User Guide

VFC 5.0

VFC is a registered trademark of MD5 Ltd

Copyright © 2007-2019 MD5 Ltd

Acknowledgments

All rights reserved.

The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by MD5 Ltd.

MD5 Ltd assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is furnished under license on a subscription basis and may only be used or copied in accordance with the terms of such license. VFC will cease to function once the subscription period expires.

VFC® and the VFC logo are registered trademarks of MD5 Ltd.

VMware® is a trademark of VMware, Inc. and may be registered in certain jurisdictions.

Microsoft® and Microsoft® Windows® are trademarks of Microsoft Corporation that may be registered in certain jurisdictions.

All other products or name brands are trademarks of their respective holders and are acknowledged.

Contact Details

Address: MD5 Ltd, PO Box 96, Normanton, West Yorkshire, WF6 1WY, United Kingdom
Phone: +44 (0) 1924 220 999
Sales: sales@md5.uk.com
Support: support@md5.uk.com

VFC5 Technical Requirements

PC running Windows 7 SP1 or later *
1024×768 resolution display or higher
Minimum 100MB free space (in practice lots more will be required for VMs)
VMware Workstation Pro/Player v12 or later
Full Admin permissions to install VFC and mount/unmount images
VFC Mount (provided) or appropriate third-party mount tool
USB port (for dongle)

* It is also possible to run VFC on an Apple Mac computing using BootCamp. We understand that this may work well but are unable to formally support this at this time

Table of Contents

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Virtual Forensic Computing

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

End-User License Agreement (EULA) of Virtual Forensic Computing (VFC)

This End-User License Agreement ("EULA") is a legal agreement between you (“You” or “User”) and MD5 Ltd

This EULA agreement governs your acquisition and use of Virtual Forensic Computing (hereafter “VFC”) software ("Software") directly from MD5 Ltd or indirectly through a MD5 Ltd authorized reseller or distributor (a "Reseller").

Please read this EULA agreement carefully before completing the installation process and using the VFC software. By pressing the “I Agree” button you enter into the terms of this binding contract between you and MD5 Ltd and it validates a license to use the VFC software and contains warranty information and liability disclaimers and constitutes acceptance of the terms of this License Agreement

If you do not agree with the terms of the license, Choose the “I Do Not Agree” button and/or exit the installation of VFC.

If you are entering into this EULA agreement on behalf of a company or other legal entity, you represent that you have the authority to bind such entity and its affiliates to these terms and conditions. If you do not have such authority or if you do not agree with the terms and conditions of this EULA agreement, do not install or use the Software, and you must not accept this EULA agreement.

This EULA agreement shall apply only to the Software supplied by MD5 Ltd herewith regardless of whether other software is referred to or described herein. The terms also apply to any MD5 Ltd updates, supplements, Internet-based services, and support services for the Software, unless other terms accompany those items on delivery. If so, those terms apply.

License Grant

MD5 Ltd hereby grants you a limited, non-transferable, non-exclusive license to use VFC software on your devices in accordance with the terms of this EULA agreement.

You are permitted to load the VFC software (for example a PC, laptop, mobile or tablet) under your control. You are responsible for ensuring your device meets the minimum requirements of the VFC software.

You are not permitted to:

- Edit, alter, modify, adapt, translate or otherwise change the whole or any part of the Software nor permit the whole or any part of the Software to be combined with or become incorporated in any other software, nor decompile, disassemble or reverse engineer the Software or attempt to do any such things
- Reproduce, copy, distribute, resell or otherwise use the Software for any commercial purpose
- Allow any third party to use the Software on behalf of or for the benefit of any third party

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

- Use the Software in any way which breaches any applicable local, national or international law
- Use the Software for any purpose that MD5 Ltd considers is a breach of this EULA agreement

VFC Usage

VFC is licensed for legitimate investigatory purposes only.
By accepting this agreement, the user is confirming that they are:

1. Using VFC in compliance with the laws of your jurisdiction.
2. Using VFC for a legitimate investigatory purpose
3. Accepting responsibility for compliance with third party software licenses and have permission to use third party software for investigatory purposes

Support

MD5 Ltd reserves the right to modify the Software from time to time without obligation to notify you, or any other person or organization of such revision or change.

Intellectual Property and Ownership

MD5 Ltd shall at all times retain ownership of the Software as originally downloaded by you and all subsequent downloads of the Software by you. The Software (and the copyright, and other intellectual property rights of whatever nature in the Software, including any modifications made thereto) are and shall remain the property of MD5 Ltd.

MD5 Ltd reserves the right to grant licenses to use the Software to third parties.

Limitation of Liability

IN NO EVENT WILL MD5 LTD BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOST OPPORTUNITY OR PROFITS, COST OF COVER OR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, DIRECT OR INDIRECT DAMAGES ARISING FROM OR RELATING TO THE USE OF THE SOFTWARE, HOWEVER CAUSED ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF MD5 LTD HAS BEEN ADVISED OR GIVEN NOTICE OF THE POSSIBILITY OF SUCH DAMAGE. THE ENTIRE RISK AS TO THE USE OF THE SOFTWARE IS ASSUMED BY THE USER. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CERTAIN INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES, THIS LIMITATION MAY NOT APPLY TO YOU.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Disclaimer of Warranty

TO THE EXTENT PERMITTED BY APPLICABLE LAW ALL MD5 LTD SOFTWARE, INCLUDING THE IMAGES AND/OR COMPONENTS, IS PROVIDED "AS IS" AND WITHOUT EXPRESS OR IMPLIED WARRANTY OF ANY KIND BY EITHER MD5 LTD OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF SUCH SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE. NO COVENANTS, WARRANTIES OR INDEMNITIES OF ANY KIND ARE GRANTED BY MD5 LTD TO THE USER.

Government Rights

If used or acquired by the Government, the Government acknowledges that (a) the Software constitutes "commercial computer software" or "commercial computer software documentation" for purposes of 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-3, as applicable and (b) the Government's rights are limited to those specifically granted to you pursuant to this License. The contractor/manufacturer is MD5 LTD, PO BOX 96, Normanton, West Yorkshire, WF6 1WY, UK.

Termination

This EULA agreement is effective from the date you first use the Software and shall continue until terminated. You may terminate it at any time.

It will also terminate immediately if you fail to comply with any term of this EULA agreement. Upon such termination, the licenses granted by this EULA agreement will immediately terminate and you agree to stop all access and use of the Software. The provisions that by their nature continue and will survive any termination of this EULA agreement.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Overview of VFC

VFC (Virtual Forensic Computing) is a forensic application designed to handle a variety of hard disk drive sources (physical disk, bit-for-bit disk copy or 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. This mounted disk is read-only and cannot be directly modified.

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 'ACTIVE' will be the one containing the Operating System. With certain systems (such as Windows Vista and above) the ACTIVE 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.

For Windows Operating Systems, once the required partition is selected, VFC default behaviour is to analyse the OS by querying registry data, the SAM file and system files. The resultant information 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 of the VFC VM. If building a VM with multiple drives, it can be prudent to change the name of the Virtual Disk so that the boot disk is easily recognisable for other features such as password bypass.

Once the VFC VM has been generated, the launch facility is enabled and the machine can be booted into a virtual environment. VFC 4.50 introduced the Launch Now/Later pop-up to speed up the launch process & prompt the user to consider additional steps prior to launch (e.g. modifying the hardware).

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. Installing VMware tools will resolve a lot of minor issues surrounding screen resolution and mouse compatibility and will enable files to be copied out to the host system.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

If a logon password is required but not known, the machine can be suspended and the VFC Password Bypass (PWB) routine can be utilised for local Windows User Accounts. This works on systems that our Development Team have encountered and have thus developed the Bypass Routine for. If a routine does not exist, recent versions include a Fuzzy Logic search feature – here, VFC will try multiple alternative PWB routines in case another one works. This will increase the chance of success with bypassing the password on that system but will take longer. Please note, the PWB process only works on local user accounts and does not currently work on PIN protected devices or domain/online authenticated accounts.

The PWB process works by patching the virtual memory file so it can also be used on VMs found or built outside of VFC provided they have been launched and suspended. Please note, if a bypassed system is restarted or powered down for any reason, the PWB will need to be reapplied.

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 VFC VM generation had implemented and the system will therefore (most likely) fail to boot from a restored session. This is expected behaviour and VFC contains a 'fix' for this. Simply power off the VFC VM and utilise the Patch VM/Restore Point Forensics feature to reinject the necessary system drivers and thus enable a successful boot to the required System Restore Point.

This 'fix' can now be applied to any VM that is failing to boot and when utilised, VFC will endeavour to make the necessary changes to the VMX configuration to get past the impediment.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Installation of VFC and associated applications

VFC was originally developed to automate and expedite the steps required to create a functional working VMware Virtual Machine (VM) (primarily) from a mounted Expert Witness Format (EWF) file.

By nature of the way it interacts with evidence files on a physical disk level, users of VFC **must** have full Administrator level access and privileges for the program to work effectively. Not having these privileges will stop VFC from working correctly – this is caused primarily by disk access rights.

As indicated above, one of the required components of this methodology is access to and use of the VMware Virtualisation platform. The recommended platform is VMware Workstation Pro, as this application provides additional functionality over other available VMware desktop platforms, which the end-user investigator may find useful.

VFC can create VM's that will work with VMware Workstation Player and VMware Workstation Pro. Workstation Player has fewer features enabled but is free for non-commercial use. Both products require registration and if used as part of work for an agency, unless otherwise agreed with the vendor, attract a modest annual licence fee. On their evaluation version download site, VMware state the following*:

> *"The free version is available for non-commercial, personal and home use. We also encourage students and non-profit organizations to benefit from this offering.*
>
> ***Commercial organizations require commercial licenses to use Workstation Player."***
> **correct at time of going to print 27/06/2019*

Another component required in order to successfully use VFC is the VMware mount utility which is deployed within the VMware VDDK (Virtual Disk Development Kit – v5.1.4 is supplied in the VFC Setup file). The VMware mount utility is used to mount a specific volume of a virtual disk (via snapshot files) so that access can be gained to the file system in a forensically sound manner.

Historically, VFC was used – and developed – with images mounted using third-party mounting tools such as Access Data's FTK Imager, Guidance Software's EnCase Physical Disk Emulator (PDE) or GetData's Mount Image Pro (MIP). FTK Imager and MIP can now be quickly launched using buttons found in the GUI of VFC5. Other 3rd-party utilities may also be available but these have not been tested by MD5 Ltd.

VFC5 now includes its own VFC Mount utility which is preconfigured with the most commonly required mount settings. The VFC Mount tool is a separate program that will keep running once VFC is closed to support any open VMs based on the current mounted volumes. The program can be opened (and the volumes unmounted) via the icon in the Windows notification area (system tray).

VFC5 also includes integration components for use with third-party forensic analysis tools including EnCase and X-Ways Forensics. These can be used to simplify the process of mounting the current case files into VFC Mount and then automatically launching VFC.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

NB: VFC utilises a mounted physical disk, a 'real' physical disk or a raw, bit-for-bit, and 'dd' image. The VFC Method and the VFC application were originally developed utilising MIP and latterly, FTK Imager. VFC Mount is a step away from reliance upon these third-party tools and has allowed us to deliver enhanced command line integration with forensic analysis tools, and crucially for the front-line user, reduce instances of the Physical Disk In Use (PDIU) error.

In the early years of development, there were mixed reports with using FTK Imager in that some images would not virtualise unless mounted with MIP. MD5 have not seen any evidence of this in later releases and given the price differential, if greater control over mounting settings is required, MD5 now recommend FTK Imager.

Please note, if using Encase PDE, the end-user is limited to mounting a single disk at a time so building multi-drive VMs from image files will not be possible.

It has been found that the best method of installing VFC and other required applications when using a Windows 7 host system is by right clicking the relevant executable and selecting 'Run as Administrator' from the subsequently displayed context menu. User Access Control (UAC) can cause occasional issues and it can help if this is disabled on the forensic investigator's host system; however, this is a decision left entirely up to the investigator. VFC and all associated applications (VMware, mounting tools, VDDK) should be installed with full administrator privileges.

VFC and VFC Mount must be run with administrator privileges. Both tools will prompt you to launch with admin. rights and cannot be used from a non-admin user account.

The following instructions describe how to install VFC5, VMware Workstation and VDDK.

Installation of VFC

VFC5 utilises an MSI Installer package.

Installation instructions with links to the latest download locations for supporting software are available on request from support@md5.uk.com.

VFC License Manager and the latest PWB5.BIN file can be found at vfc.uk.com/downloads. You will need to download License Manager and have a valid VFC dongle to be able to download VFC5.

The "Download Updates" button within License Manager will be activated if a current, valid VFC dongle is detected. Clicking on "Download Updates" will take you to a web page of downloads relevant to you (e.g. the latest version of VFC5). For full instructions, see overleaf.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

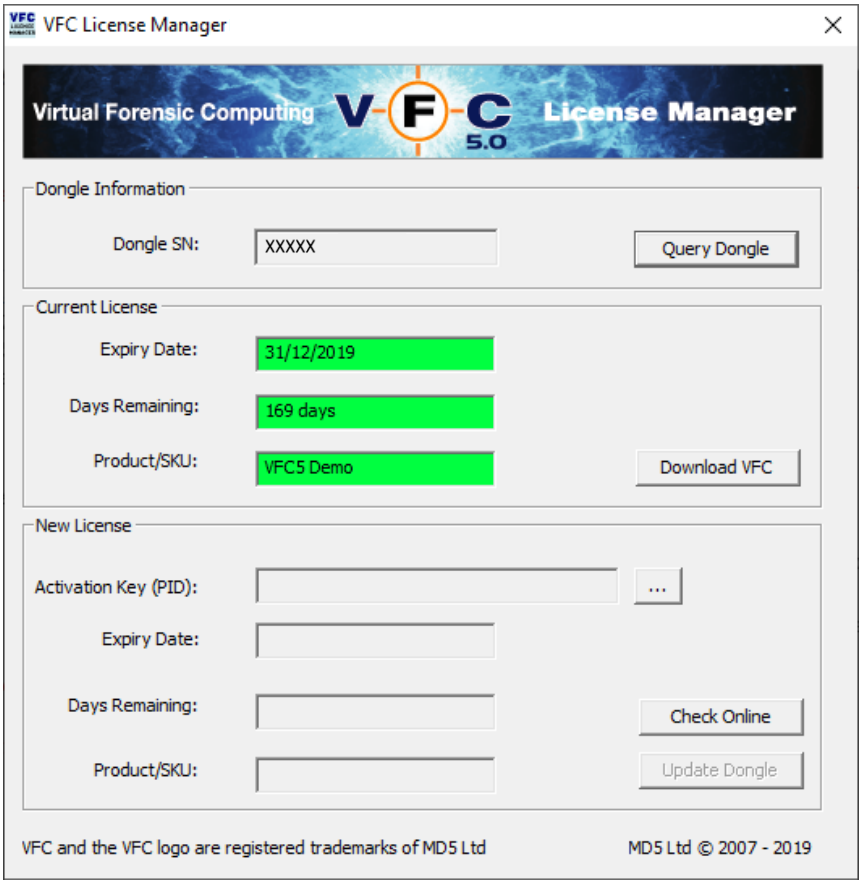
Downloading the Latest Version of VFC

NB *To download the latest VFC release, you must have access to either a valid VFC dongle or a direct download link from our sales team.*

Please proceed as follows:

1. Check your dongle is correctly connected (and driver installed if using a green dongle)

2. Start **VFC License Manager**. This is included with the installation package for VFC and is also available for standalone download from https://vfc.uk.com/downloads



3. Click “Query Dongle”

4. Confirm you have a current VFC license (shown in green). If you do not have a current license please contact Technical Support

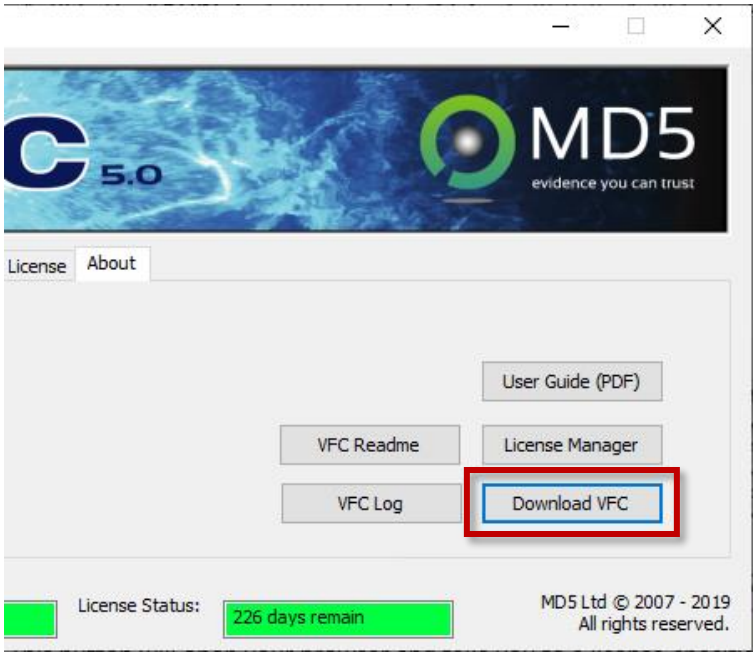
   NB *If the Product/SKU displays “[Legacy]”, please update your dongle first*

5. Click “Download VFC”

6. Follow the on-screen instructions (see next page)

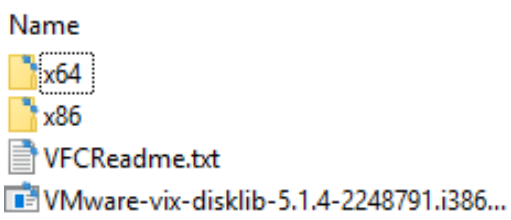
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

You can also download VFC from within VFC, using the “Download VFC” button on the “About” tab:



This button will open your browser and take you to a license-specific download link. Please ensure you are connected to the internet, click the “Download VFC” button and follow the onscreen instructions.

