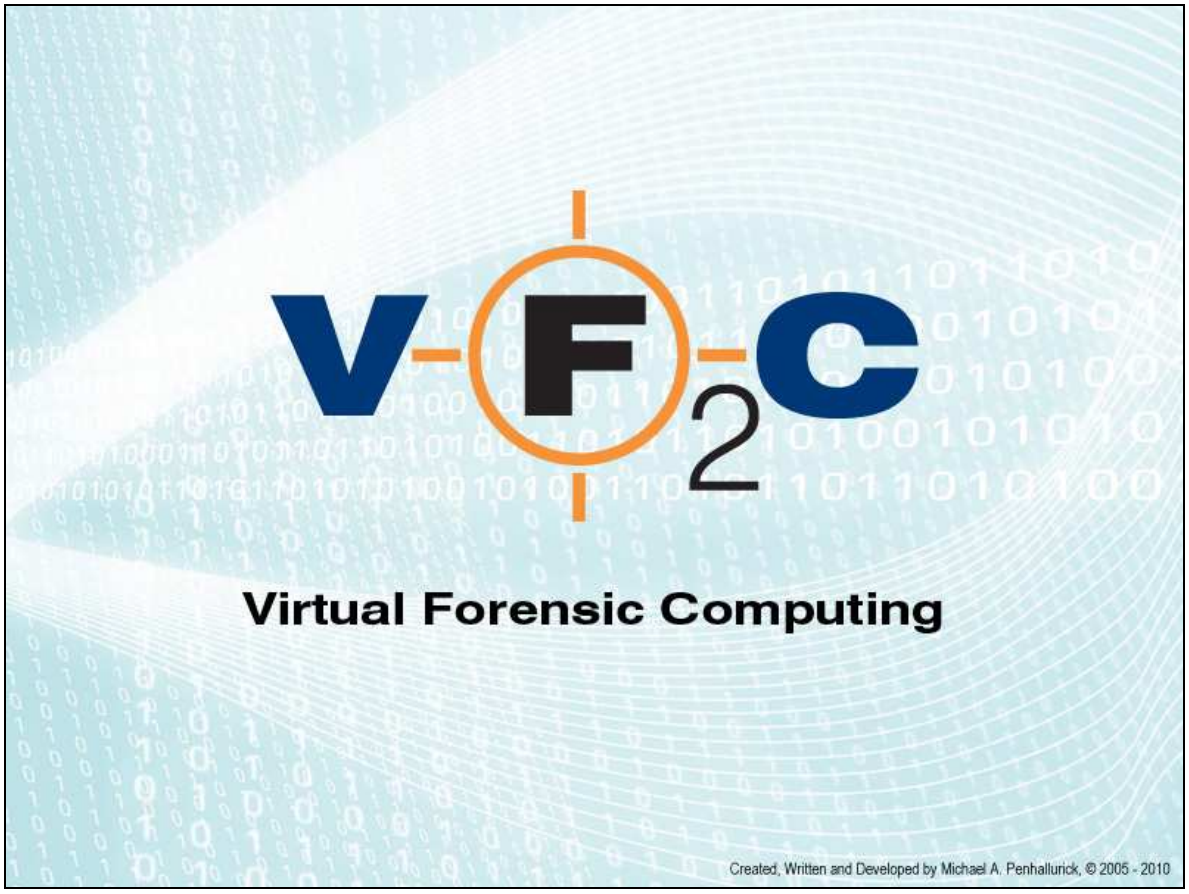


User Guide v1.0

VFC 2.10.10.4

VFC2™ User Guide

Table of Contents

Overview

VFC (Virtual Forensic Computing) is a forensic application based upon the VFC Methodology. It has been developed to handle a variety of hard disk drive sources (physical disk, bit-for-bit disk copy or mounted forensic image file) and successfully transpose over 95% of such images into virtual machines - without expensive physical hardware disk caches or time-consuming conversion processes.

VFC is designed to predominantly utilise user mounted forensic whole-disk image files which are then presented to the system as an available physical disk.

A forensic disk image which is mounted read-only cannot be directly modified, thus ensuring the forensic integrity of the original image.

VFC can also utilise (write-blocked) 'real' physical disks or bit-for-bit 'flat' disk images, commonly referred to as RAW or DD images.

Without the use of a write-block device, original disks can (and probably will) be altered, thus compromising the integrity of the original data. The same is true of DD images when accessed directly.

VFC interrogates the selected device and calculates the disk geometry and partition information. It uses these calculations to create a virtual disk cache so that the required partition can be queried without risk of altering the underlying data.

Once the image source has been selected, VFC will list the available partitions and display them on the main system dialog. In general, the partition marked 'Bootable' will be the one containing the Operating System (OS). With certain systems (such as Windows Vista and above) the bootable partition may only be around 100MB and will not actually contain an OS. In these instances, select the next available partition, which will typically occupy the remainder of available disk space and will contain the OS.

Once the required partition is selected, VFC default behaviour is to analyse the OS by querying registry data and other relevant system files. The resultant information thus gleaned is displayed on the main VFC screen.

At this stage, VFC has sufficient information with which to create the required disk files and inject any required system fixes. The default file names of 'New Virtual Machine' and 'New Virtual Disk' can optionally be manually changed prior to generation.

Once the VFC VM has been generated, the launch facility is enabled and the machine can be booted into a virtual environment. Whilst there may be some limitations (particularly with screen resolution and OEM hardware devices), the

user can then interrogate and interact with the virtualised system in as close an approximation to the original as is possible.

If a logon password is required but not known, the machine can be suspended and the VFC Password Bypass routine can be utilised. (Windows Only)

If there are system restore points available, the in-built Windows System Restore feature can be used to 'rewind' the VFC VM to an earlier date. In so doing, this will undo necessary changes that the initial generation has implemented and the system will fail to boot from a restored session.

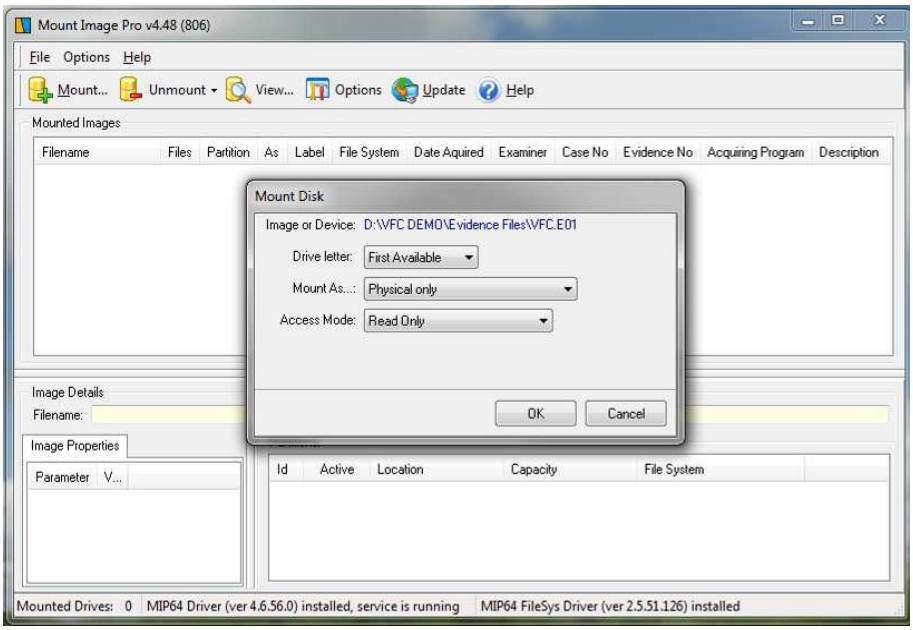
This is expected behaviour.

Simply power off the VFC VM and utilise the Restore Point Forensics feature to re-inject the necessary system drivers and thus enable a successful boot to the required System Restore Point.

Step-by-Step

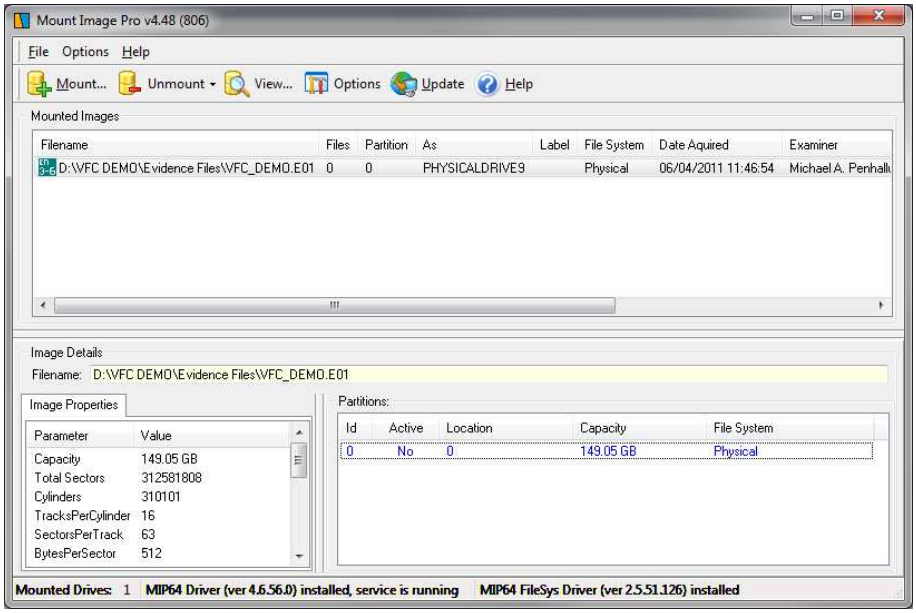
Mount a forensic whole disk image

There are several methods by which a forensic whole disk image can be mounted; the author's preferred mounting tool is Mount Image Pro and the drag-and-drop mode whereby the first image file (*.E01) is dragged into an open MIP session and mounted as a physical disk (no associated drive letter).



Once the image has been successfully mounted, the mounting application can be minimised as no further direct interaction is required.

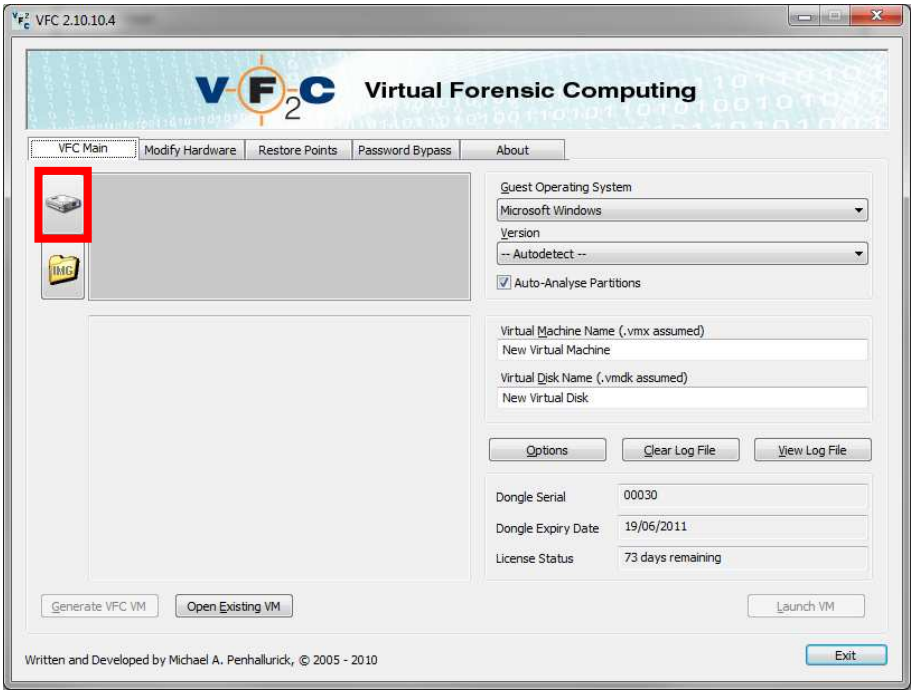
NB If using either Encase PDE or the FTK Imager mount function, closing the application will dismount the image. The MIP GUI can be closed but will minimise the application to the system tray whilst maintaining the mounted status of the image.



