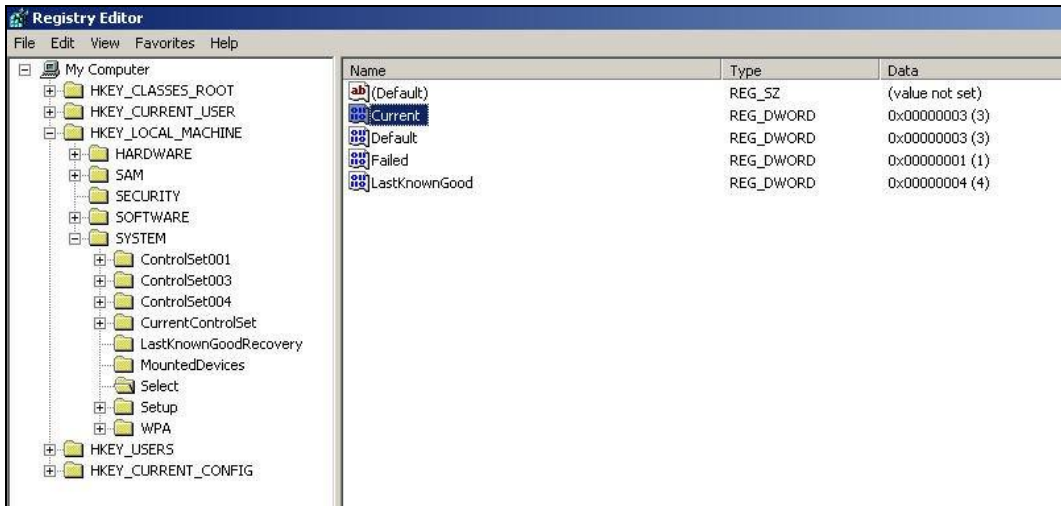


Figure 14 - CurrentControlSet

Figure 15 overleaf details the specific steps required to merge registry entries into an 'offline' registry.

**WARNING:** Using Registry Editor (REGEDIT.EXE or REGEDT32.EXE) incorrectly can cause serious, system-wide problems that may require you to reinstall Windows to correct them. Prior to undertaking the following steps, back up your registry first (using either NTBackup.exe or RDisk.exe /s).

**This area intentionally left blank**

1. Load the **system** hive from the subject machine into the examination machine registry under the HKEY\_LOCAL\_MACHINE section. Call the newly loaded hive NEWSYSTEM.  
  
e.g. HKEY\_LOCAL\_MACHINE\NEWSYSTEM\ControlSet001\
  2. Use the regedit File/Import option to update the loaded hive with the contents of 'mergeide.reg'.  
  
This will dynamically add the appropriate keys to the critical device database section of the loaded hive.
  3. Copy the appropriate **intelide.sys** file into the WINDOWS\system32\drivers folder (WinXP) or WINNT\system32\drivers (Win2k).  
  
This file can be extracted from the driver.cab cabinet file located in C:\WINDOWS\Driver Cache\i386 (WinXP) or C:\WINNT\Driver Cache\i386 (Win2k).
  4. Unload the NEWSYSTEM hive and close regedit.
  5. Close the vdk mounted drive image.
  6. Start the modified VMware virtual machine.  
  
The system should now boot without incident and new hardware will automatically be detected by the operating system. (The hardware may not be detected until such a time as a user has been logged in to the system).

**Figure 15 - Registry modifications**

Appendix 1 details the required registry entries. This Appendix contains a modified Intel specific version of a file available from the Microsoft Help and Support Site<sup>8</sup>. If necessary, a text editor can be used to modify the 'mergeide.reg' registry file in order to reflect the loaded hive name and the relevant control set of the subject machine.

From experimentation, it has been found that there is no need to reboot until all relevant drivers have been identified and installed by the OS and the desktop has been loaded. Prompts to reboot can be ignored.

Once the system has been started, the VMware suspend feature can be used to 'pause' the machine at any point. The suspend feature works entirely independently of the snapshot feature.

### **Password extraction from Win2k/WinXP systems**

An obvious benefit of being able to manipulate the subject registry in a repeatable manner is in the use of exploits to assist in breaking passwords, as opposed to simply resetting them and potentially losing access to encrypted files in the restored system.

With the introduction of the more secure systems of Windows 2000 and Windows XP, previously used methods of password extraction for Windows NT machines are obsolete. Where previously the SAM (Security Access Manager) file could be copied and the password hashes attacked directly, the introduction of syskey into 2000 and XP has introduced another level of security to inhibit password extraction.

If physical access to the operating system is available from the cloned image, including the ability to manipulate the registry from the host system, password cracking is again possible with little effort, provided the right tools are available. Albeit it is possible to crack passwords through some forensic suites, these methods may require the relatively time consuming aspects of disk indexing prior to the attack being launched.