The downloaded file will contain folders for both 32-bit and 64-bit installations. We recommend that the 64-bit (x64 folder) installation is used for 64-bit systems. While the 32-bit version (x86 folder) will work on a 64-bit system, this is designed for use on older systems and will eventually be phased out:

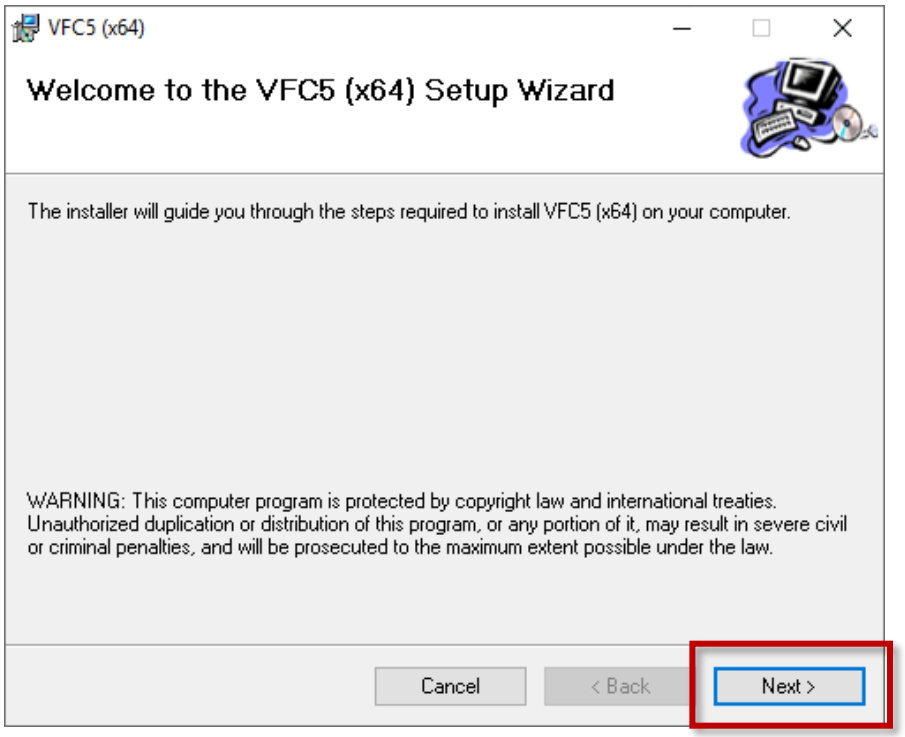


It can help to extract the contents to your host system before continuing. The MSI installer will put the requisite shortcuts onto your system and will also ensure all the ancillary components that are required are installed and made available as expected.

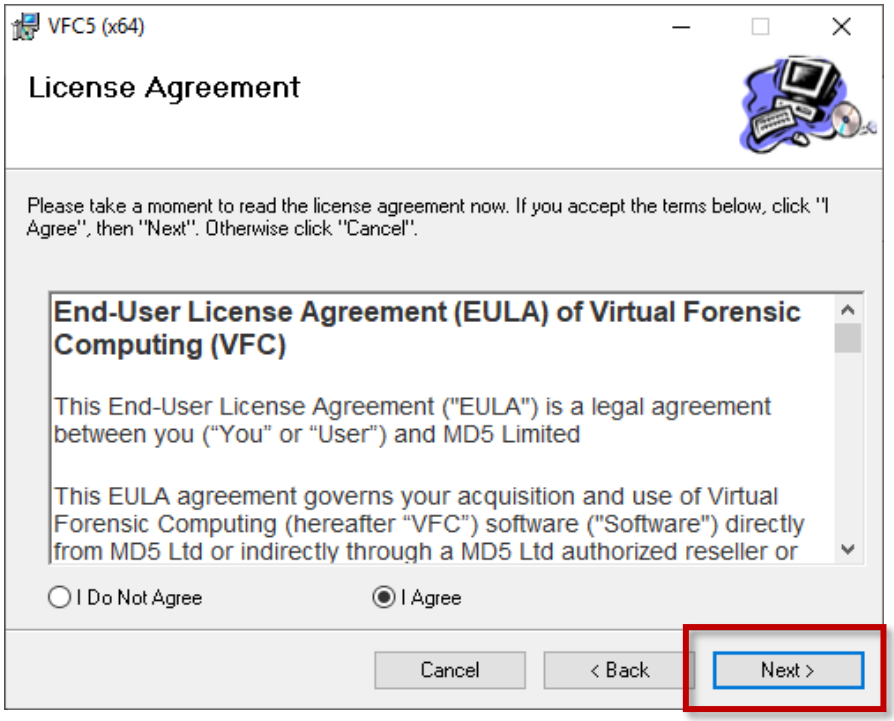
Both versions offer the same features.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

In File Explorer, navigate to the location where you have saved the extracted installation files, right-click on the “VFC5 Setup v5.X.X.XXXX x64.msi” file and select ‘Run as administrator’.

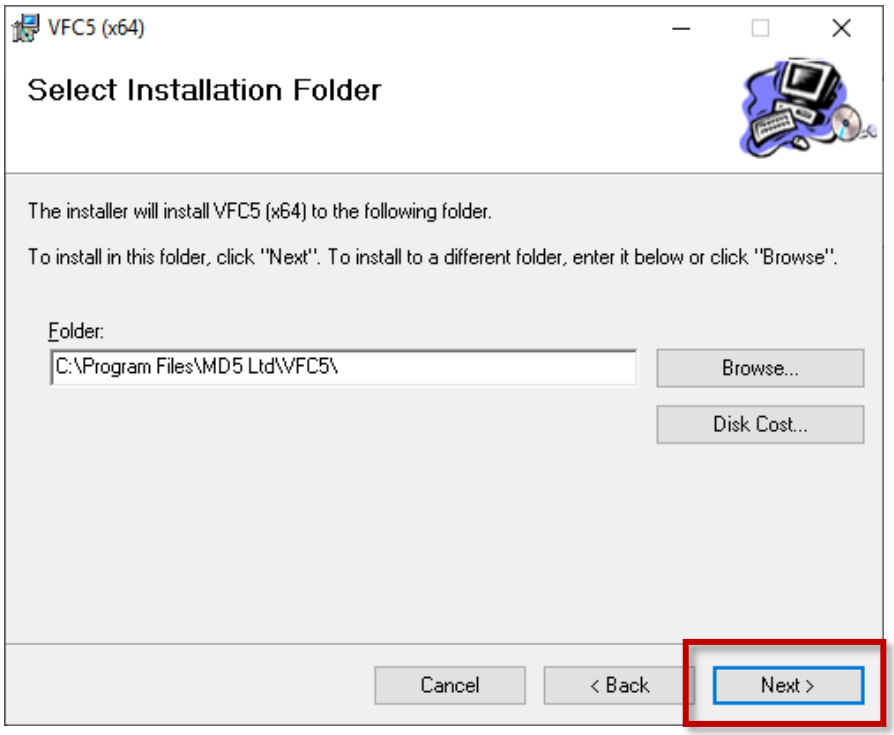


Click ‘Next’ and then accept the End User License Agreement:

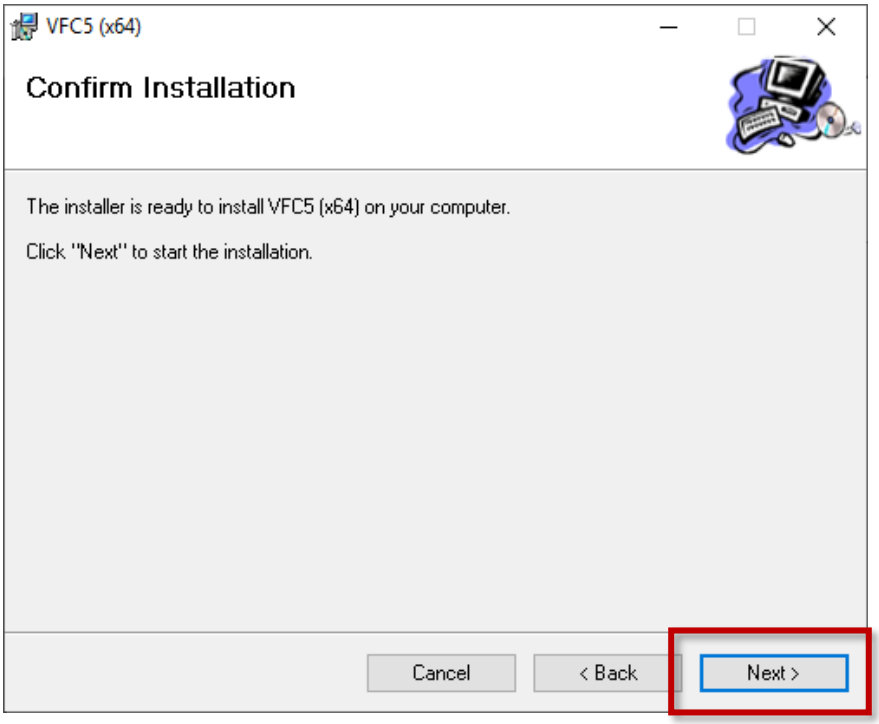


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Click ‘Next’ and specify the location for installation or accept the default name and location. The default location will either be “Program Files” or “Program Files (x86)” depending on your Windows platform. It is recommended that you accept the defaults. Choose who should have access to the program following installation and click ‘Next’ to proceed:

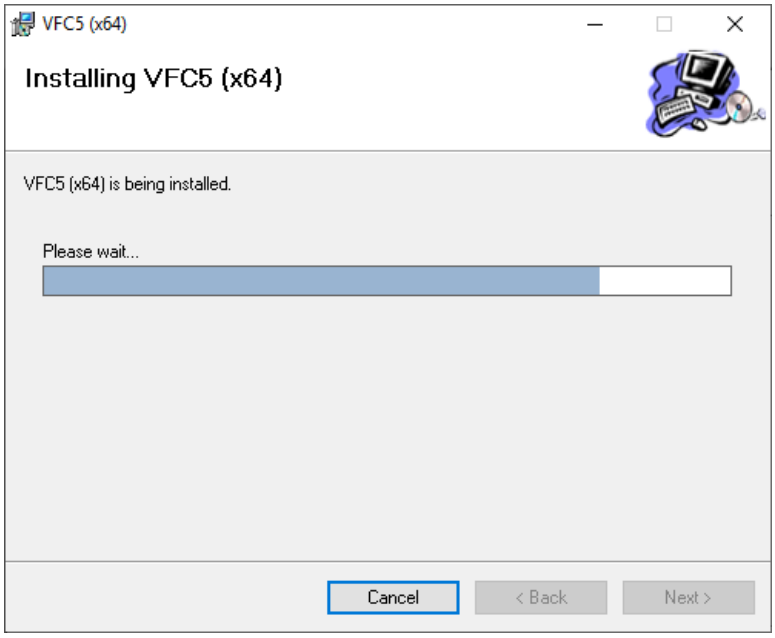


Click Next again to install the program:

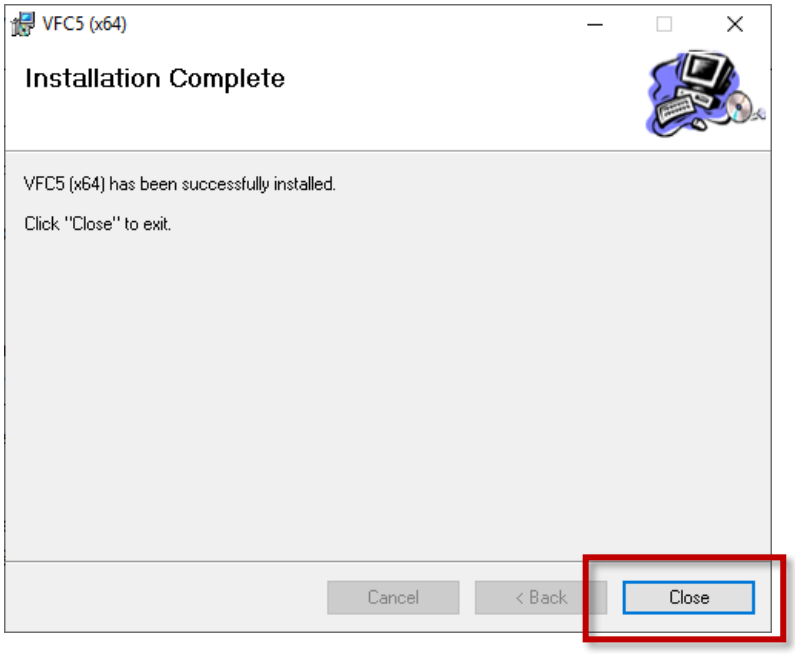


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Wait…

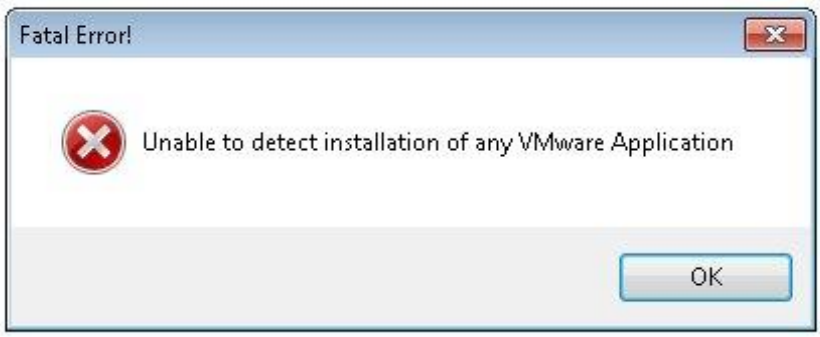


Close the installer and you're ready to go:

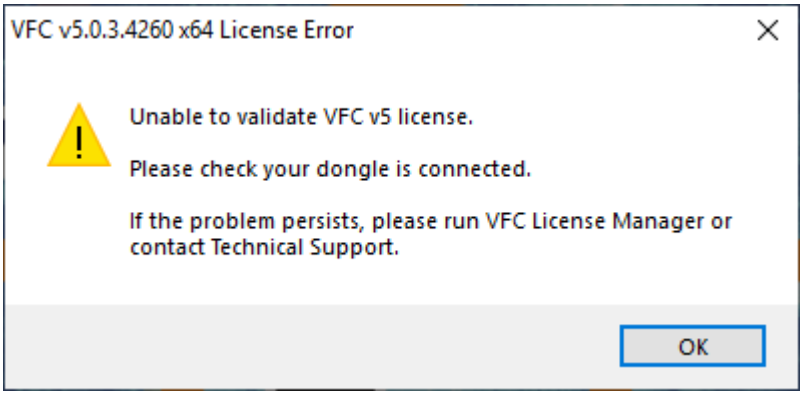


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

You will need to install both a VMware Workstation desktop product and the VMware VDDK before VFC can be utilised. If either of these applications is not present, VFC will fail to start with the following error message:



If no dongle is present (or the correct dongle drivers have not been installed – see next section) or your dongle does not contain a VFC v5 license you will see this message:



To resolve this problem, please open VFC License Manager and check for an updated license. See the following sections on Installing the Dongle Driver (Green Dongle Only) and License Manager for more information.