As can be seen from the above, the VFC_DEMO.E01 image has been mounted as PHYSICALDRIVE9 and is now available to the system.

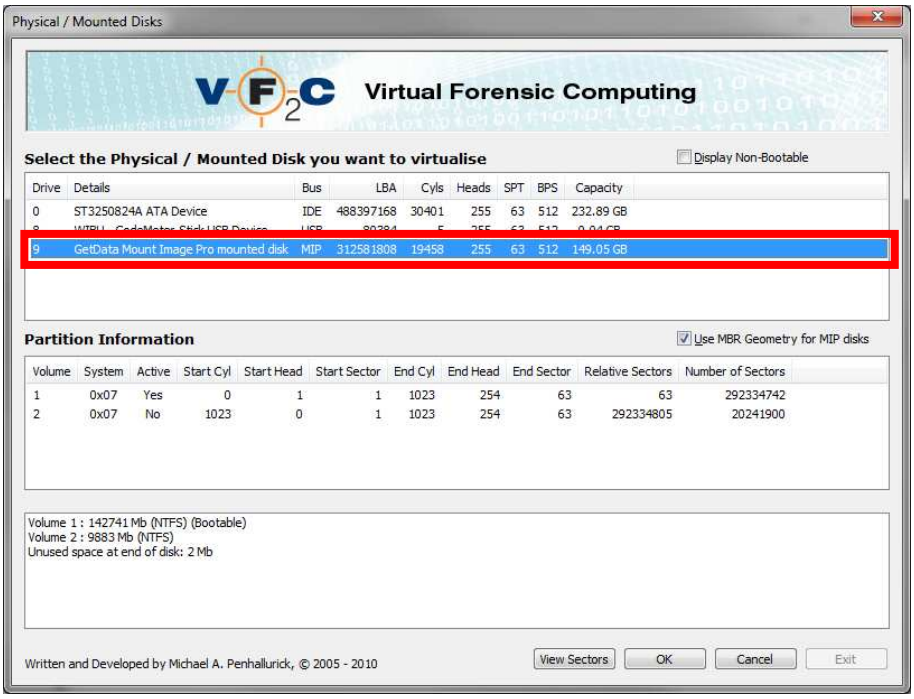
From this point, the MIP GUI is no longer directly required by VFC and can be minimised.

Select Source Device



Start VFC and use the hard disk icon located at the upper left of the screen to launch the drive selection dialog.

This process will enumerate all physical storage devices attached to the system and may take several moments.



Once enumeration is complete, the mounted drive will be displayed in the drive selection dialog.

If the mounted drive is not displayed, then VFC has been unable to ascertain that there is an active (bootable) partition present on the disk. This is most common with disks that have been used for data storage only, such as external hard disks or secondary storage devices.

Rarely, you may need to reboot the host machine and remount the drive before it is correctly detected by VFC. This may happen when a large number of disk images have been mounted / dismounted and multiple machines have been generated.

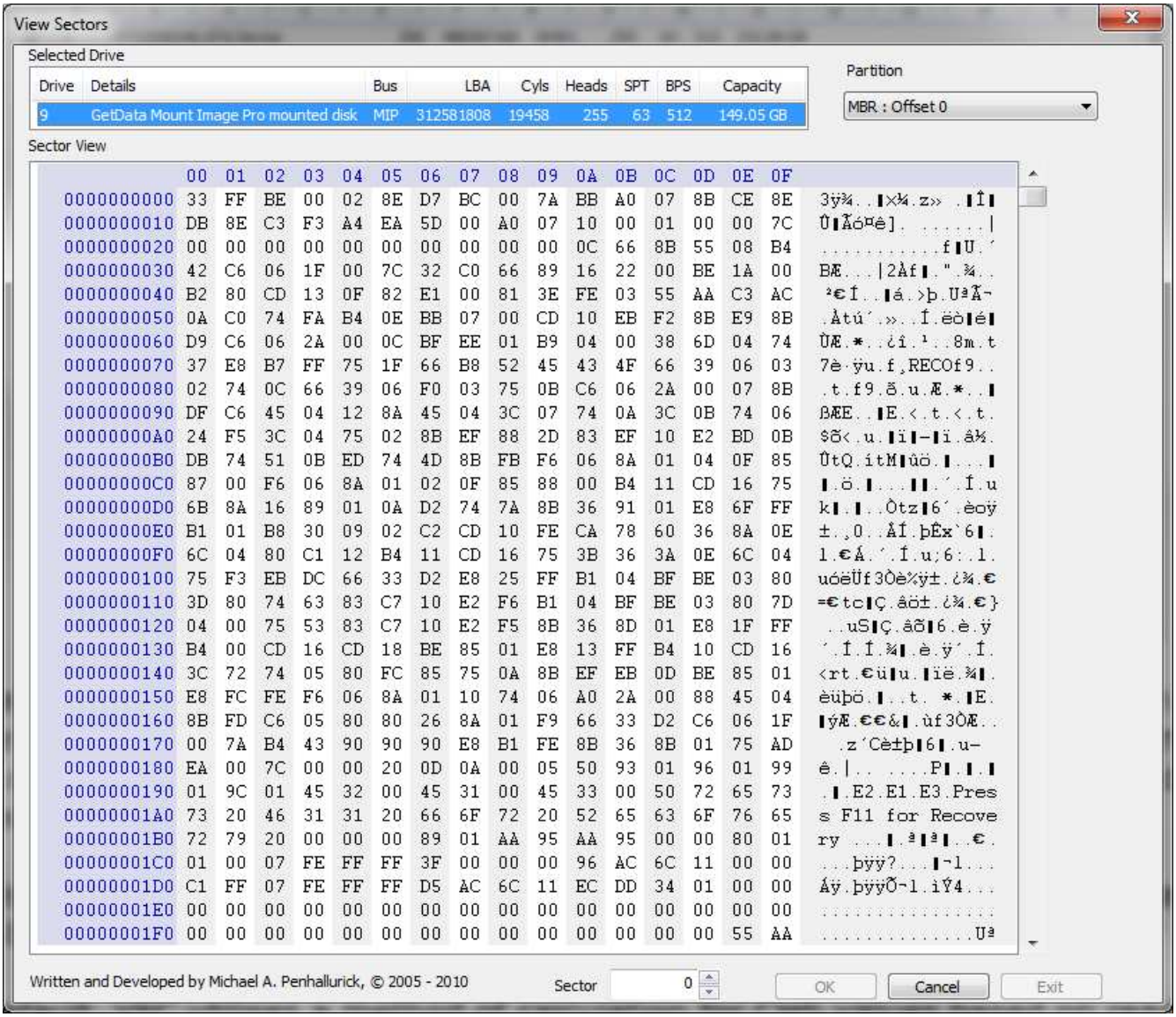
To display non-bootable drives, simply select the 'Display Non-Bootable' check-box located in the upper right of the drive selection dialog.

By default, VFC utilises a method of calculation for CHS values based on reading the MBR and then calculating Cylinders = LBA / Heads / Sectors. MIP3 & MIP4 use an alternate method of calculation which may result in a different set of values for the resultant CHS. The MIP calculation can be utilised by un-checking the 'Use MBR Geometry for MIP disks'.

Albeit MIP may mount the disk correctly and logical drives may be accessed via Windows Explorer, it has been noted that the default MIP calculation may cause the subsequent VFC generated VM to fail to boot. Using the MBR method, the same machine will successfully start.

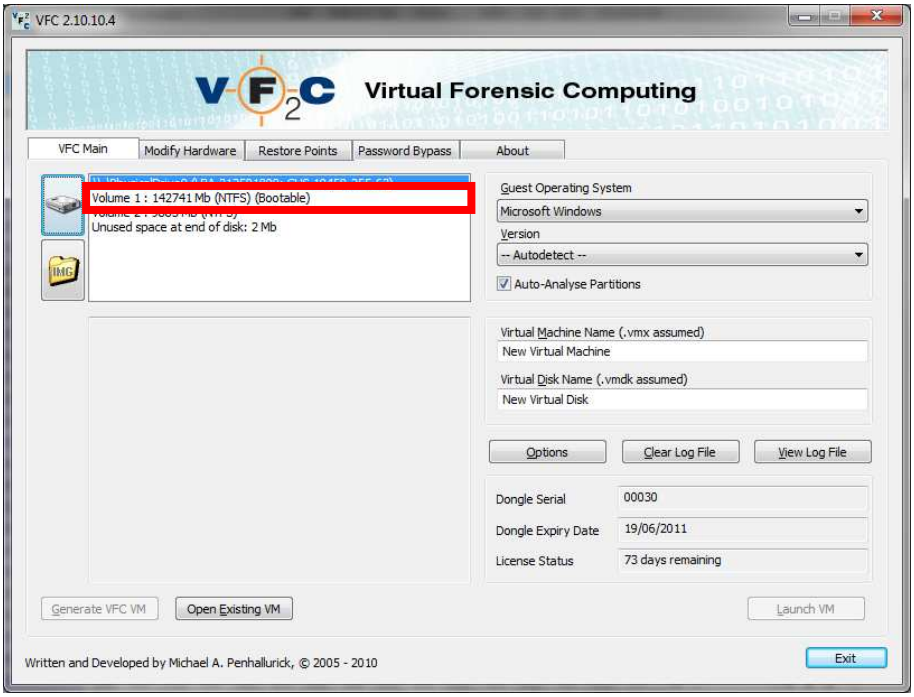
View Sectors

The 'View Sectors' option enables the user to quickly examine the disk contents in read-only hex-format. There are options available to quickly navigate to the first sector of the disk, the first sector of any identified partitions or to any selected sector on the disk.



Select Partition

Once the required physical drive has been selected, the available partitions (along with capacity, file system and status) will be displayed on the main dialog screen.

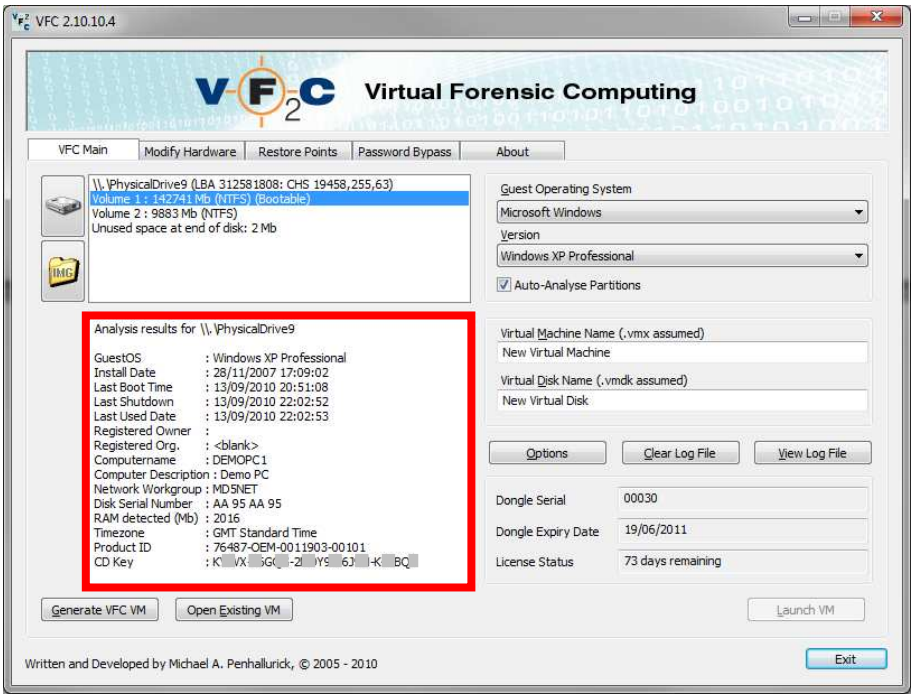


If the 'Auto-Analyse Partitions' check box is selected, selecting any of the available partitions will lead to an attempt to auto-detect the installed Windows OS.