A known password exploit for Windows 2000 and XP is that of changing the logon screensaver to a command prompt<sup>13</sup>. This affords administrator level access directly to the system and allows interaction with the SAM with syskey activated. Third party tools can then be utilised to enable extraction of usernames and the related password hash.

The registry keys located within the Control Panel\Desktop section of the HKEY\_USERS\.Default hive controls Screensaver activity.

If the REDO files are again mounted using vdk, the 'default' hive can be loaded into regedit as described previously and some minor alterations can be made to no more than four keys, as shown in Figure 16.

```
[HKEY_USERS\.Default\Control Panel\Desktop]
SCRNSAVE.EXE = "cmd.exe" (Default = logon.scr)
ScreenSaveTimeOut = 15 (Default = 600 secs)
ScreenSaveActive = 1 (Default = 0)
ScreenSaverIsSecure = 0
```

**Figure 16 - Screensaver 'command prompt' exploit**

A utility such as 'pwdump2'<sup>15</sup> or 'john the ripper'<sup>16</sup> can then be used to extract the usernames and password hashes. These utilities are available from a number of Internet sites. Once obtained, the password hashes can be attacked and decrypted using any number of tools, such as commercially available products from @Stake (l0phtcrack)<sup>17</sup> or AccessData (Password Recovery Toolkit)<sup>18</sup>.

Once the passwords have been decrypted, the registry modifications that have been undertaken to facilitate the extraction of the password hashes can be reversed if so desired. Alternatively, *all* changes can be discarded and the machine activated as if from its original cloned state. This may however necessitate repeating the steps described to merge the registry entries to resolve the blue screen issue, if the machine is one that is thus affected unless a snapshot had been taken.

### **Hardware Solution**

There exists a physical device (the VOOM ShadowDrive)<sup>14</sup> which can both simultaneously write-protect a subject hard disk and afford a cache to intercept any required disk-writes. This product is around \$1295 per unit and is only available inside the US and Canada as of November 2004.

It is anticipated that the above-described methodology will work equally effectively using such a hardware device; however this has yet to be tested.

## **Conclusions**

The above methods of booting subject hard disk drives have been extensively tested by the author on both Intel and AMD host machines at processor speeds of up to 3.02GHz.

The direct image process described in Method 1 provides rapid access to an emulated system, however it is reliant upon continued access to the original forensic image files. These files may be of considerable size and, when considering the type of access to the system that is ultimately required, a vast proportion of the disk image may be irrelevant. An example of this would be a 80GB hard disk image that only contains 2GB of relevant live data. The entire restored virtual system, if cloned out to virtual hardware using Method 2, would comfortably fit on a DVD or other more compact media. This would provide for easier and more efficient transportation of the resultant system.

Having access to an emulated system that can be recreated in a repeatable manner gives the investigator a number of hitherto unavailable opportunities. The subject system can be experienced as would have been by an original user of the system, in terms of such items as the layout of the desktop or personalised settings relating to installed software. Additionally, such software can be utilised as found on the subject, without the need for extraction of multiple files and recreation of registry settings. In essence, the entire system can be investigated in a 'live' state without fear of changing evidential content. Any changes to the system can be discarded simply by reverting to the initial snapshot taken at the point of the completed cloning of the subject drive.

The two solutions discussed are far from definitive for all restorative issues, however they provide a forensically repeatable method of investigating 'live' system(s).

In addition to the benefits that an investigator can derive from the use of such a methodology, researchers too can readily utilise similar steps to assist in creating wholly safe and 'repeatable' environments for use in analysing software. Whilst the versatility of the VMware environment offers a relatively unique way in which to control experimentation, it should be noted that the speed of the host processor might have some effect on the resultant guest system. On virtual systems where the host processor is considerably faster than on any previous (cloned) guest, the system may run inordinately fast with issues arising as discussed in this paper. Conversely, it may be that the host processor is considerably slower than was the original guest; this too might well impact upon the operation of software being scrutinised.

## **Recommendations**

The focus of this paper has been on restoring Windows based systems to an Intel based VMware virtual environment, with Mount Image Pro and VMware workstation as the primary tools used to facilitate the requisite processes. It would be desirable to ascertain if the same results can be achieved using the Encase PDE and Microsoft VirtualPC, either in place of, or in conjunction with, either of the above applications.

Future research in this area could be directed at the restoration of alternative mainstream operating systems such as Linux and Novell, both of which can be found on PC based architectures. It is likely that architecture related issues might be encountered on these restored systems similar to those issues that have been described above.

Additionally, research into the utilisation of the hardware solution potentially afforded by the ShadowDrive, as mentioned above, would be of value. As and when this item of hardware becomes available outside of the US and Canada, this too may afford another method of access to a bootable subject drive which will remain repeatable and forensically sound.