If this still fails or you have yet to purchase a v5 license, please contact MD5 Sales/Technical Support.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

The VFC Standalone Dongle and Dongle Drivers

You will need to have a VFC dongle inserted to run VFC.

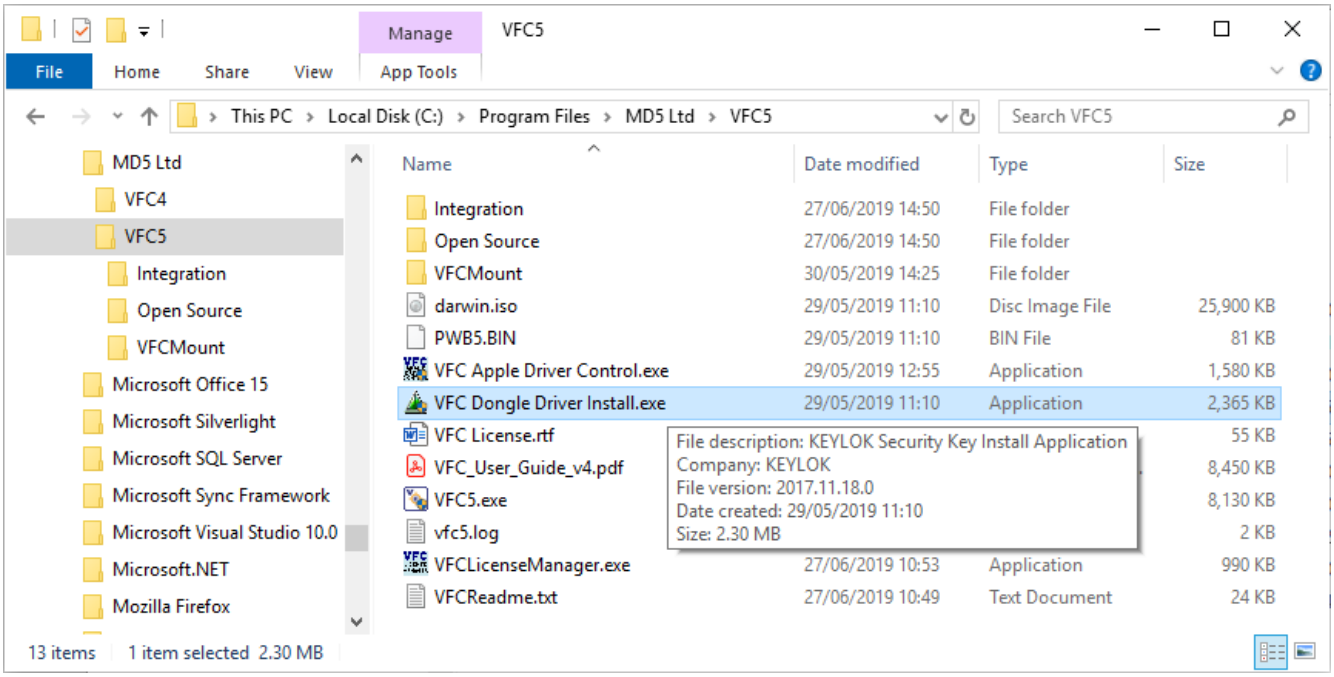
VFC supports two different types of dongle. Older licenses typically used a Green dongle. This requires drivers to function (please see below).

More recent licenses use a White dongle. This does not require any drivers.

Installing the Dongle Driver (Green Dongle Only)

To run VFC with a Green dongle, you will need to install the required dongle drivers using the VFC Dongle Driver Install executable which is located either in your installation folder.

With VFC5, the installation folder is located in either:
Program Files>MD5 Ltd>VFC5 or **Program Files (x86)>MD5 Ltd>VFC5**



You must remove the dongle from the Host machine prior to installing the dongle drivers.

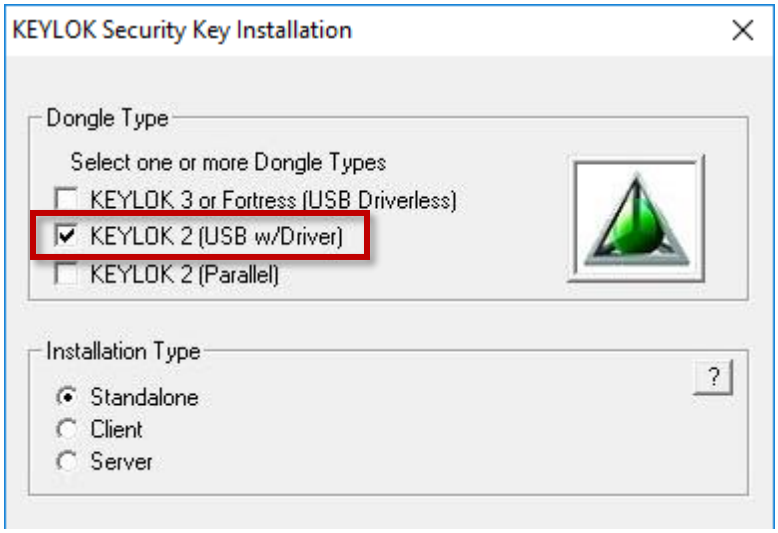
The Dongle Driver Installation should be run as an administrator. Right click on the appropriate executable and select 'Run as administrator'.

You will be presented with installation options. VFC5 is only designed to work as a standalone license. Old Green dongles should be installed as 'KEYLOK 2 (USB w/Driver)' and 'Standalone'.

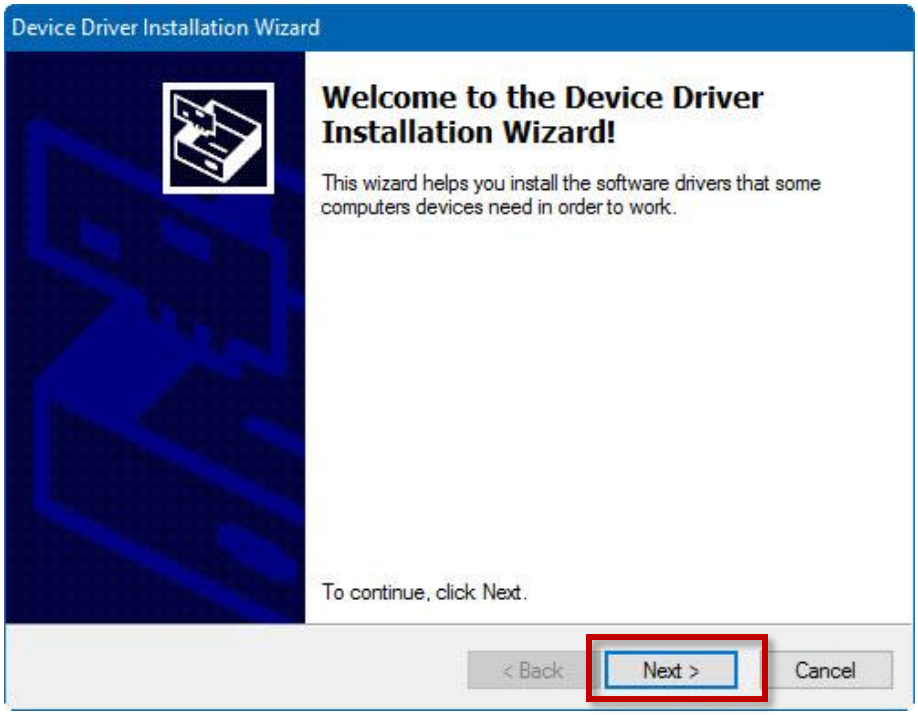
NB *Please note if you have a legacy multi-seat Network dongle, these do not work with VFC v5. This is a 'Fortress' dongle so you can try installing the driver as 'KEYLOK 3 or Fortress (USB Driverless)' and 'Standalone' but this will only allow one user to use it at a time. If you experience difficulties, or need more assistance, please contact technical Support to replace your dongle.*

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Select ‘KEYLOK 2 (USB w/Driver)’ and Standalone:

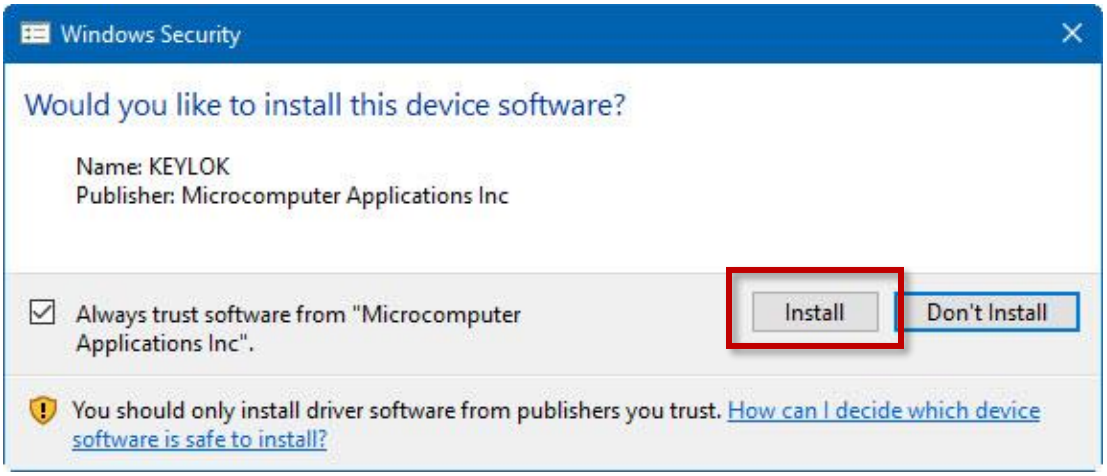


Select the correct settings and choose and ‘Begin Install’ to start the installation wizard.



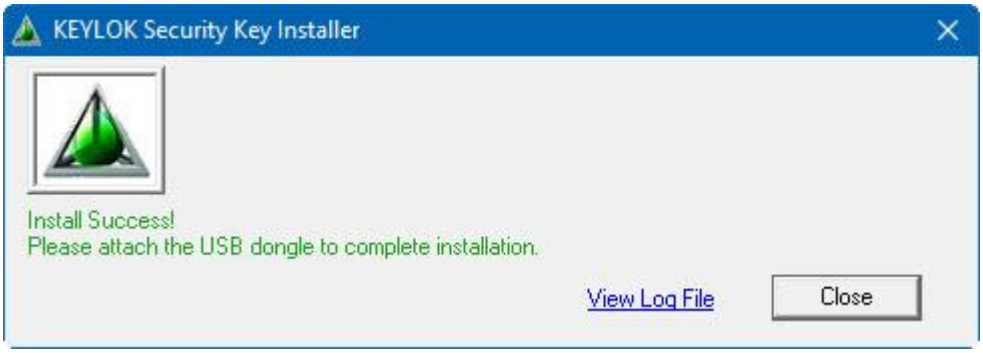
Click Next

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8



Click Install

Click Finish



Because the VFC License Manager application (used to download software updates, update license subscriptions and refresh dongle data) requires a dongle to be present in order to query and process updates, the Dongle Drivers will also be required to use this, if using a green dongle.

If you attempt to run VFC without a dongle, or with a green dongle and the dongle drivers have not been installed, you will see an error message; please refer above for instructions.

If you still experience problems, please visit the FAQs section of this guide/our website and failing that, contact our support team via support@md5.uk.com.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

VFC License Manager

VFC License Manager is used to refresh the dongle data when the subscription has been renewed on a registered dongle and to download the software (including updates).

NB *License Manager needs to be able to recognise that a VFC dongle is present to query and process updates, so if using a green dongle, the respective dongle drivers will also need to be installed.*

VFC License Manager is installed alongside VFC and the latest version can always be accessed via the VFC downloads page. Once downloaded and installed, it can also be found in the VFC program installation folder (Program Files>MD5 Ltd>VFC5 or Program Files (x86)>MD5 Ltd>VFC5) or in the Standalone folder of the VFC software download .ZIP file. If your expired dongle is available, you should also be able to access 'License Manager' from within VFC.

License Manager requires a valid PID authentication key to update your dongle. This can be retrieved online if your system has access to the Internet (it utilises the settings set within Internet Explorer on your host system) or a PID may have been sent to you via other means such as email or even physical mail.

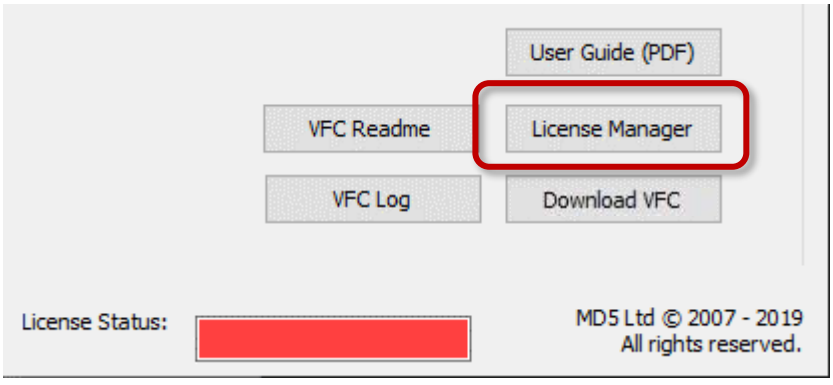
** IMPORTANT ** Please always use VFC License Manager v5.0 or later. This supports VFC3 upwards. Please do not use VFC License Manager v4 or older versions of the software. If you have shortcuts to this software on the system you use to download updates, we recommend you remove them because the legacy version of License Manager can corrupt v5 and later dongles which can in turn require them to be re-programmed.

Please check the VFC Downloads page for the latest version (https://vfc.uk.com/downloads/).