The resultant analysis will also try to extract relevant information relating to the installed Windows OS, which will then be displayed in the lower-left section of the main dialog.

The 'Auto-Analyse Partitions' feature can be disabled if required and the OS version can be manually selected. Disabling 'Auto-Analyse Partitions' will preclude the extraction of any of the aforementioned information.

If required, various options which affect the generation of the Virtual Machine can be altered as desired (see Options, below).

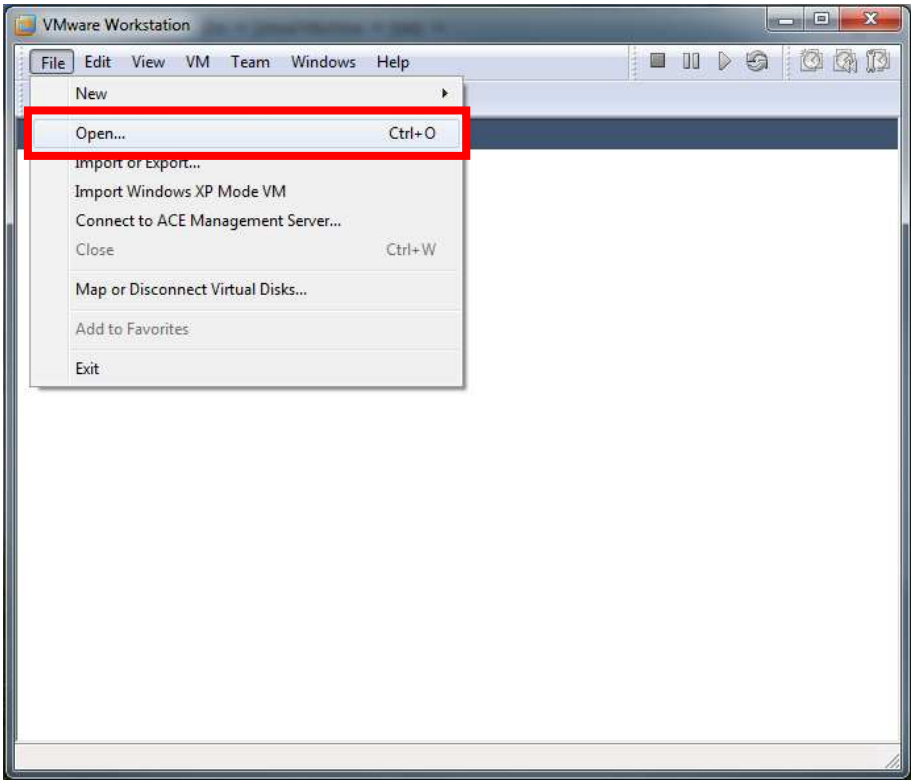


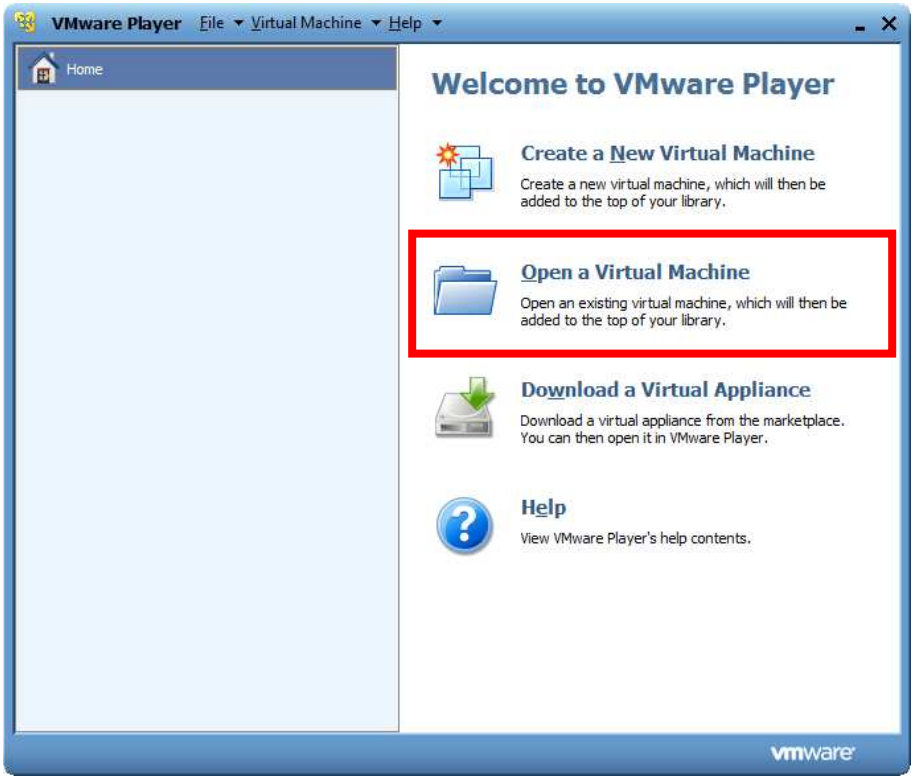
Once the analysis has been completed, you have the option of changing the Virtual Machine Name (default 'New Virtual Machine') and the Virtual Disk Name (default 'New Virtual Disk'). These values should be typically adjusted to reflect the details of the forensic image under investigation (e.g. Coakley-PC, HDD0).

When all relevant data has been entered and analysed, the 'Generate VFC VM' button will become active and the requisite files can be created, along with the application of any necessary system patches.

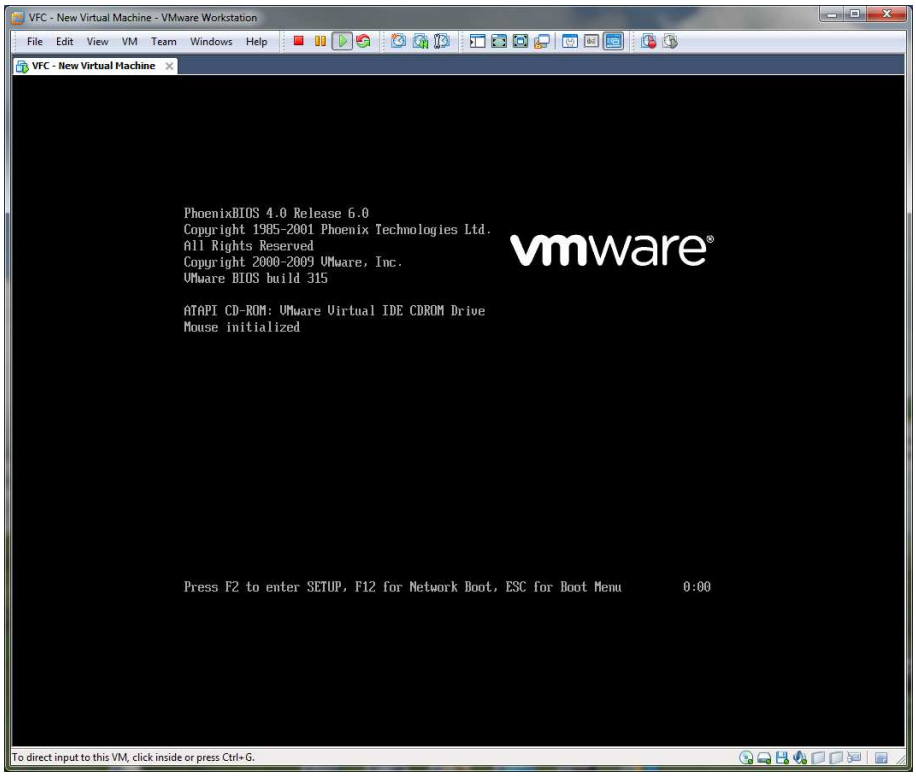
A successful generation will result in the creation of those files necessary to enable the subject mounted disk image to be booted in a Vmware virtual environment. This can be achieved by using the 'Launch' button located at the lower right of the main dialog screen.

Alternatively, the machine can be launched manually, typically by either double-clicking the generated .vmx file via Windows Explorer, or by starting the VMware application and using the various options to Open a Virtual Machine.





Once the Virtual Machine has been manually opened, it will be necessary to 'Power On' the virtual machine.



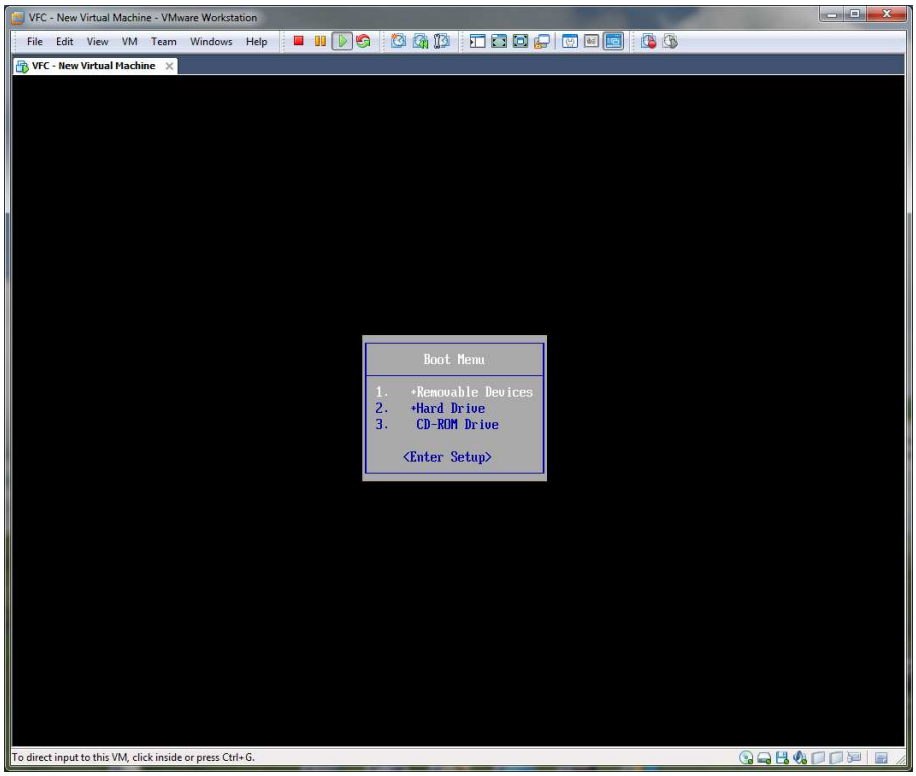
During the boot process, VMware displays options to access Setup (F2), Network Boot (F12) or the Boot Menu (Esc).

By default, VFC does not add any network connectivity.