## References

1. ACPO Good Practice Guide for Computer Based Evidence  
<http://www.4law.co.il/Lea92.htm>  
Last visited 23 Nov 2004
2. Guidance Software Physical Disk Emulator  
<http://www.guidancesoftware.com/support/EnCaseForensic/version4/dl.asp>  
Last visited 23 Nov 2004
3. Mount Image Pro  
<http://www.mountimage.com/>  
Last visited 23 Nov 2004
4. VMware Workstation 4.5  
[http://www.vmware.com/products/desktop/ws\\_features.html](http://www.vmware.com/products/desktop/ws_features.html)  
Last visited 23 Nov 2004
5. Microsoft VirtualPC 2004  
<http://www.microsoft.com/windows/virtualpc/default.mspx>  
Last visited 23 Nov 2004
6. VMware's back – Virtual Disk Driver  
<http://chitchat.at.infoseek.co.jp/vmware/vdk.html>  
Last visited 23 Nov 2004
7. VMware support  
[http://www.vmware.com/support/kb/enduser/std\\_adp.php?p\\_faqid=36](http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=36)  
Last visited 23 Nov 2004
8. Microsoft Help and Support – Stop 0x7B  
[http://support.microsoft.com/default.aspx?scid=kb:\[LN\];Q314082](http://support.microsoft.com/default.aspx?scid=kb:[LN];Q314082)  
Last visited 23 Nov 2004
9. Microsoft Windows 95 AMDK6UPD  
[http://www.microsoft.com/windows95/downloads/contents/WURecommended/S\\_WUServ  
icePacks/AMDPatch/Default.asp](http://www.microsoft.com/windows95/downloads/contents/WURecommended/S_WUServ<br/>icePacks/AMDPatch/Default.asp)  
Last visited 24 Nov 2004
10. Windows Protection Error in NDIS with a CPU That Is Faster Than 2.1 GHz  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;312108>  
<http://support.microsoft.com/kb/243199/EN-US>  
Last visited 10 January 2005
11. Hotfix file for Win9x NDIS issue  
[http://www.geocities.com/ghavipour/Ndis\\_en.html](http://www.geocities.com/ghavipour/Ndis_en.html)  
Last visited 10 January 2005
12. VMware Disk Mount Utility  
<http://www.vmware.com/download/diskmount.html>  
Last visited 23 Nov 2004
13. Reset Administrator Password  
[http://snakefoot.fateback.com/tweak/winnt/install.html#RESET\\_PASSWD](http://snakefoot.fateback.com/tweak/winnt/install.html#RESET_PASSWD)  
Last visited 23 Nov 2004

14. Voom ShadowDrive  
[http://www.voomtech.com/voom\\_products/smart\\_storage\\_solutions/Shadow.html](http://www.voomtech.com/voom_products/smart_storage_solutions/Shadow.html)  
[http://www.voomtech.com/voom\\_pdf/ShadowDriveNoOptions.pdf](http://www.voomtech.com/voom_pdf/ShadowDriveNoOptions.pdf)  
Last visited 23 Nov 2004
15. pwdump2  
[http://www.bindview.com/Support/RAZOR/Utilities/Windows/pwdump2\\_readme.cfm](http://www.bindview.com/Support/RAZOR/Utilities/Windows/pwdump2_readme.cfm)  
Last visited 23 Nov 2004
16. john the ripper  
<http://www.openwall.com/john/>  
Last visited 23 Nov 2004
17. l0phtcrack  
<http://www.atstake.com/products/lc/>  
Last visited 23 Nov 2004
18. AccessData PRTK  
[http://www.accessdata.com/Product00\\_Overview.htm](http://www.accessdata.com/Product00_Overview.htm)  
Last visited 23 Nov 2004

**This area intentionally left blank**

## Appendix 1 – mergeide.reg

### Registry entries required to activate Intel based disk drivers when transferring a system from a non-Intel based motherboard

; ---START COPY HERE

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_1222]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_1230]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_2411]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_2421]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_7010]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_7111]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Control\CriticalDeviceDatabase\pci
#ven_8086&dev_7199]
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
"Service"="intelide"
```

; Add driver for intelide (requires intelide.sys in drivers directory)

```
[HKEY_LOCAL_MACHINE\NEWSYSTEM\ControlSet001\Services\IntelIde]
"ErrorControl"=dword:00000001
"Group"="System Bus Extender"
"Start"=dword:00000000
"Tag"=dword:00000004
"Type"=dword:00000001
"ImagePath"=hex(2):53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,44,00,\
52,00,49,00,56,00,45,00,52,00,53,00,5c,00,69,00,6e,00,74,00,65,00,6c,00,69,\
00,64,00,65,00,2e,00,73,00,79,00,73,00,00,00
```

; --- END COPY HERE