Updating or Upgrading your VFC License

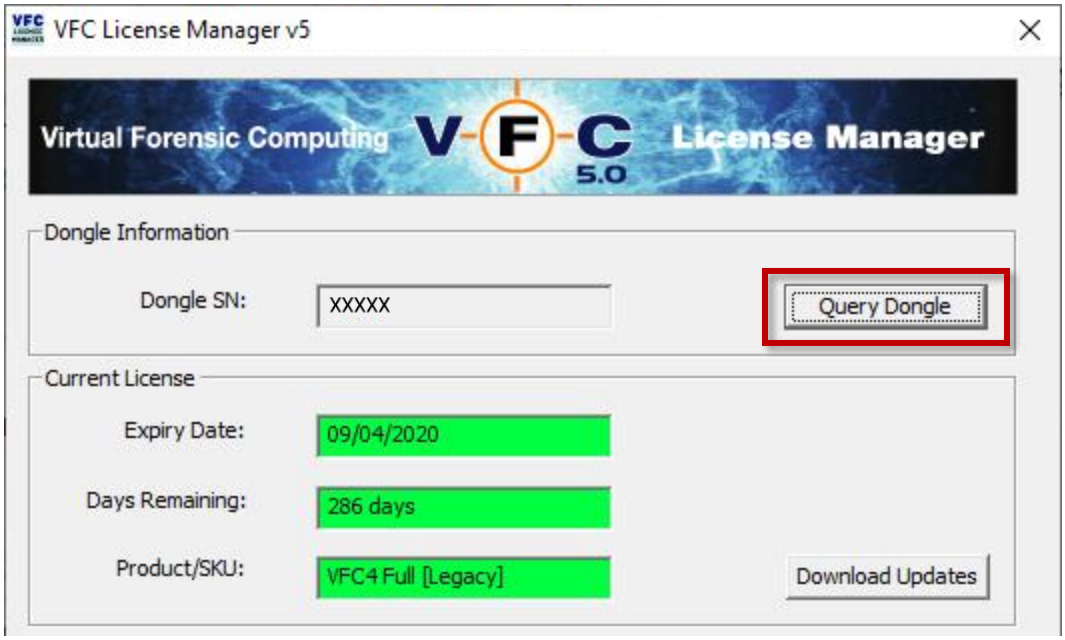
Please note, if your License has not already been upgraded to VFC5, during the process of opening VFC 5.0 to access License Manager, it will report that the license is invalid.

When you click OK, it will take you to the About tab of VFC 5.0 where you can then launch the new License Manager tool:

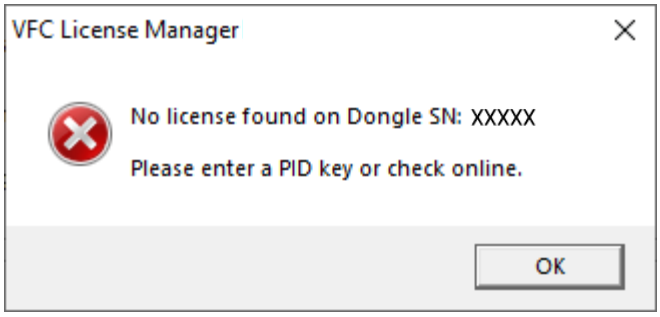


To use License Manager:

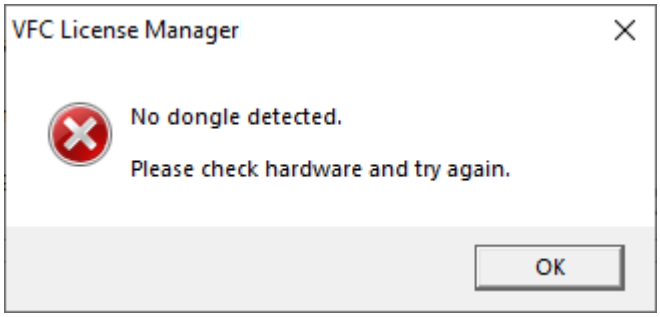
1. Click on “Query Dongle”. If your license is not already set up for v5, it should report there is a Legacy license:



If you see the message “No license found on Dongle SN: XXXXX”, please contact sales@md5.uk.com to check that the license is still in date, or to renew your subscription:



If you see the message, “No dongle detected. Please check hardware and try again,”, please ensure your dongle is plugged in correctly:



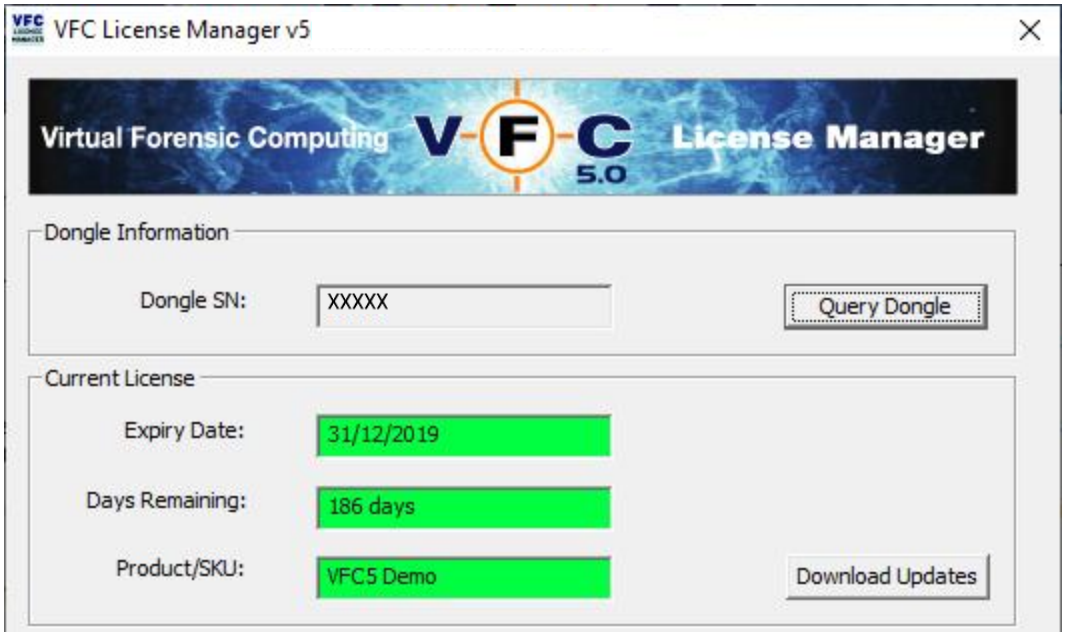
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

2. If you have been emailed a PID activation key, click on the "…" button to browse and then enter your PID.

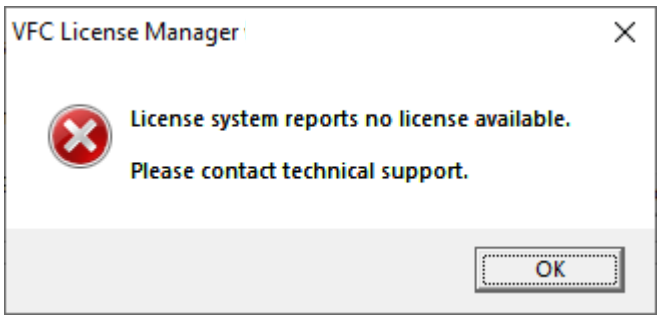
   A PID will take the form of "RJRTCX-WDPKWF-KQJJQT-JNBHRD" and will be specific to each dongle.

   If you have not been emailed a PID, your license will have been updated on our database and will be ready for an online update.

   Please ensure you have an internet connection and click "Check Online". This should update your dongle if a valid license exists:



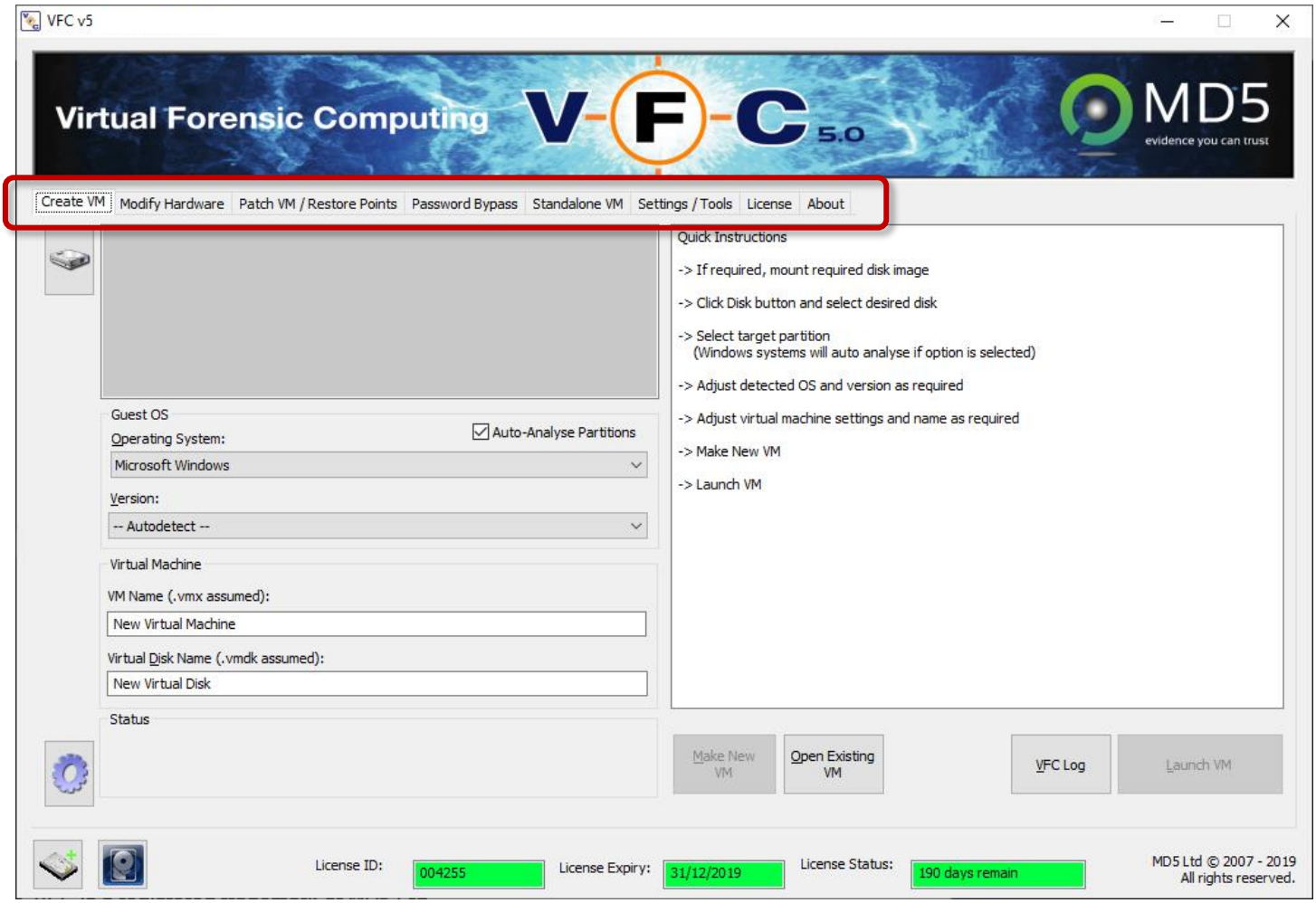
   If you see the message "License system reports no license available.", it could be that you are trying to access our database via a proxy server, or that the database doesn't currently hold an update for your dongle. If you see this message, please contact sales@md5.uk.com:



Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

3. Provided the update has been applied properly, the license indicator at the bottom of VFC 5.0 should turn green:

4. You will now need to close and restart VFC to activate the full program:

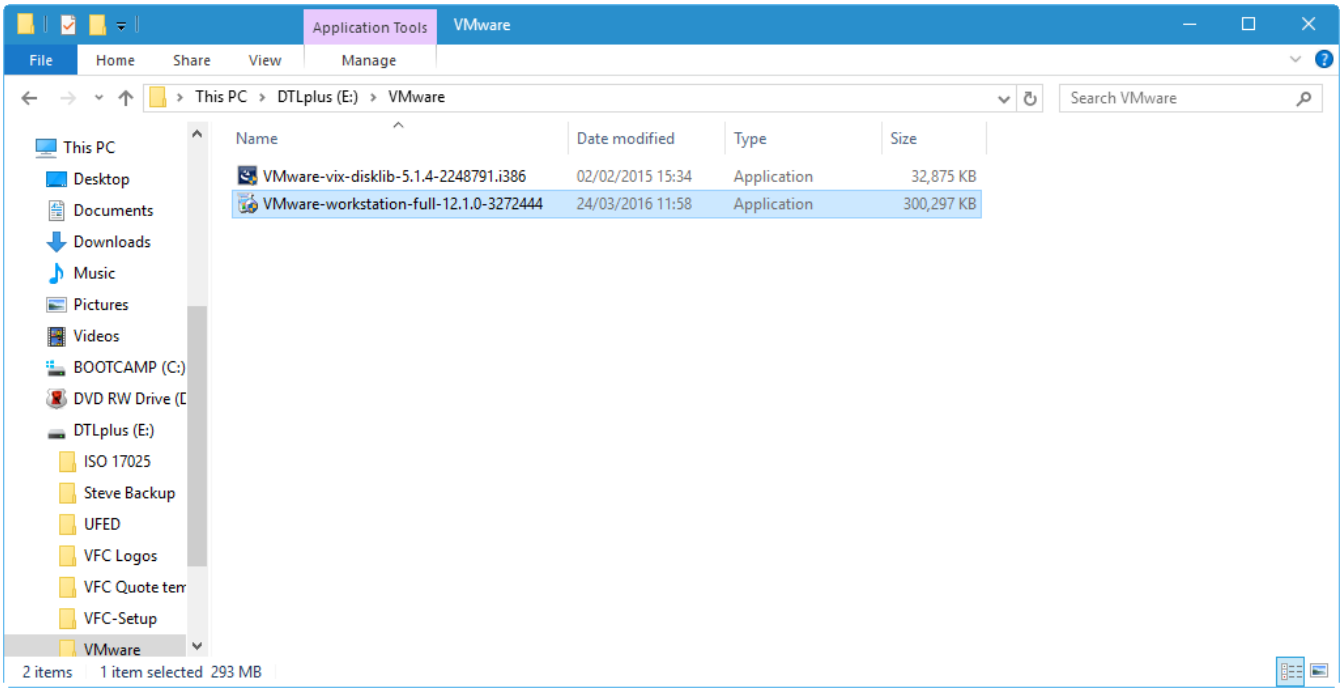


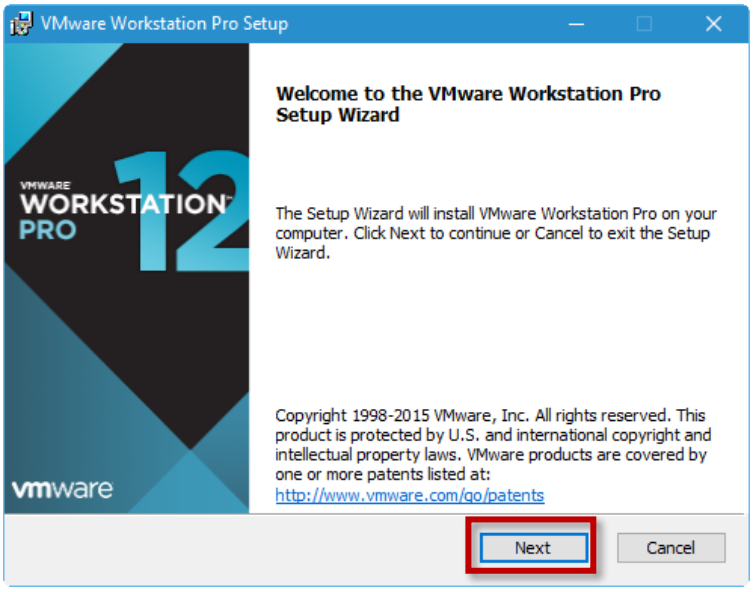
NB *To update multiple dongles, they must be updated one at a time. Please refer to the instructions for 'Updating your dongle' found in the troubleshooting section for more information.*

Installation of VMware Workstation

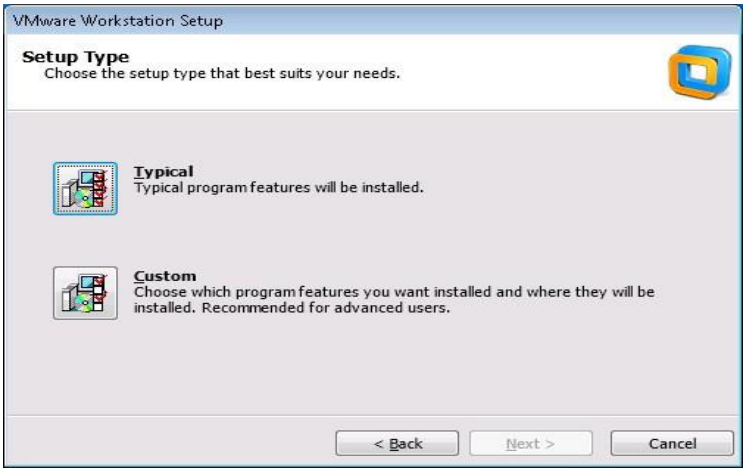
he following section describes how to install VMware Workstation. These instructions were written for VMware Workstation v12. A similar process may be used for VMware Player and subsequent versions of both products.