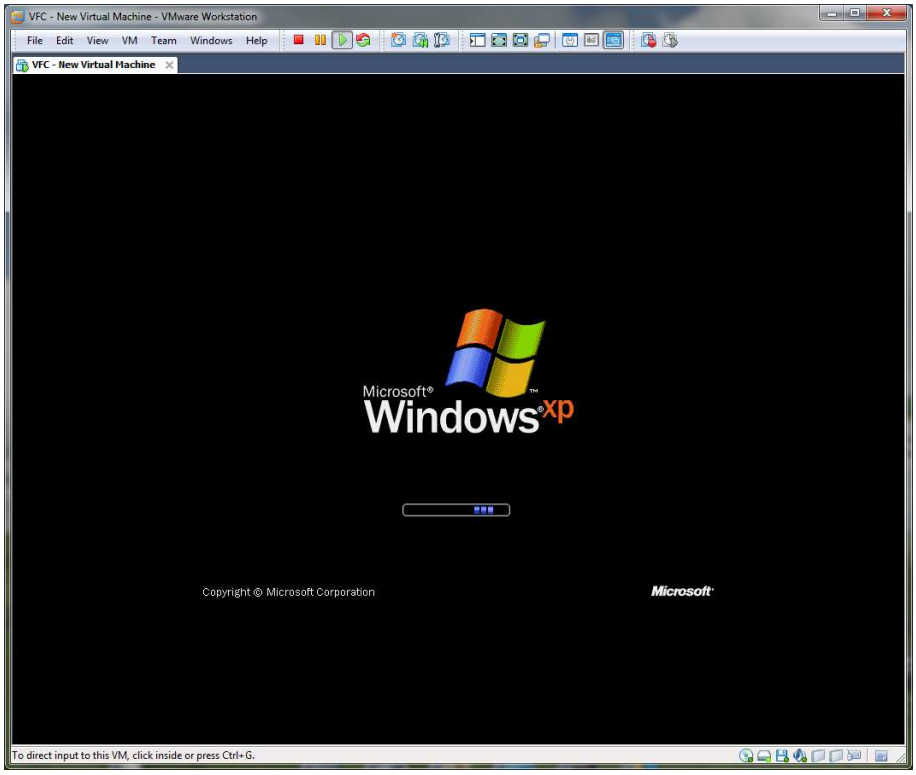
The default boot order is Floppy Disk, Hard Disk then CD-ROM. Typically the Boot Menu will need to be accessed in circumstances whereby the user wishes to boot from a CD or an attached ISO image.

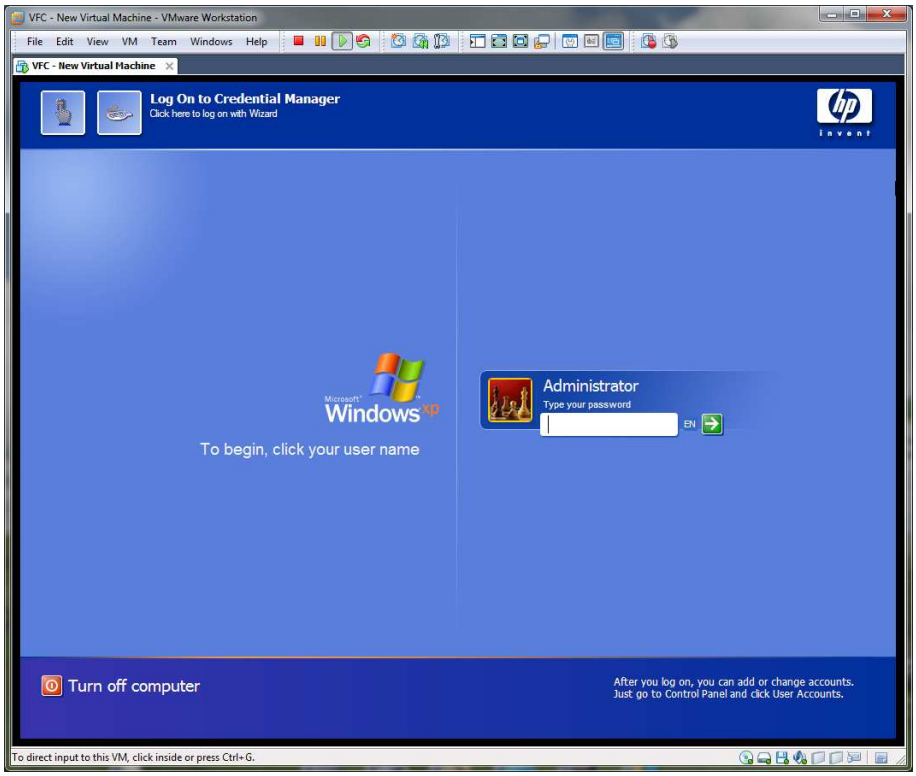
In order to access any of the boot options via the available boot keys, it is first necessary to give focus to the VMware application. Once you power on the virtual machine, move the mouse to a point inside the VMware boot screen and left-click until the mouse cursor disappears. At this point, access to the virtual keyboard will be enabled and pressing the 'Esc' key will display the Boot Menu.

VFC will set the boot delay to 3 seconds (3000 milliseconds) to allow easier access to the boot menu. This value can be manually increased further by editing the generated .vmx file and adjusting the value for 'bios.bootDelay'. To allow a 10 second delay, set this value to '10000'.



Once the desired boot option has been selected (or automatically if the boot menu is not accessed) the boot process will continue and either the logon screen will be displayed or, if the user account has not been password protected, the desktop will be displayed.

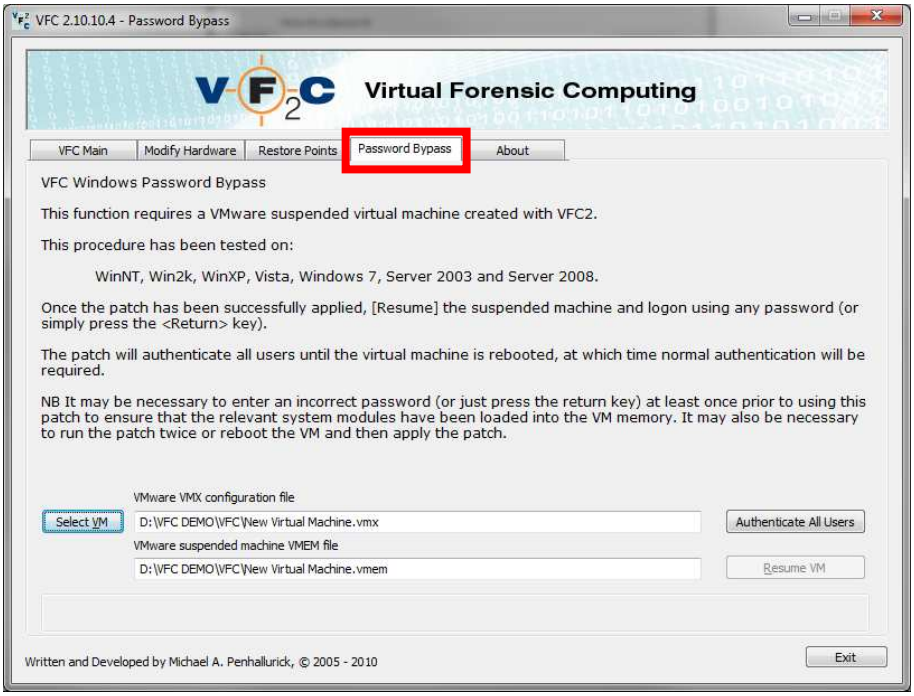




If the user account is password protected, it is possible (on Windows NT & above) to bypass the logon password by utilising the Password Bypass feature.

Password Bypass

VFC incorporates an innovative method of access to user accounts in a virtual environment with the introduction of Password Bypass. Simply suspend the virtual machine when at the logon prompt, use VFC to select the required .vmx file and then 'Authenticate All Users'.



Once the authentication routine is completed, 'Resume' the virtual machine and access the user account without the need of a password.

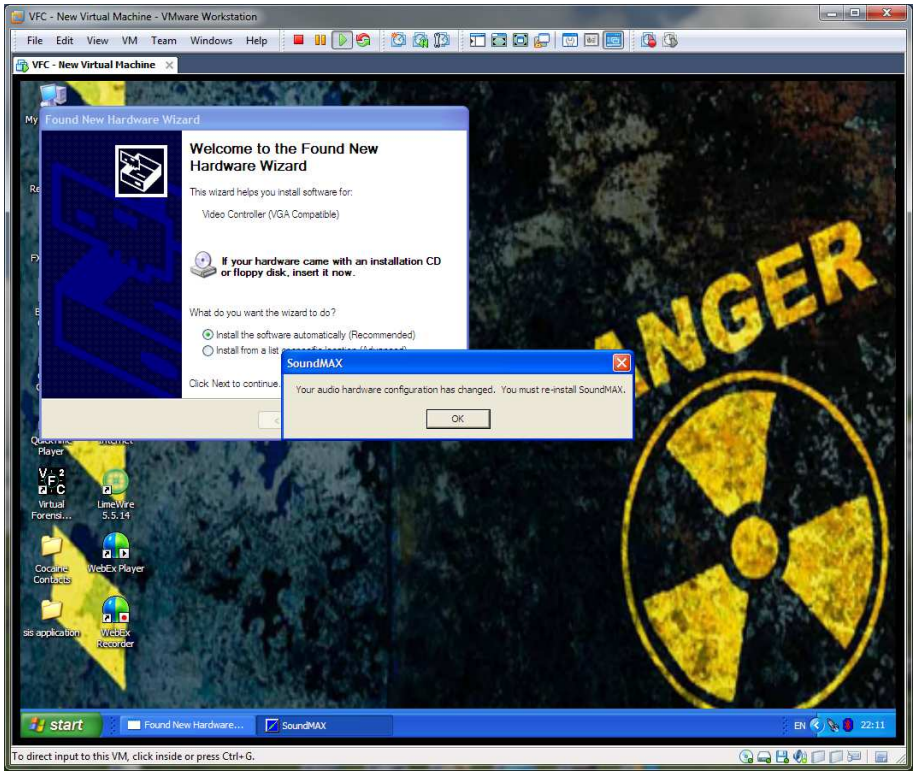
It should be noted that Password Bypass is not a password removal or cracking tool. It is a proprietary routine which works on a single suspended virtual machine session for machines generated by VFC. If the virtual machine is rebooted, memory will be reset and either the password must be utilised or the Password Bypass must be re-applied. No disk files are altered and the effect is merely transitory in nature.

Additionally, Password Bypass will affect all user accounts on the system, whether they are local user accounts or domain user accounts. When Password Bypass has been applied, access will be available to any relevant user profile present on the system.

On occasion, VFC may be unable to successfully patch the virtual memory to enable a password bypass. In these instances, VFC can extract relevant system information which is encrypted into a VFC2.PWB file for return to the author such that additional research can be undertaken. No user identifiable information is stored within the PWB file.

Once you have successfully accessed the desired account, the installed OS will begin to identify new hardware that is detected as a result of the transition to a virtual environment as well as identifying that expected hardware is no longer available.

You will most likely experience a number of message boxes indicating that driver files are being updated/installed. It is likely that certain drivers may not be immediately available, such as the Video Controller (VGA Compatible). Some drivers will become available after the installation of the Vmware Tools package, others (e.g. Sound drivers on Vista and above) may require additional manual installation.

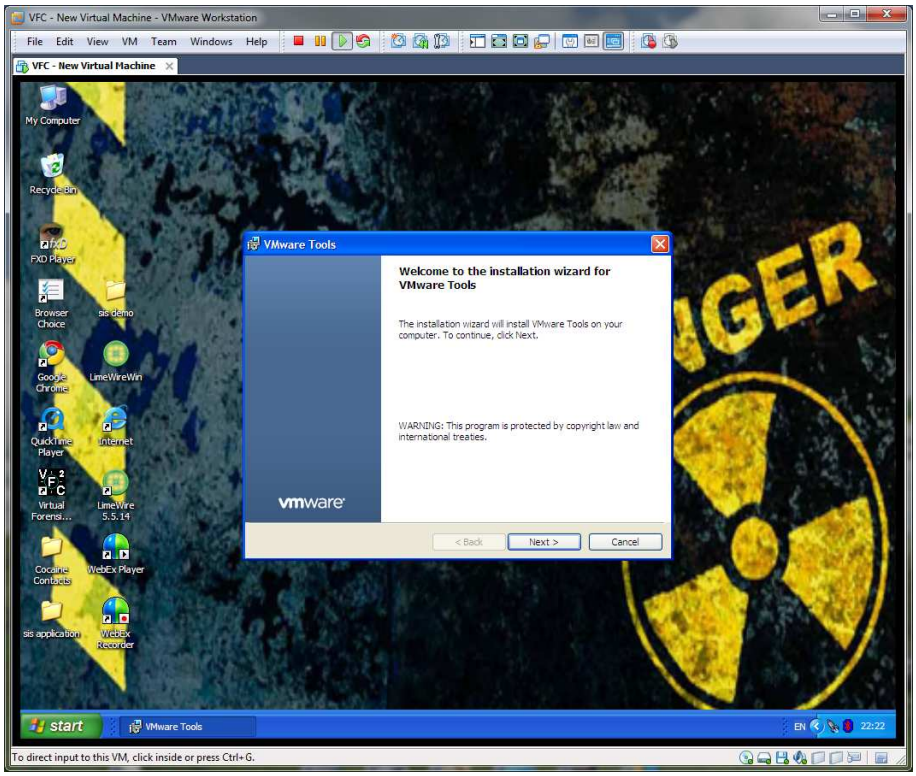


VMware Tools Installation

A typical installation of VMware Tools will provide enhanced graphic control by utilising the VMware SVGA driver as well as better mouse control and the ability to drag and drop between Host and Guest and vice versa.

Whilst the installation of the VMware Tools is described as vital by VMware (and indeed is required for both enhanced user interaction and to most accurately re-create the original environment), it should be noted that the installation procedure will most likely generate a System Restore Point event.

Equally, if rewinding the machine to an earlier point using System Restore functionality, this will effectively remove the installed Tools from the system and they will need to be installed again.



Once the Vmware Tools are installed, it is necessary to restart the machine for configuration changes to take effect.

During the reboot process after installation of the Vmware Tools, the screen resolution may be affected and desktop icons may be re-arranged. It may be possible to adjust screen resolution to the desired final setting prior to the installation of the Vmware Tools. Pre-adjusting resolution may avoid unwanted desktop icon relocation.

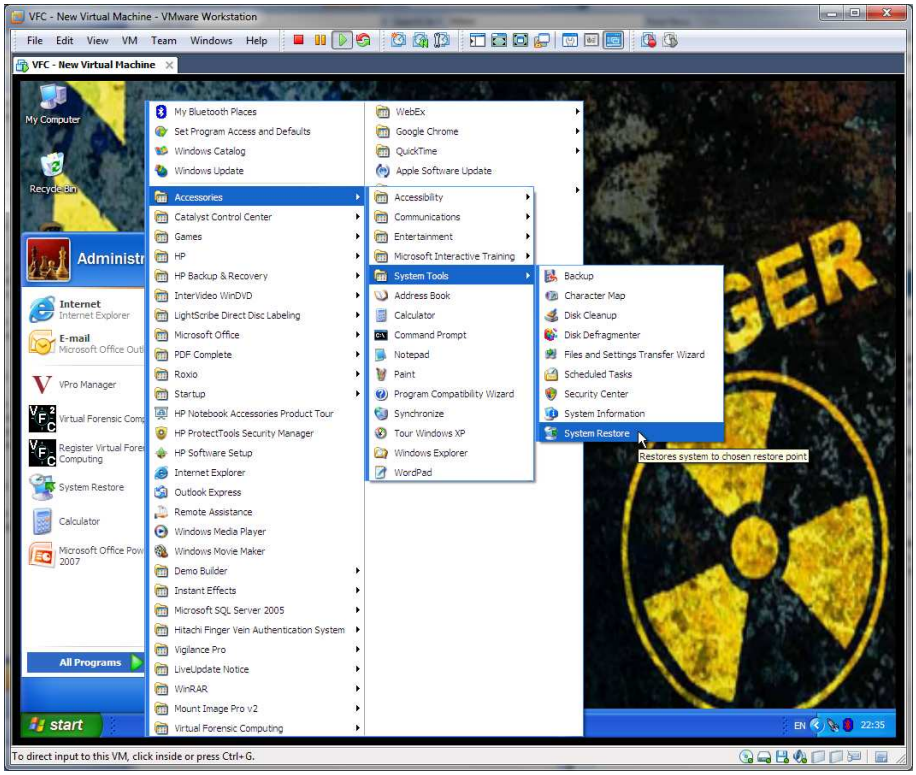
Upon successful reboot (and password bypass if required), you will likely notice a VM tray icon in the lower right of the screen. This can (and probably should) be disabled as it has no direct effect on user data and would not be present on an original machine.

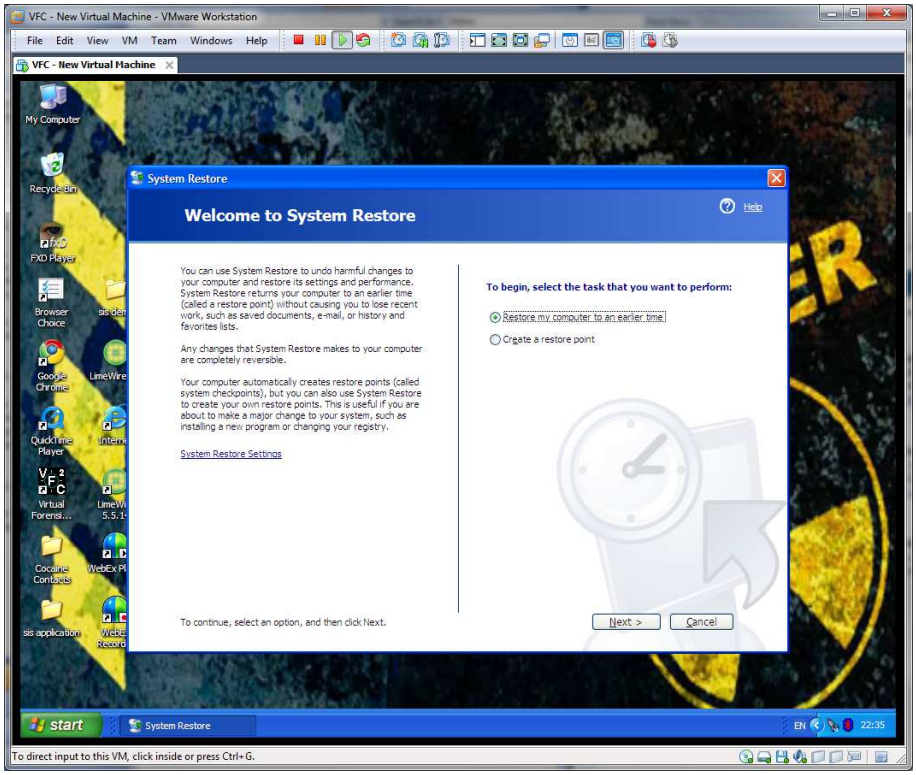
Detailed information about Vmware Tools is available within the VMware Workstation User's Manual on the VMware web-site.

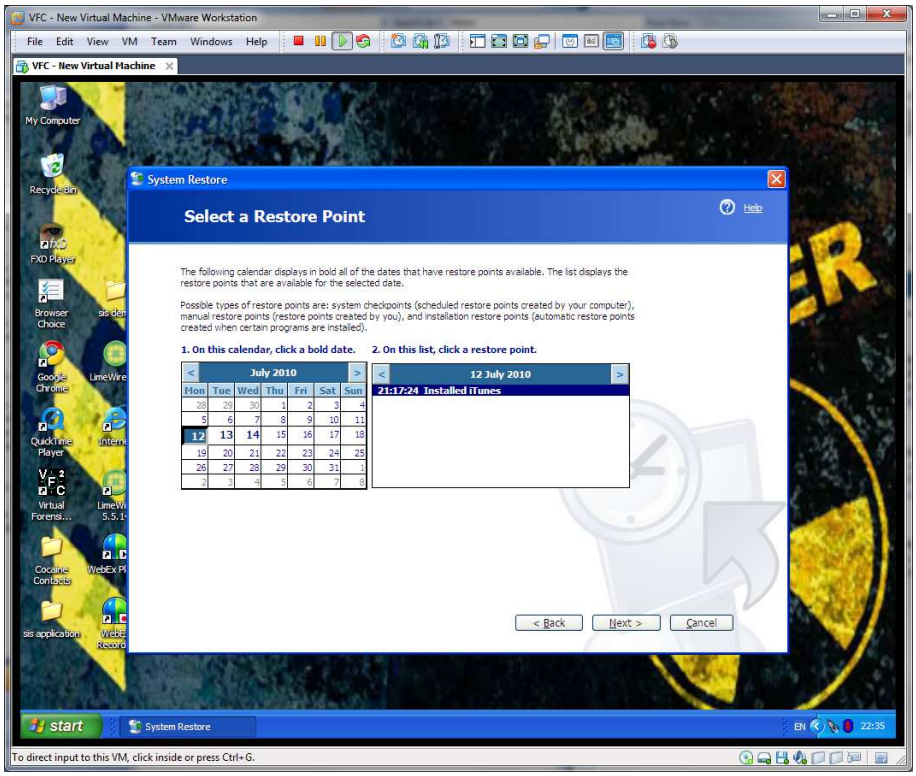
(http://www.vmware.com/pdf/ws71_manual.pdf)

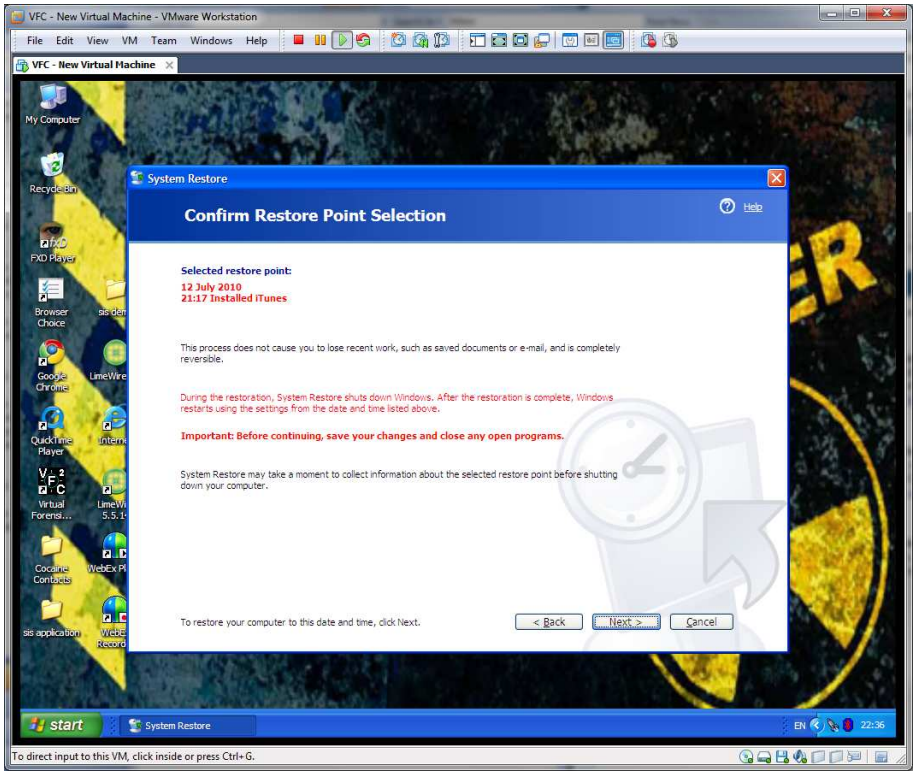
System Restore

It is possible to utilise the in-built System Restore functionality of Windows XP and above to revert a machine to an earlier state.