In Windows Explorer, navigate to the location where you have saved the installation files, right-click on the VMware-workstation-full-12.1.0-3272444.exe file (or whichever version you have access to) and select 'Run as administrator':

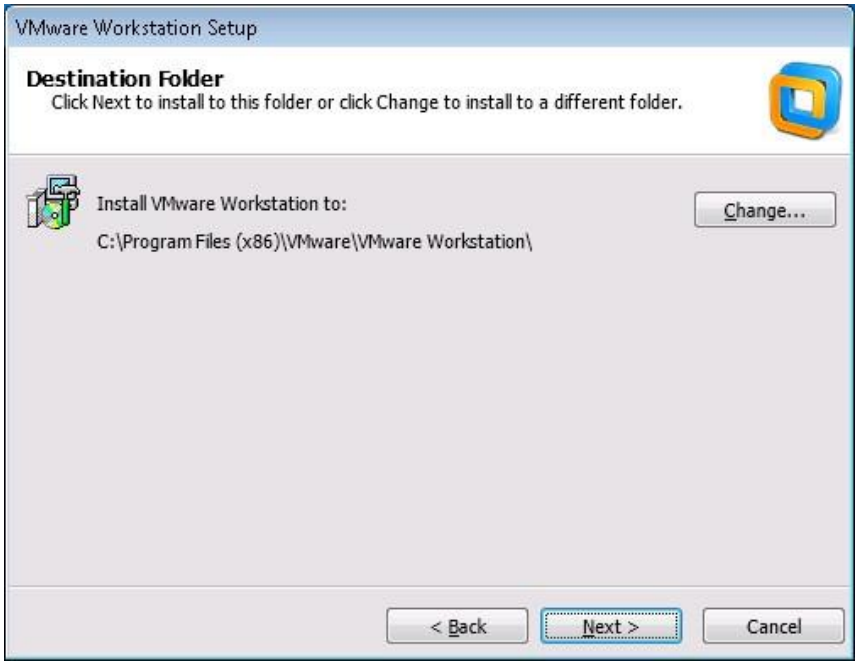




A typical installation of Workstation Pro should suffice. Click 'Next' to proceed.

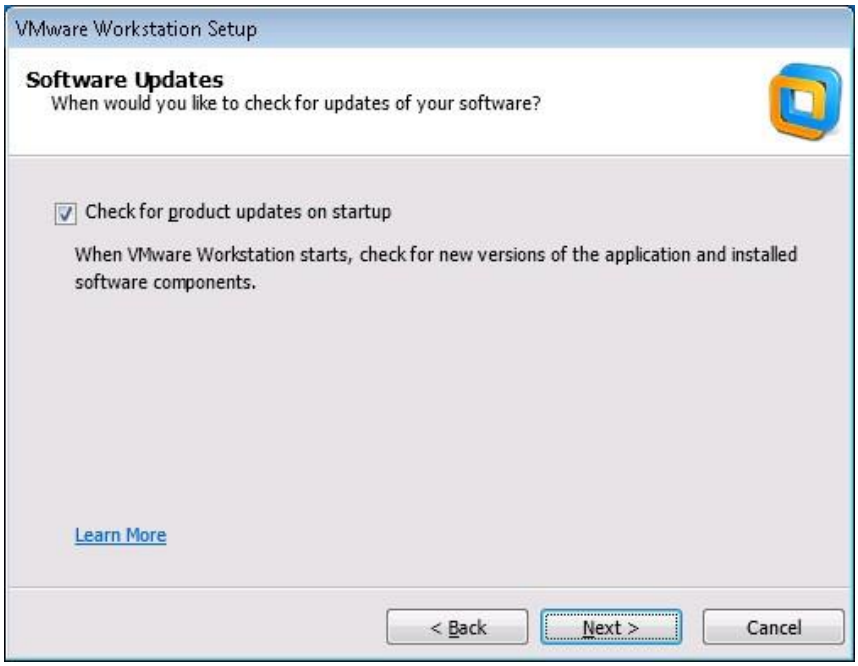


Either accept the default installation folder (recommended) or change the installation location and click 'Next'.

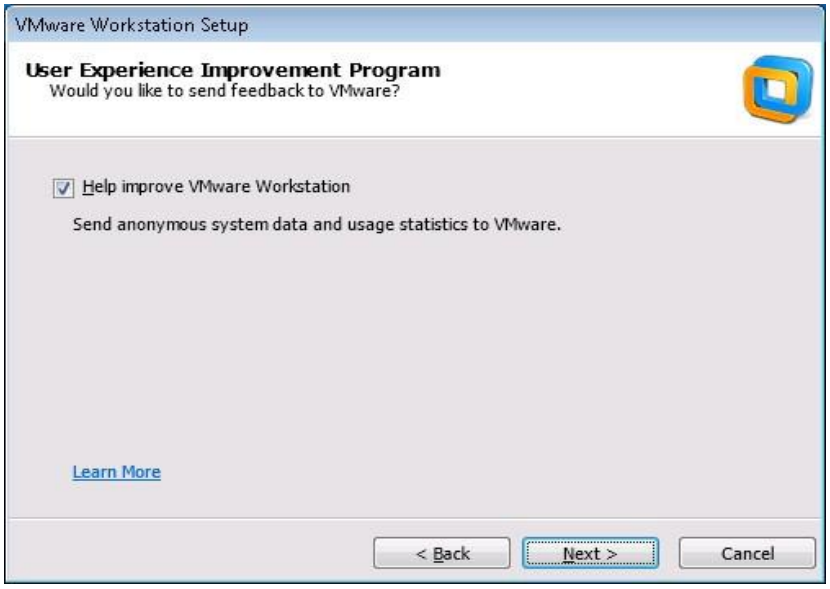


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Check for product updates can be disabled if using a non-Internet connected Host System

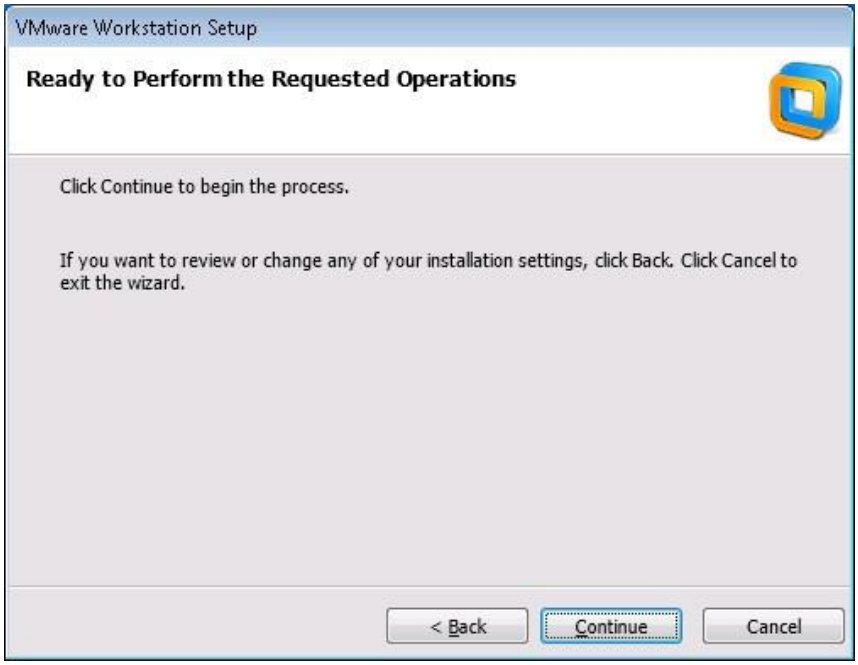


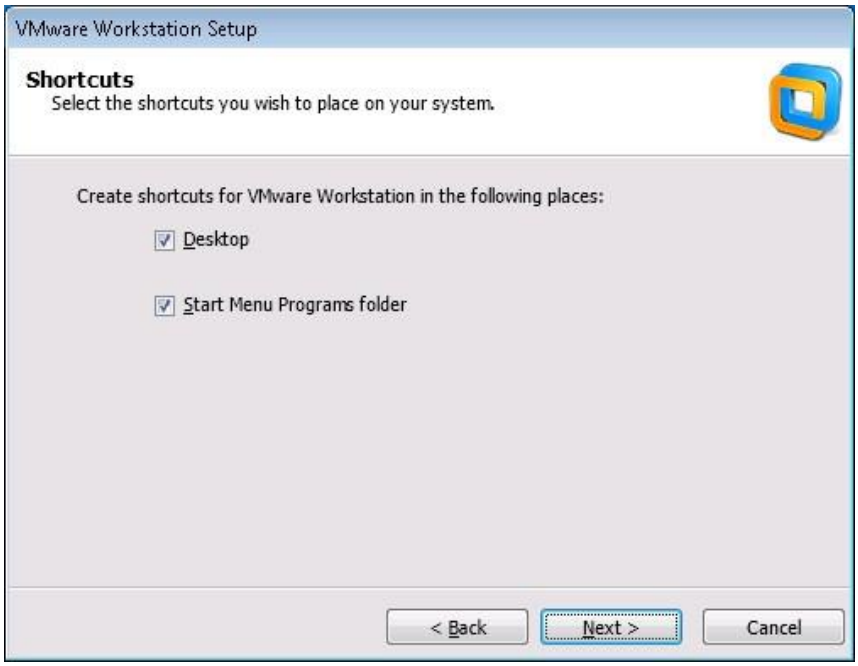
Click 'Next to continue



Sending system and usage data can be disabled if required. Click 'Next to continue.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

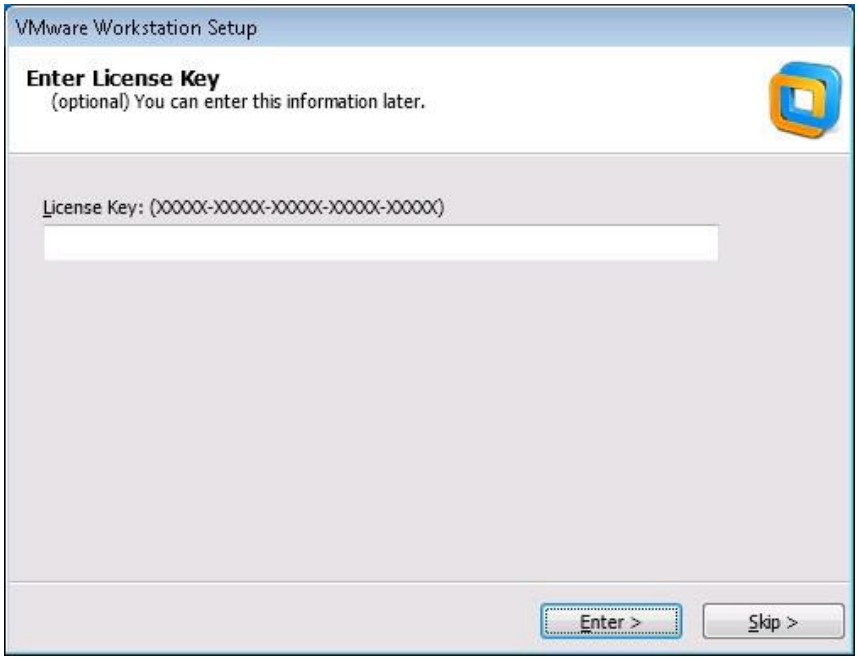


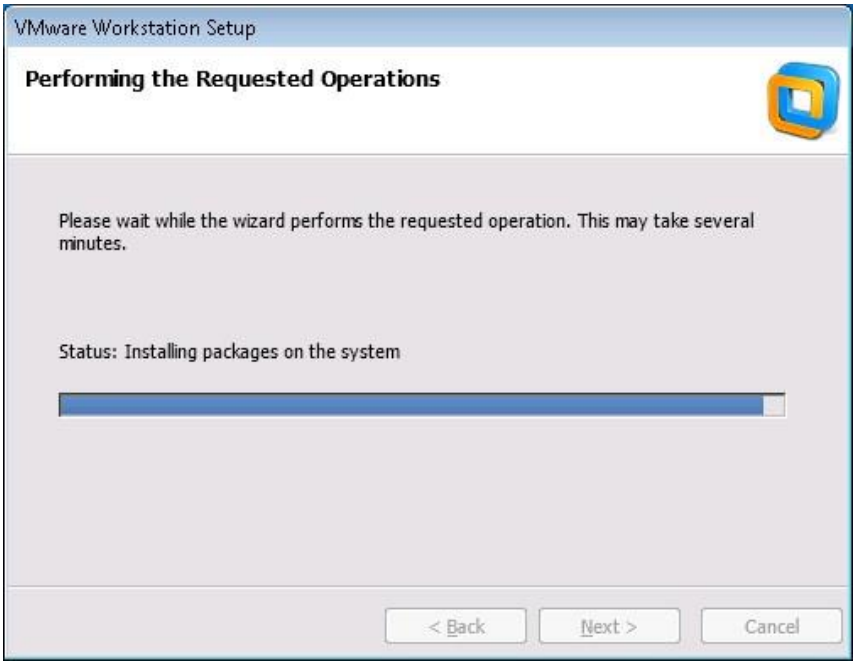


Default options for creating shortcuts on desktop and Start menu are enabled but can be disabled if required. Click 'Next to continue.

Clicking 'Continue' will start the installation process.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8





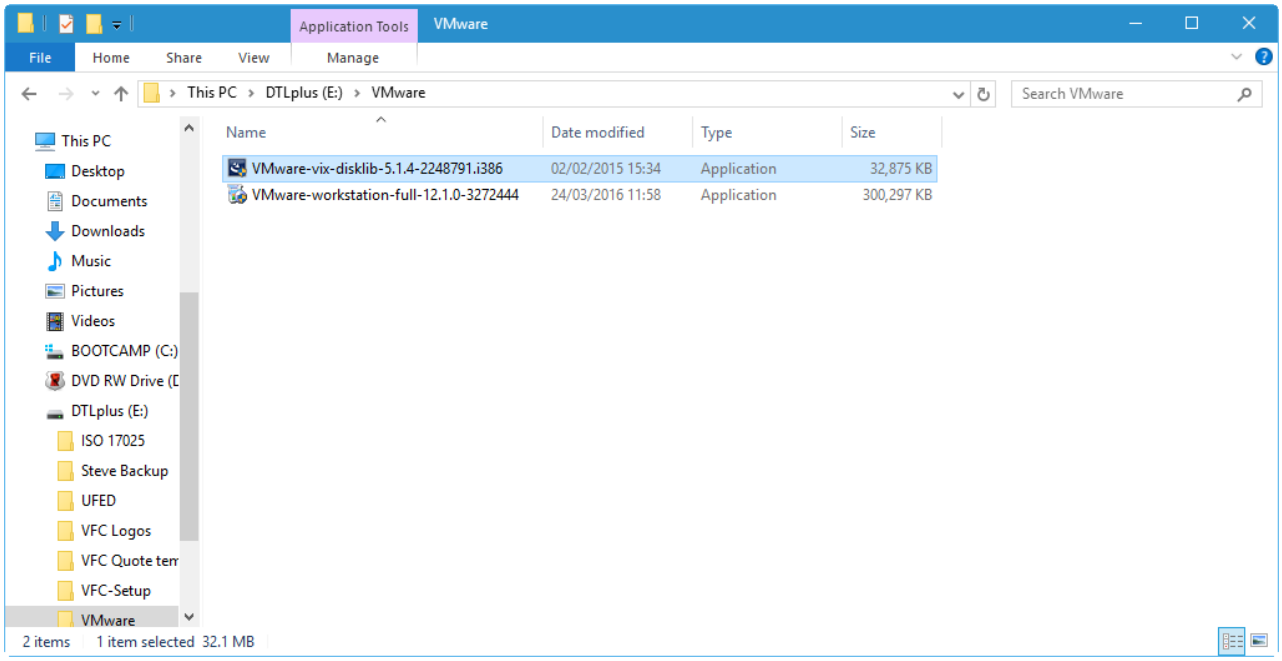
The installation can take several minutes.

VMware Workstation Pro requires a license registration key but can work in trial mode for up to 30 days. VMware Workstation Player is free for personal, non-commercial use but any business, agency or institution should seek to agree a licensing arrangement with VMware.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Installation of VMware VDDK

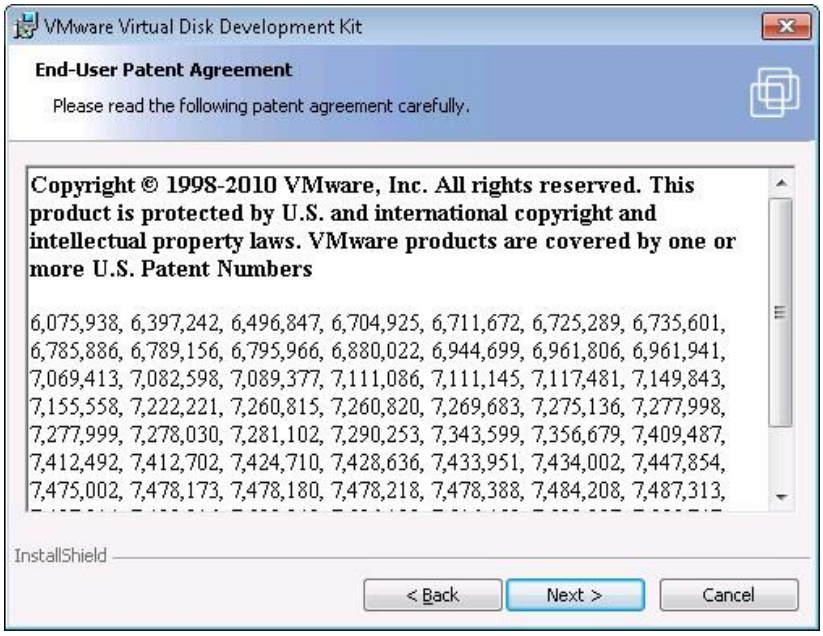
VFC is supplied with version 5.1.4 of VMware's Virtual Disk Development Kit (VMware VDDK) and it Is recommended this version is used.



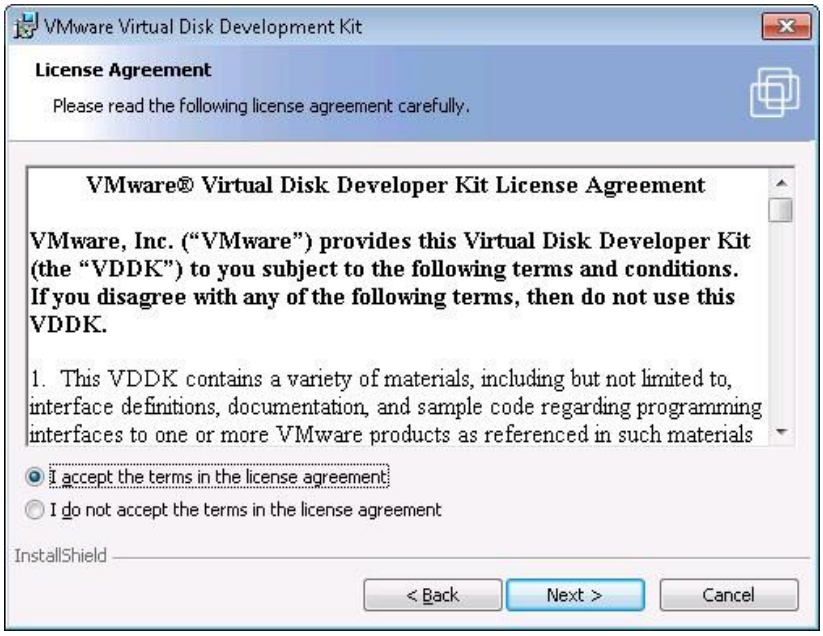
In Windows Explorer, navigate to the location where you have saved the installation files, right-click on the VMware-vix-disklib-5.1.4-2248791.i386 file (or whichever version you have access to) and select 'Run as administrator'. Please note that earlier versions of this application are not guaranteed to work with VFC as expected and as such are unsupported.

Click 'Next' to continue.

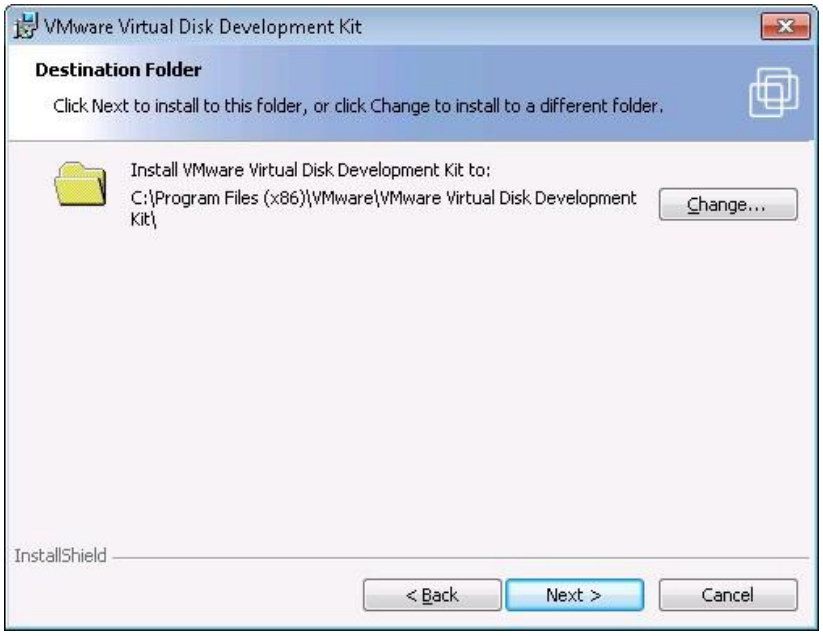
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8



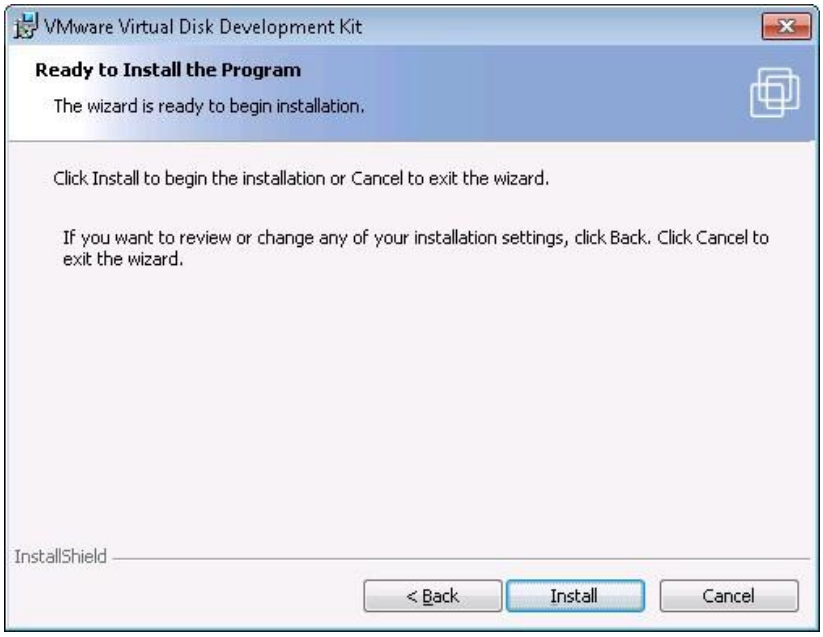
The End User Patent Agreement will be displayed. Click 'Next' to continue.



The End User License Agreement will be displayed. Accept the terms and Click 'Next' to continue.



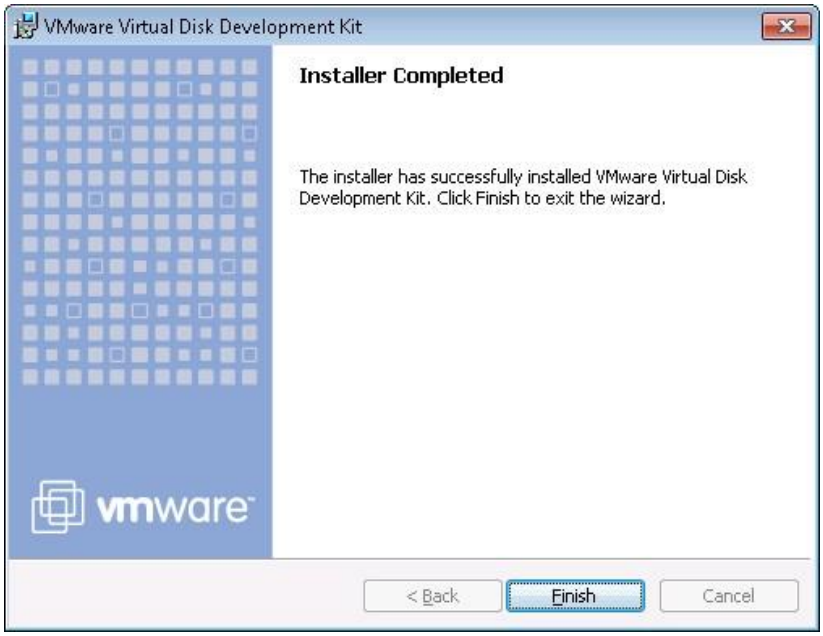
You can either accept the default installation folder (recommended) or change the installation location and click 'Next'.



Click 'Install' to begin the installation process.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

The installation may take several minutes.



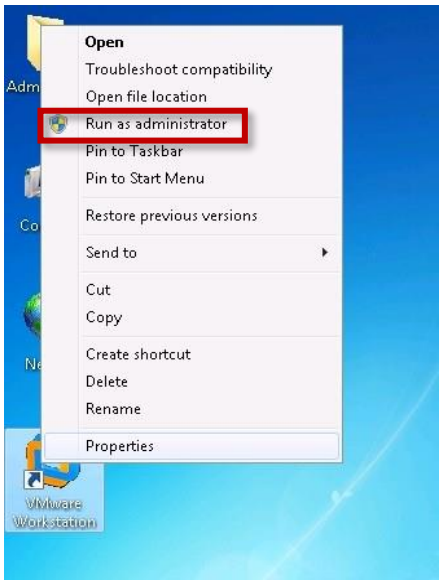
Click 'Finish' to exit the installation wizard.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

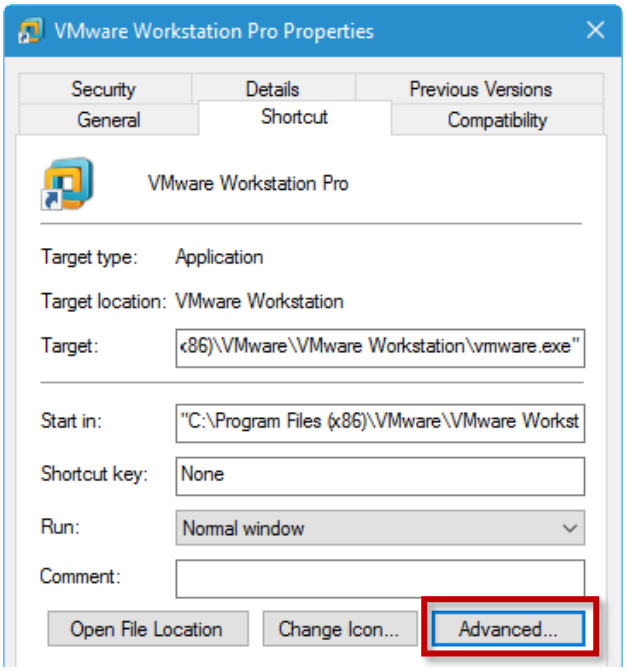
Always Run as Administrator

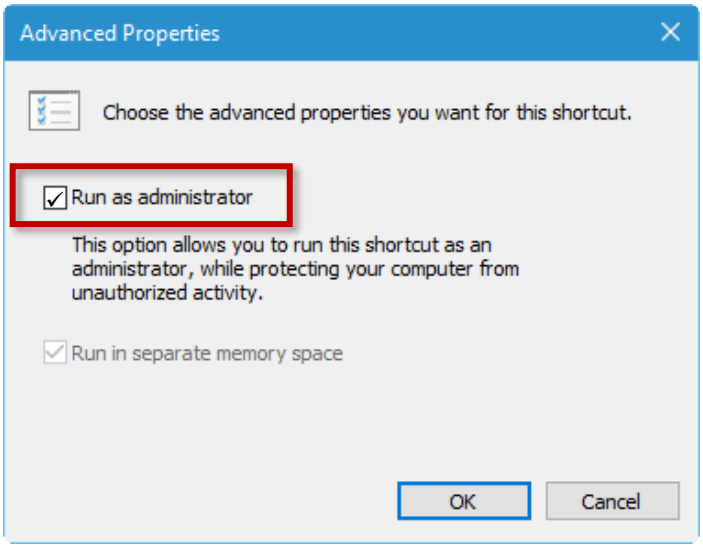
When all relevant applications have been installed, it is useful to change the properties of any desktop icons to 'Always run as administrator'.

Right-click on the relevant desktop icon:



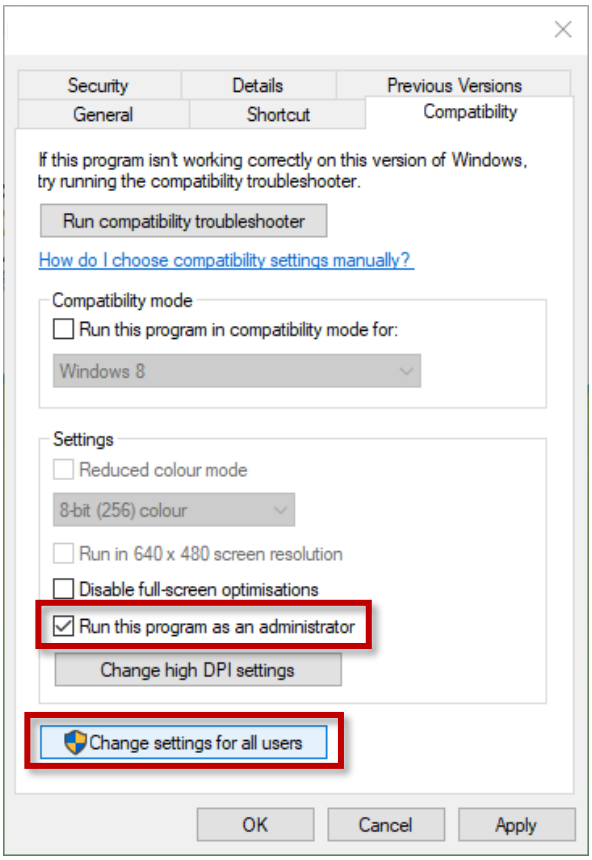
Depending on your version of Windows, either click directly on "Run as Administrator" or Click "Properties" and then check the box for 'Run this program as an administrator' or select 'Advanced' then 'Run as Administrator'. If using a workstation which multiple users may have access to, select 'Change settings for all users' first:

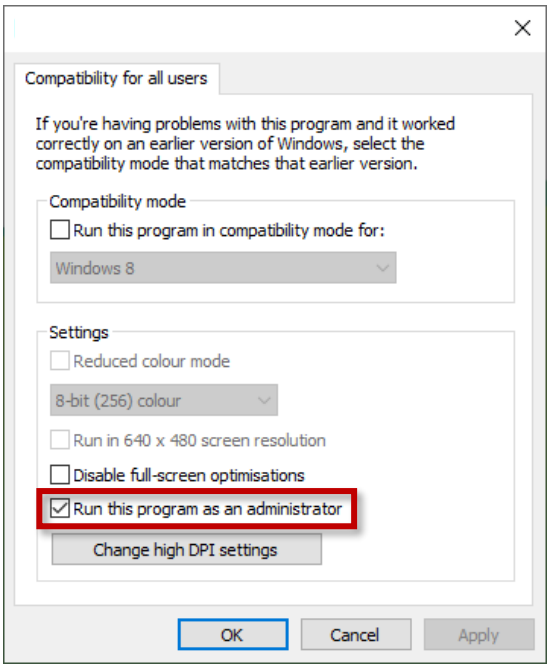




Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

On newer systems, the setting is commonly found on the Compatibility tab:





Check the 'Run this program as an administrator' option and click 'OK'.