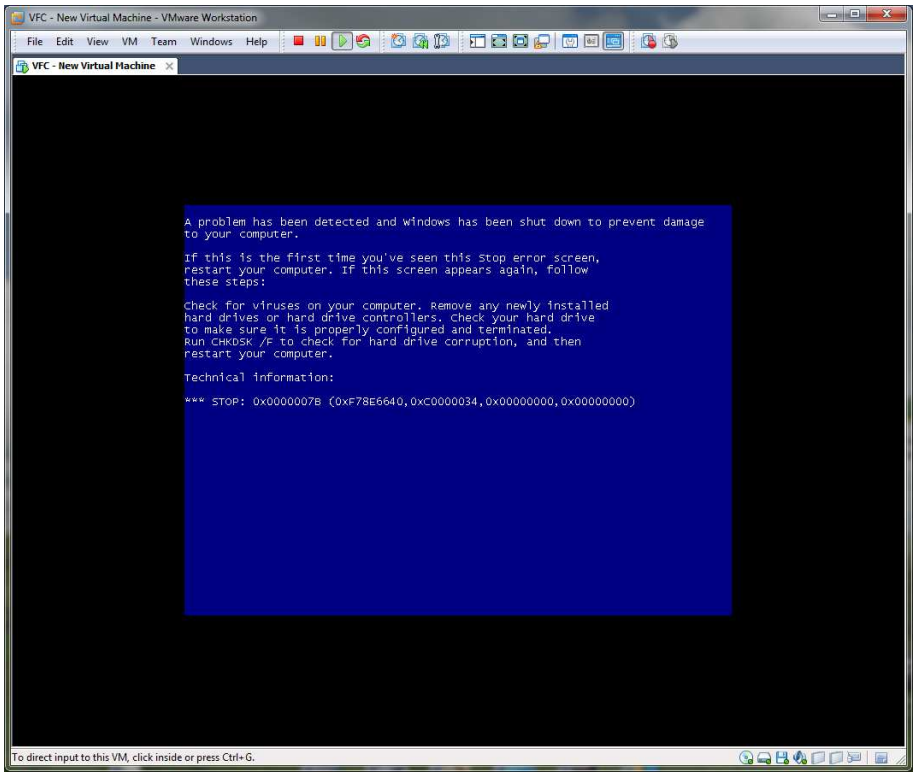




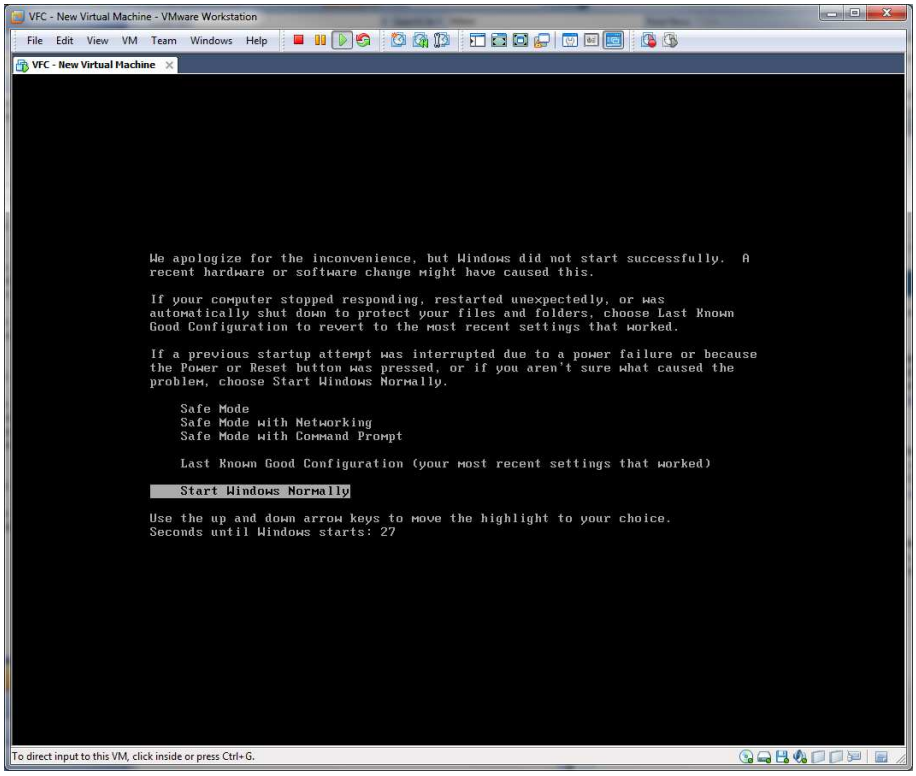


When utilising this functionality, any changes made to the system by VFC and any subsequently installed applications (such as Vmware Tools) will be removed.

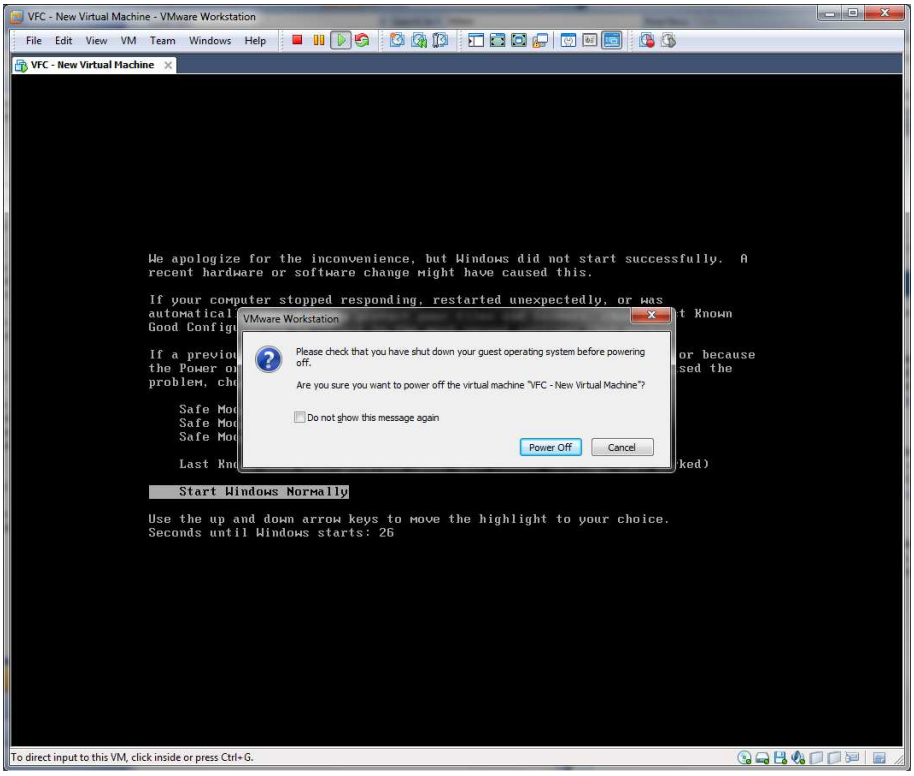
Undoing the VFC changes will cause a 0x7B BSOD (Blue Screen of Death) part way through the process. This is expected behaviour.



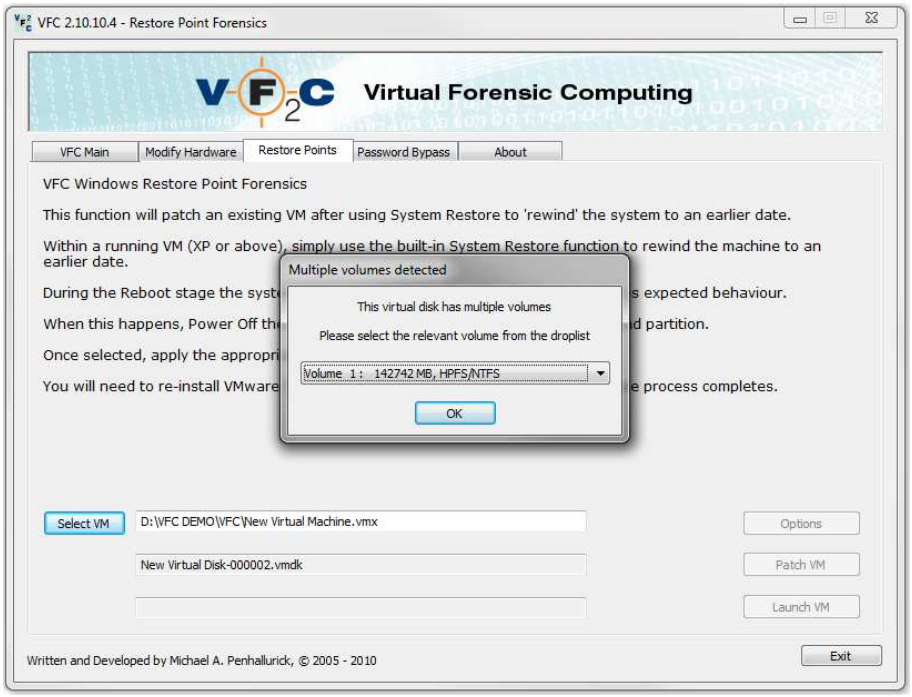
When the system crashes, it will likely go into a cyclical reboot.