Repeat these steps for the desktop icons (and Quick Launch icons if applicable) for VFC, FTK Imager and VMware and any other associated programs.

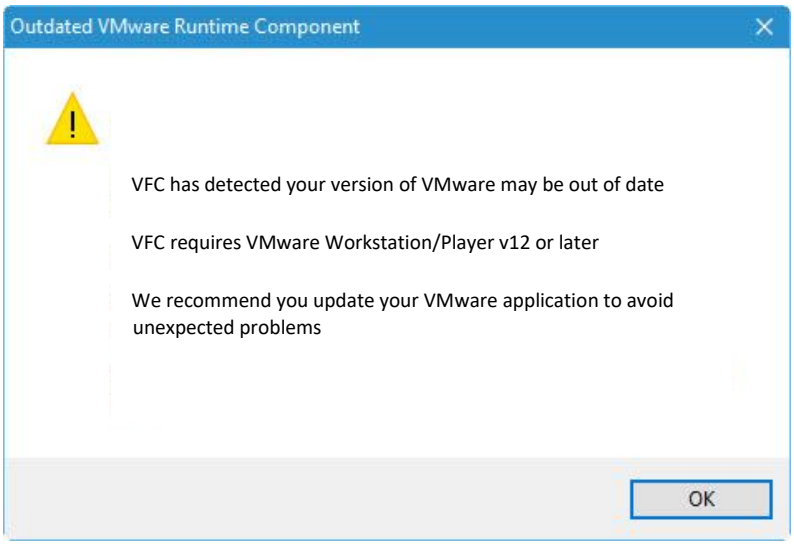
This is not relevant to VFC which will always launch as Administrator but is relevant to VMware. We would certainly recommend that you only run VMware as administrator because it will need this to mount physical/emulated disks.

Because VFC always runs as Administrator, everything it touches (e.g. .VMX and .VMDK files) has the "administrator" touch and therefore this is always required in VMware (Workstation and VDDK) for it to work correctly. Admin rights are essential to the way VFC and VFC Mount work.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

VFC: Component check

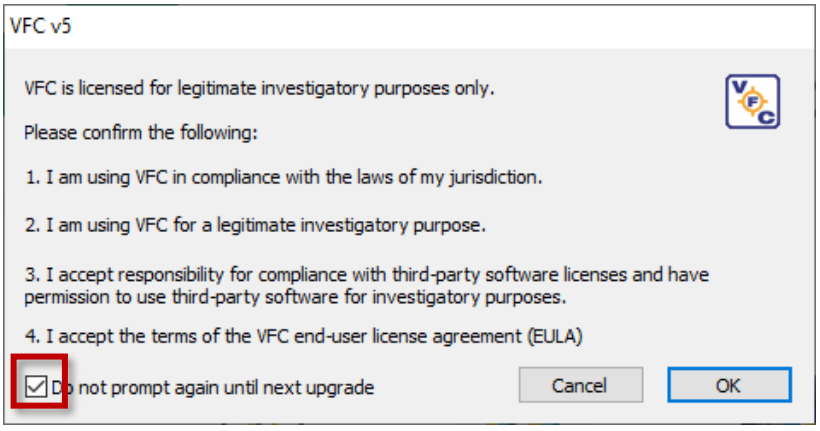
When you launch VFC with a licensed dongle inserted, VFC will initially check whether the most up to date versions of VMWare and VDDK are installed. If VFC detects that a more up to date version of one of the components is available, then a notification message will prompt you to update the relevant programme.



VFC proper usage policy

When you first launch VFC following installation or upgrade, with a licensed dongle inserted, VFC will ask you to confirm you have the appropriate permissions, motivations and legal right to use the software. You are also accepting liability for usage of any 3rd party software within the VMs you create.

If you want this to pop up every time you use the software, by way of a reminder, please leave the checkbox unticked. Otherwise, you can put a tick in the box and it won't appear again until your next upgrade:



Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

VFC: Step-by-Step

Mount a forensic whole disk image

VFC was built to work with mounted forensic whole-disk images.

VFC is mount tool agnostic. You can use whatever mounting utility you like but please bear in mind the restrictions and costs of each. EnCase Physical Disk Emulator (PDE), for instance, is limited to one mounted image at a time so prevents the generation of multiple VMs or VMs with multiple drives, unless a second mounting utility is employed, which can lead to system conflicts.

VFC can also work from physical (tangible) hard disk drives though it is recommended they are write-blocked prior to use to prevent corruption or contamination of data. The Physical Disk In Use error is common with physical drives so the features of the "Settings/Tools" tab can be employed to discard offline mount points and allow VFC to have sole access to the connected physical drive.

There are several utilities available by which a forensic whole disk image can be mounted; the main one now of course, being VFC Mount.

VFC Mount – MD5's proprietary, built-in mounting utility

VFC Mount currently supports .E01, .EX01, AFF4, .VMDK, .BIN, .IMG, .RAW, and .DD images.

VFC Mount is installed with VFC. It includes a driver component which must be installed when you first run VFC Mount. This operation is only necessary once (see instructions on next page).

To use VFC Mount, launch it for the first time from VFC. Following this, you will then also be able to launch VFC directly from forensic software using the integration components, which automatically mount the 'live' images using VFC Mount.

Integrate with EnCase using the supplied EnScript (see notes on using the EnScript here) or from X-Ways Forensics using the included integration X-Tension (see notes on using the X-Tension here)

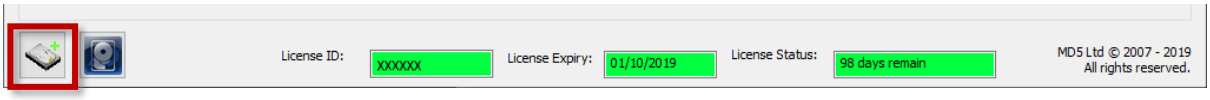
NB The 3rd-party integration components require VFC Mount to have been run at least once before you can use them.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

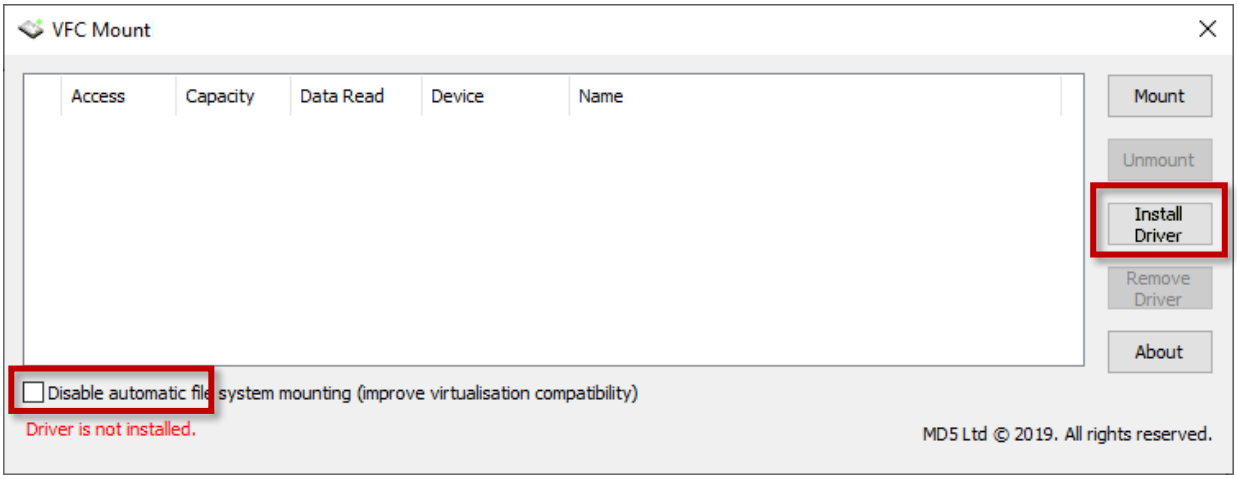
Using VFC Mount

To use VFC Mount for the first time:

1. Click icon to launch VFC Mount Click on the VFC Mount icon in the bottom left of the GUI:



2. Note text in red indicating that the driver is not installed:



3. Click Install Driver

4. If prompted, click Install (see screenshot) to authorise driver installation

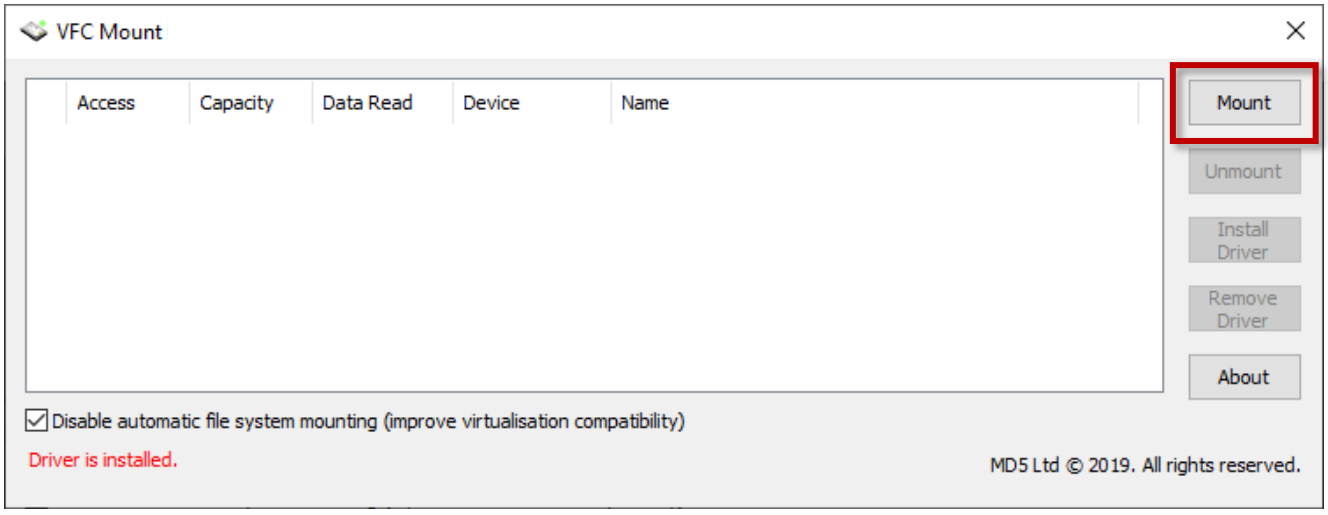
NB: This procedure is typically only required the first time VFC Mount is used or following the installation of a significant new version. Please note that regardless of the installed version of VFC, the 32-bit version of VFC Mount must be used on 32-bit systems and the 64-bit version of VFC Mount must be used on 64-bit systems. VFC automatically loads the correct version.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Mounting a Drive with VFC Mount

We have tried to simplify the process as much as possible.

Simply click on “Mount”:

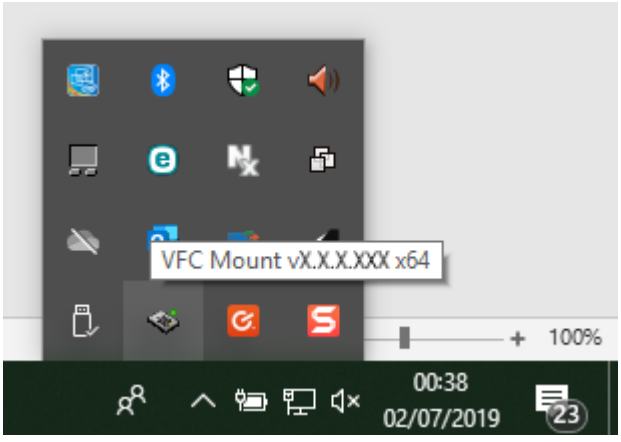


Then browse for your image, select it and click Open to mount it.

We recommend you tick the "Disable automatic file system mounting" checkbox. This box is the same as the check box on the Settings/Tools tab of VFC. It prevents Windows from mounting new file systems and should help reduce frustrating "Physical Disk in Use" errors in VMware.

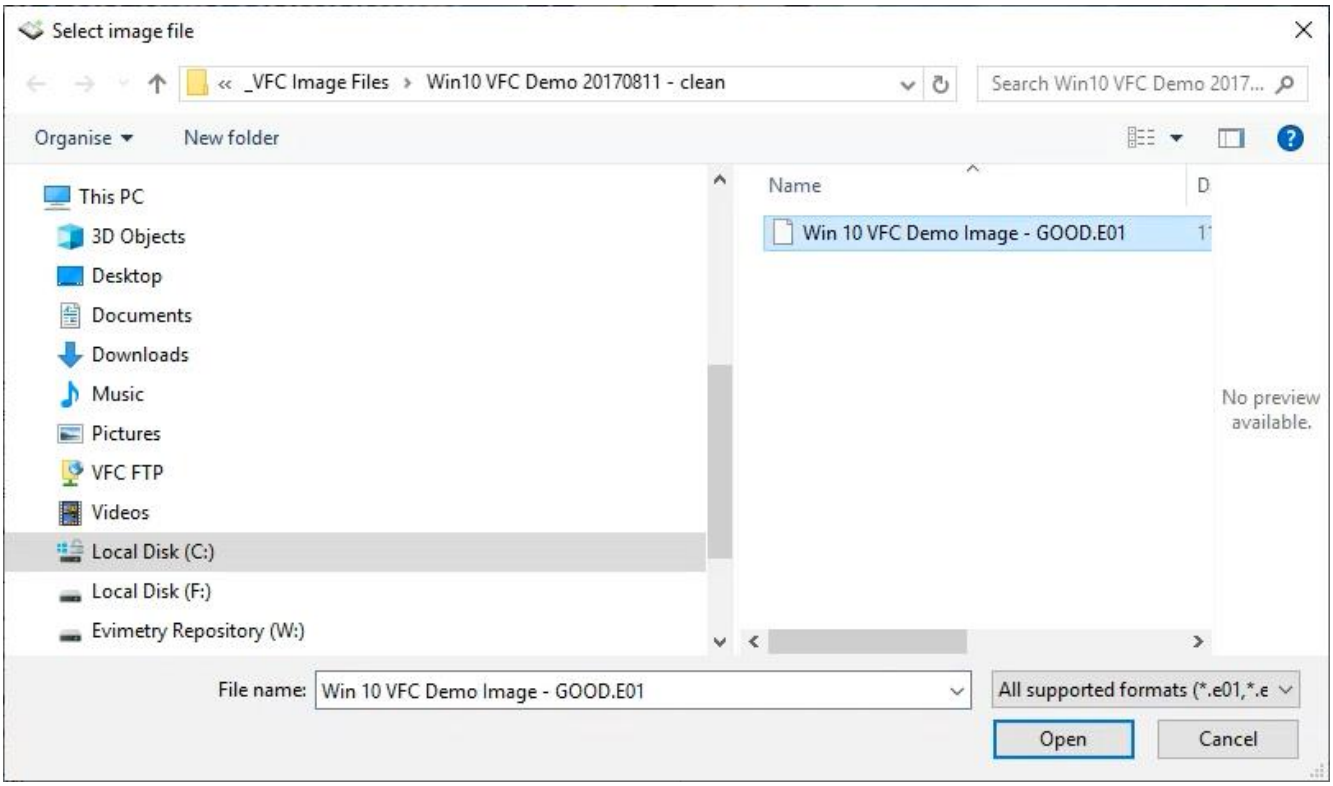
Once VFC Mount is opened, it remains open in the background until deliberately exited. VFC VMs rely upon their associated mounted drives to function so this is deliberate behaviour and is designed to prevent the failure of open VFC VMs due to exiting VFC too early.