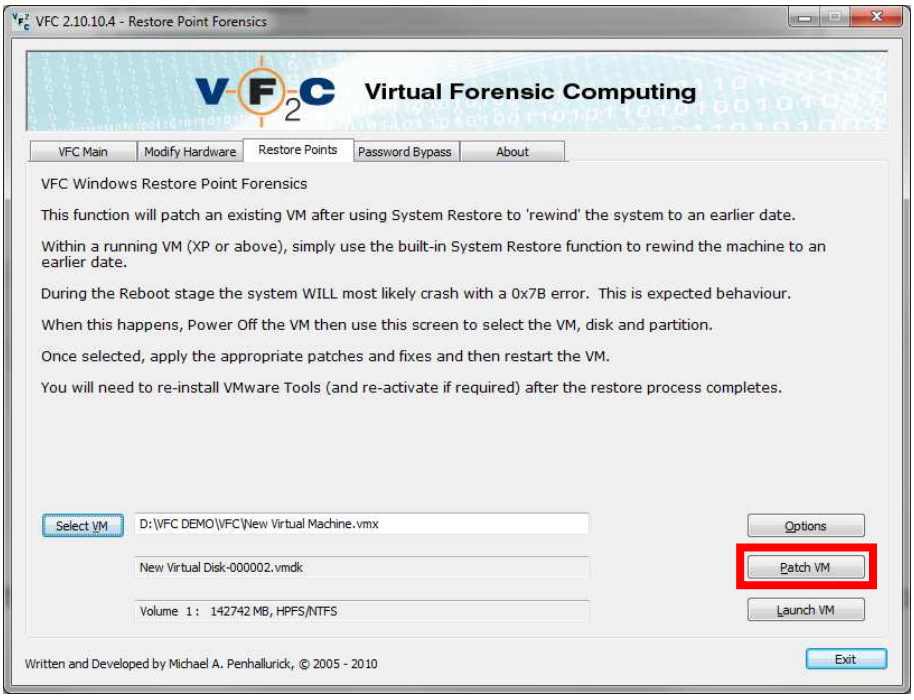


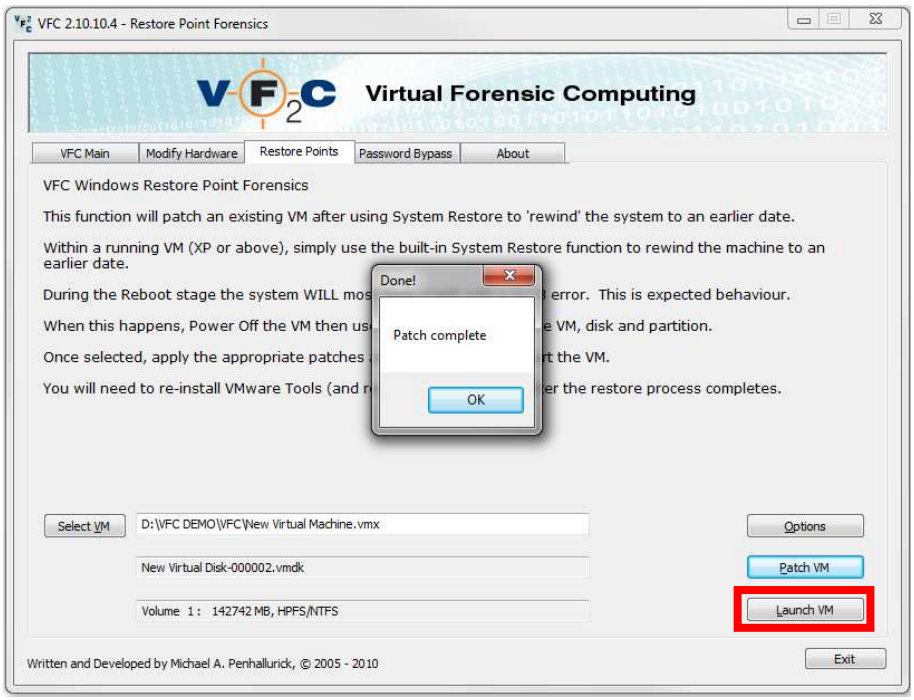
Power off and close (rather than suspend) the Virtual Machine.



Once the VM has been powered off, utilise the Restore Points tab in VFC to re-inject required system drivers and registry settings.



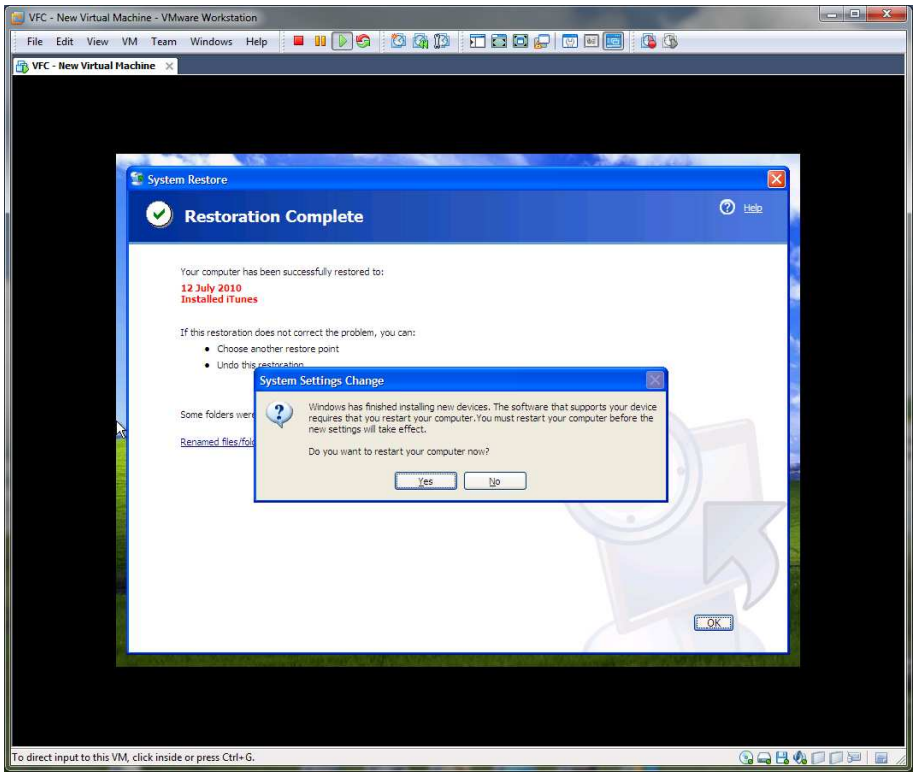


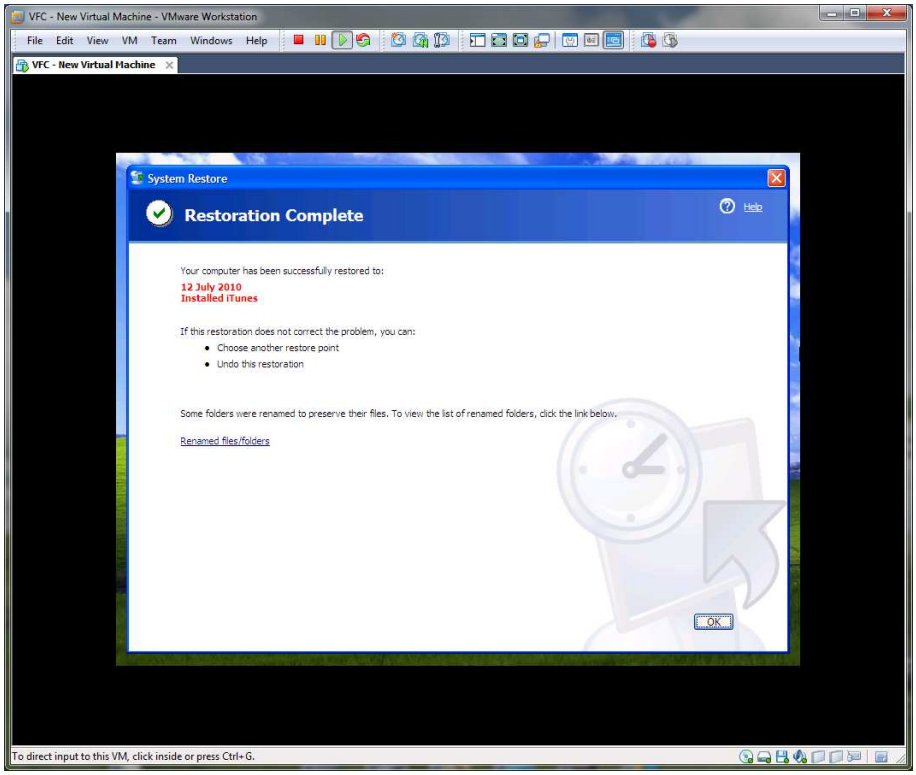


When the machine has been 'patched' you can launch the Virtual Machine and continue the restoration process.

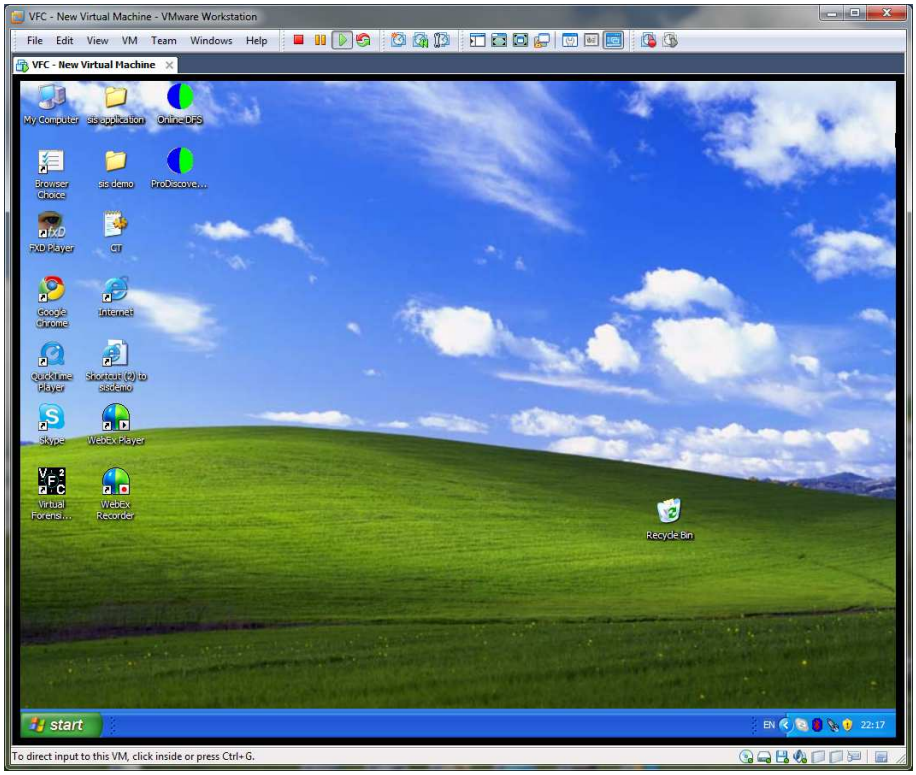
A full restoration to an available restore point may take some considerable time.

When the system completes its boot sequence you may again experience alert messages relating to hardware devices, including requests to restart the computer for new devices to take effect.





Before System Restore on 13 September 2010



After System Restore Point of 12 July 2010

Known Issues & Troubleshooting

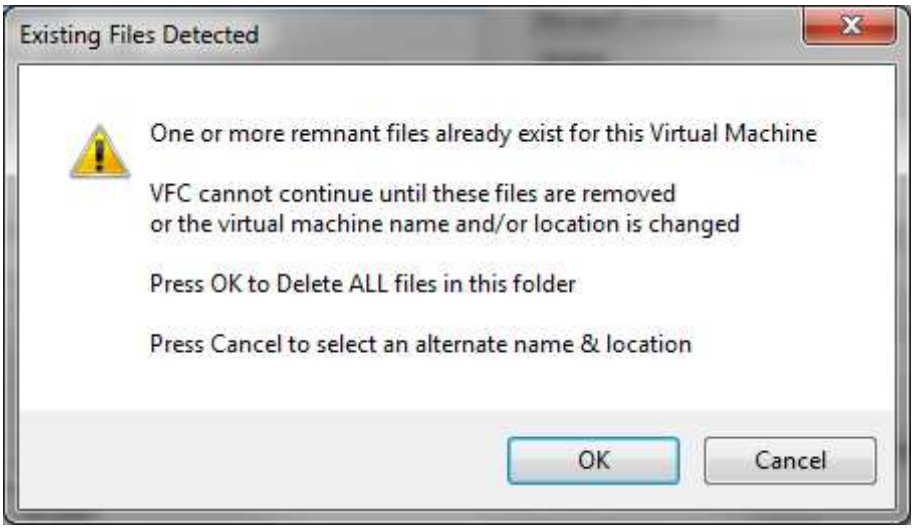
Cannot open the disk

There may be occasions when the VFC generation appears to function seamlessly yet a message similar to that displayed above is encountered when starting the machine.

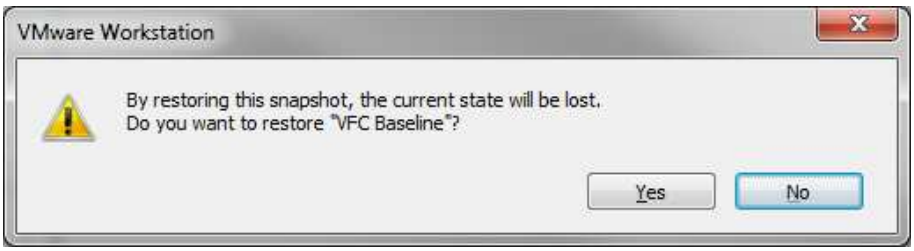
This issue is caused by an inconsistency in the time stamps of the generated virtual disk cache files and has been found to occur most often when Windows Explorer is open during the generation process. This is believed to cause an issue with cleanly dismounting the disk cache via vmware-mount.

There are several methods to resolve this issue if it is encountered.

(i) Regenerate the virtual machine in the same folder, discarding the existing files.

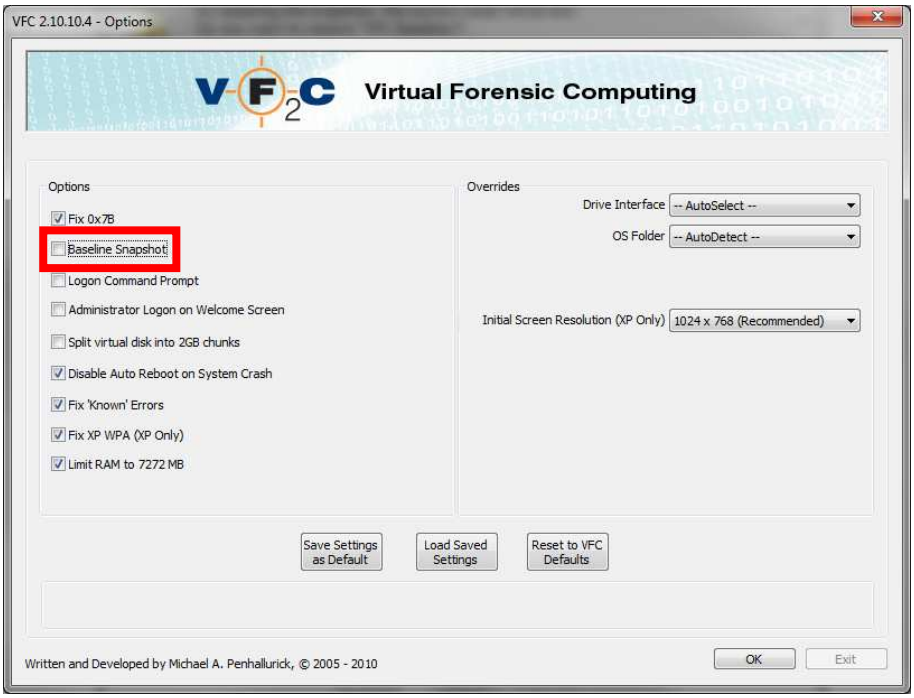


(ii) Revert to snapshot (if using Workstation) – this will flush the latest disk cache and reset the problem time stamps.



(If reverting to snapshot, do the process twice as otherwise the snapshot numbering sequence may latterly fall out of sync.)

(iii) Disable the baseline snapshot option via the Options button on the main dialog screen prior to generating the VFC VM.



Host System is Win7 x64 on a Boot Camp Mac Pro

If you are running Windows 7 x64 on a Boot Camp Apple Mac then this may cause a problem with the vmware-mount utility, (currently a required component of VFC).

Whilst VFC works fine on Windows 7 installed on standard Intel x64 architecture, there is an unknown issue with Windows 7 x64 on Mac hardware which stops vmware-mount from functioning and hence VFC also cannot function correctly.

VFC has been tested with a Mac Mini with Windows 7 x86 and has been found to function as expected.

Cannot run x64 VM even though Host is x64

Running an x64 machine requires VT support in the BIOS of your Host machine. Please make sure that any VT support extensions in your Host BIOS have been enabled and then re-launch the VM.

Please note that VFC will generate the machine regardless – Vmware requires the VT extensions to be active in order to successfully launch the machine in the Vmware environment.

Could Not Unload Registry

There is an intermittent permissions issue (especially with Vista SP1) whereby a subject registry cannot be unloaded from the host system during generation. This will cause the current session to fail and may cause subsequent sessions to also fail. In these instances it is necessary to exit VFC and manually unload any remnant hives.

The resultant VFC VM may not function correctly thereafter but once generated can be re-patched by utilising the Restore Points methodology described above.

CAUTION:

If you make a mistake when you edit the registry, your system might become unstable or unusable. Proceed with caution.

To manually unload any remnant hives which VFC cannot automatically unload, first make sure that the VFC application is closed.

Next, start REGEDIT and expand HKEY_LOCAL_MACHINE.

If there are entries for NEWSYSTEM, NEWSOFTWARE or NEWDEFAULT, these are remnant hives that have not been cleanly unloaded by VFC.

Select the remnant hive and use the menu 'File', 'Unload Hive' to remove the remnant hive from the system.

If the hive still cannot be unloaded, you may need to first restart the system to flush any system locks that are still present.

Once all remnant hives have been removed, exit REGEDIT, dismount any mounted images and restart the system.

To use the Restore Points method on the failed VFC VM, first make sure that any required disk image files have been mounted as previous and then use the 'Open Existing' option from the VFC main dialog to ensure that the PHYSICALDRIVE number allocation is consistent and matches that which VFC has recorded against the VFC VM.

Once 'Open Existing' has verified that the VFC VM is ready to launch, try to 'Launch' the VFC VM. This may result in a 0x7B BSOD. If so use the Restore Points methodology to try to re-inject necessary parameters into the VFC VM.

If the machine cannot be launched with a 'Cannot open the disk' error, follow the steps as above to resolve the snapshot time-stamp issue.

Frequently Asked Questions

Which Disk Formats are supported by VFC?

VFC continues to develop and currently supports:-

- Forensic image files mounted using Mount Image Pro v2, v3 & v4
- Forensic image files mounted using AccessData FTK Imager 3
- Forensic image files disk emulated using Guidance Software Encase PDE (Physical Disk Emulator)
- (write blocked) original physical disks (IDE, SATA, USB, IEEE1394)
- Unix style uncompressed 'dd' images and,
- Vogon format uncompressed 'img' images.

Which Systems can be booted using VFC?

VFC has been used to successfully boot:

- Windows 3.1
- Windows 95
- Windows 98
- Windows ME
- Windows NT
- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Linux (experimental)
- MAC OS X (10.5 and above) (experimental)

What do I need to run VFC?

VFC utilises the freely available VMware Player and VMware Disk Mount Utility, in conjunction with Mount Image Pro to mount forensic images files. VFC requires Windows XP or higher and also requires that you be logged in with Administrator level privileges.

Do I need to have Mount Image Pro or Encase?

No. VFC is wholly capable of using physical disks or 'dd' images.

Mount Image Pro is only required if you have forensic evidence files in the Expert Witness Format which you would like to access outside of any forensic suite.

Encase is only required if you wish to utilise the Encase PDE in order to emulate a physical disk.

How Do I Use VFC?

VFC is as easy to use as 1-2-3:

1. Mount the evidence file (or attach the [write-blocked] physical disk)
2. Select the disk (or dd image) and the relevant partition
3. Generate the machine and use the Launch feature to start it in VMware.

What limitations does VFC have?

VFC will successfully boot 95% of Windows based disks / images it is presented with. VFC cannot dynamically fix machines that are 'broken' and unable to be booted in the original machine. Similarly, VFC cannot bypass software protection that is linked / licensed to the original hardware.

Will booting an image using VFC alter the original evidence?

Not at all. VFC dynamically creates a custom disk cache and directs all subsequent reads and writes 'through' this disk cache. The original evidence is only ever 'read' and cannot be directly written to. Additionally, mounted or emulated forensic image files are opened read-only by default, as are 'dd' and 'img' disk image files.

NB *If you are using physical disks, it is imperative that you use a hardware write-blocking device to connect this disk to your own system, otherwise your system will almost certainly try to write to the physical disk and this will change the evidence.*

Does VFC support partition only images?

Yes. Partition image support is included. Development continues to implement multi-partition image support.

Does VFC support multi-boot systems?

Not at this time. Multi-boot system support is under development.

I've used VFC but still get a BSOD halfway through the boot sequence!

It may be necessary to boot into safe mode and disable services specific to the original hardware, such as:

- NVidia or ATI graphic drivers,
- custom audio drivers or

- OEM specific utilities.

Do I need to install the drivers for the New Detected Hardware?

It is not absolutely necessary to install these drivers, however the virtual machine may not function properly without them and you may find that the CD, mouse or floppy disk (for example) do not function at all. It is recommended that you let the VM detect and install the necessary files.

How can I improve the performance of the New Virtual Machine?

If you are using either VMware Workstation or VMware Server or VMware Player 3 or above, you can install the VMware Tools Package to improve the performance of your virtual machine. This option is not directly available with the standalone Vmware Player 2 or earlier.

Can I access the Internet from the New Virtual Machine?

VFC is designed to be a forensic application and does not add any network support to the New Virtual Machine to ensure it remains isolated from the 'real' world. It is possible to add network support and hence connect to other networks (including the Internet), but this is not recommended.

Can I transfer data between the New Virtual Machine and my own System?

You can use virtual (or real) floppy disks, USB devices and you can even connect a physical data disk as a raw device and write directly to that disk. You can also use CD/DVD media (or ISO files) to read data into the New Virtual Machine.

If Vmware Tools have been installed, you can drag and drop from the VFC virtual machine to your own Host machine and vice versa.

NB Not all of these methods are readily available with the standalone Vmware Player.

Why does the New Virtual Machine need to be activated?

Windows XP and above may require activation due to the number of hardware changes that are inevitable from changing between a physical and a virtual environment. Not all machines can successfully be activated but all machines can be accessed in 'Safe Mode' and this will enable at least a partial interaction with the original desktop.

Can I create additional Snapshots?

Yes, VFC allows the VM to create multiple snapshots. Snapshot creation is dependant upon the version of Vmware being utilised.

What does VFC actually do?

VFC creates a disk cache that is used by Vmware to intercept any changes to the underlying original disk, whether this is a physical device, mounted forensic image or a full bit-for-bit image file.

VFC makes the minimum necessary modifications via the disk cache in order to ensure that it can successfully boot in a virtual environment.

The whole ethos behind VFC is to keep the underlying image as close as possible to the original and yet still make it function in VMware. In situ upgrades, which are advocated as one method of achieving the same goal, were deemed too intrusive of the 'forensic' process.

The Creator of VFC

Michael Penhallurick

Michael Penhallurick holds a Master of Science Degree in Forensic Computing from the Royal Military College of Science / Cranfield University and was a regular visiting lecturer at that establishment between 2002 and 2005. He has also been involved in the development of training packages with the National Specialist Law Enforcement Centre Hi Tech Crime Training Team.

Michael joined MD5 Limited in November 2006 having previously served as a Police Officer with the South Yorkshire Police for almost 13 years, the last four years of which were as Computer Forensic Manager for their Hi-Tech Crime Unit. He also undertook a year as Computer Forensics Manager in a corporate environment for The Risk Advisory Group based in the centre of London.

In both roles he was responsible for undertaking and overseeing major criminal investigations for a variety of criminal activities ranging from indecency through to fraud and murder. He was also responsible for ensuring the smooth day-to-day running of the unit including staff development and identification of training needs, as well as liaison with external agencies such as the Crown Prosecution Service, the Probation Service and the Courts and regular client conferences.

Michael has been involved in computing in general since 1986 and prior to joining the Police Service, he lived and worked in Dubai, United Arab Emirates, working as a freelance computer systems consultant for both small and large businesses including financial advisors, several oil companies, an aerial survey company, the Dubai Ports Authority and the Government of Dubai Water Department.

Michael Penhallurick has been involved in Forensic Computing since 1997 and has had extensive training and first hand use of the Vogon, Encase, AccessData and iLook suites of forensic tools.