The red X will only close the GUI so you can check the status of or re-use the tool from within VFC at any time. If you have closed VFC, you always retrieve the VFC Mount program from the system tray:



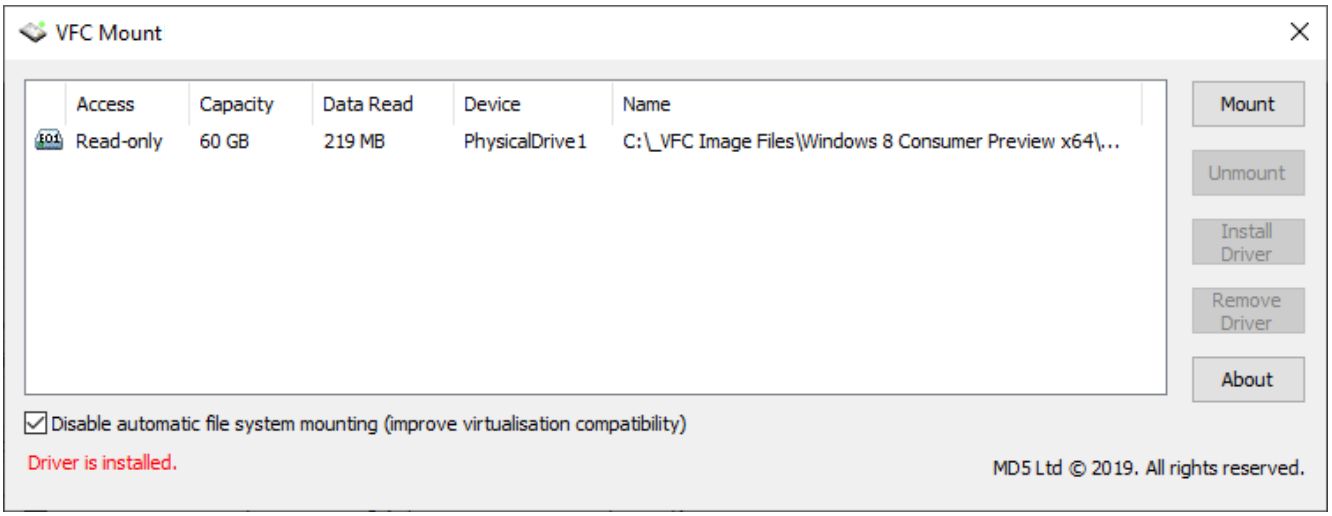
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

When you click “Mount”, VFC will open a browser dialogue. Navigate to the folder where your forensic image is located and choose the one you want. VFC Mount should only display supported file-types and will select the header file (e.g. .E01) to reduce clutter and help identify the required file quickly and easily:



Select your image and click “Open”. VFC Mount will then select the optimum settings for a VFC VM.

There will be a short delay before the mounted image appears in VFC Mount. This delay is deliberate and is intended to minimise instances of the frustrating "Physical Disk in Use" error in VMware:

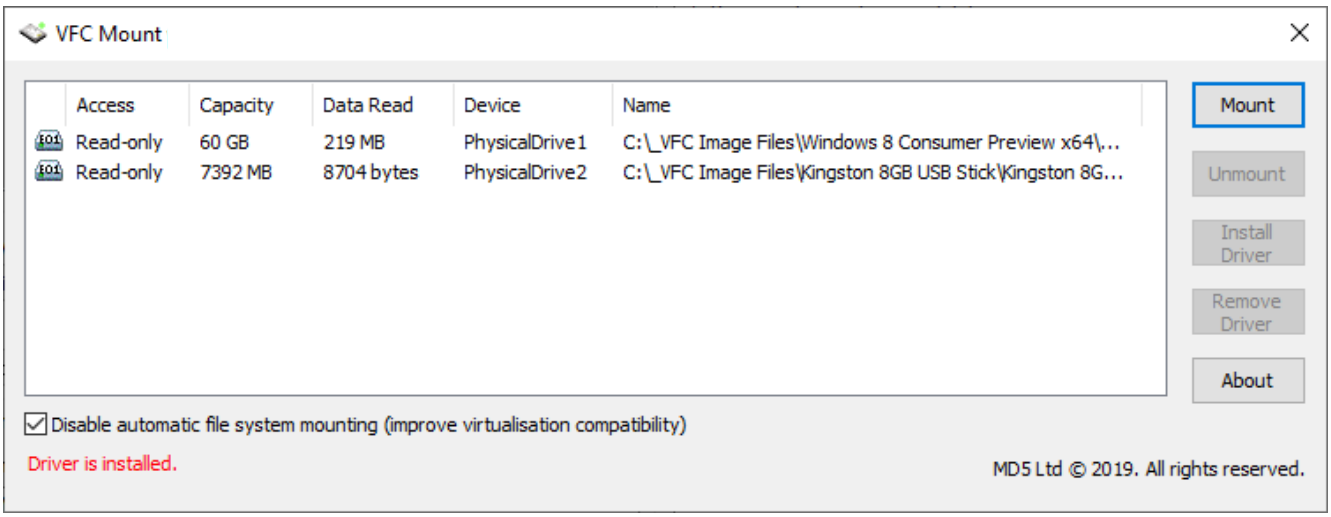


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Mounting Multiple Images

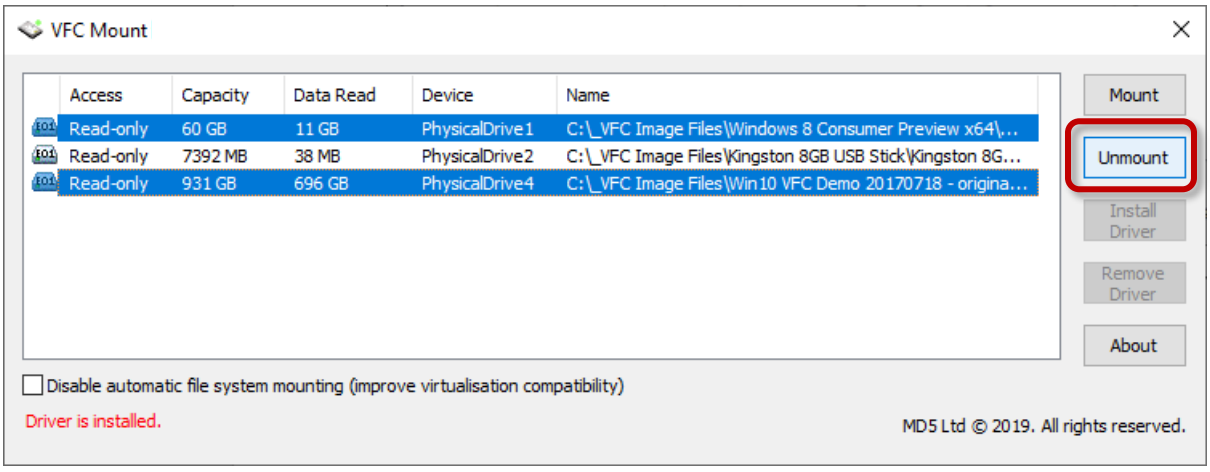
If creating multiple VMs or creating VMs with multiple drives, you will need to mount more than one image. You can always add more images later but if you know what you're going to be working with, we suggest you mount them all now.

Just click "Mount" again to add another image and follow the instructions above – and keep going till you have all your drives:



Unmounting Images

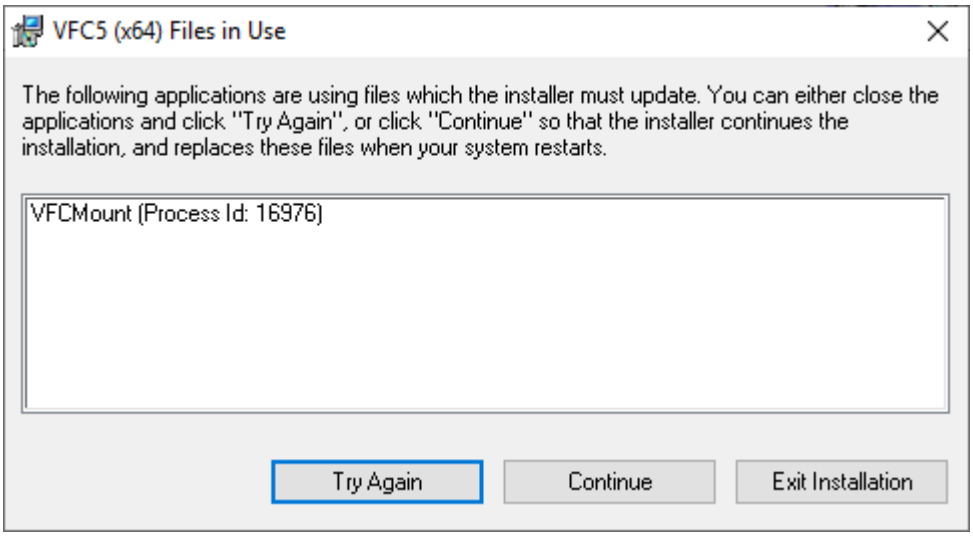
Once you are finished with your mounted drives, simply highlight the no-longer-required files and click on "Unmount". You can select multiple drives using either Control or Shift + Click as with most Windows programs:



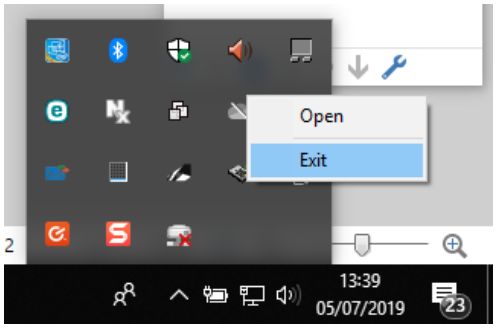
NB: Please remember that when you unmount an image it is equivalent to unplugging a physical disk. Any running VM that is using that image will immediately fail. We recommend you leave images mounted until all VMs are closed. It is not necessary to unmount images before shutting down the workstation; this will happen automatically when you log out of Windows.

Updating VFC Mount

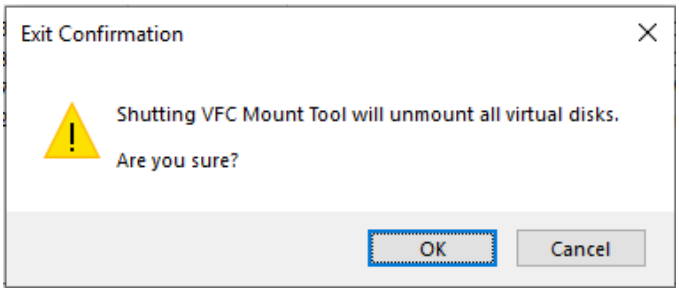
Occasionally, when VFC is updated, VFC Mount will also receive updates. Because VFC Mount keeps running in the background and doesn't shut down with VFC, when this happens, you may find you need to close VFC Mount:



To do this, access the program in the system tray, "right click" and select "Exit":



If you have images mounted at the time you exit, VFC will notify you. To continue, select "OK":

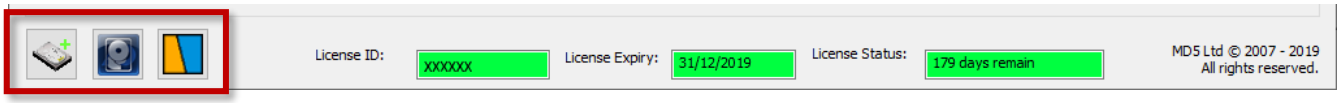


You will then be able to install the updates.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Mounting a Disk with External Mounting Tools

VFC now provides built-in icons to launch common mount tools. This currently supports FTK Imager (FTK), Mount Image Pro (MIP) and OSFMount. These “quick launch” icon(s) will appear in the bottom left of the GUI if the associated third-party applications are installed:



VFC FTK MIP

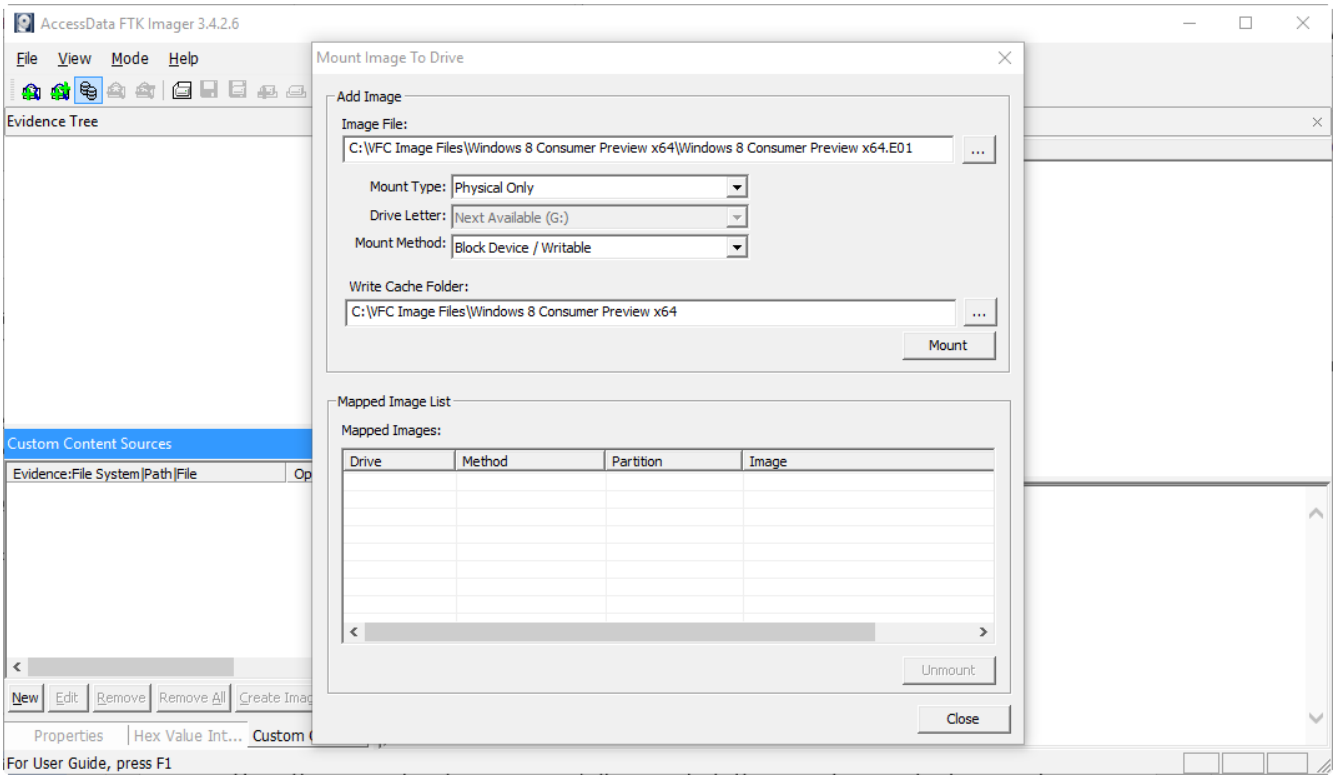
MD5 Development Team’s preferred mounting tool VFC Mount. We recommend you use the built-in VFC Mount unless you need specific additional functionality as this has been specifically designed to reduce errors and enhance the user experience. If using an external tool, we recommended FTK.

Tips for using FTK Imager

The FTK button in VFC should launch the mount dialogue, saving a couple of crucial seconds.

The image file (*.E01) should be mounted as “Physical Only”, FTK will allocate the next available drive letter.

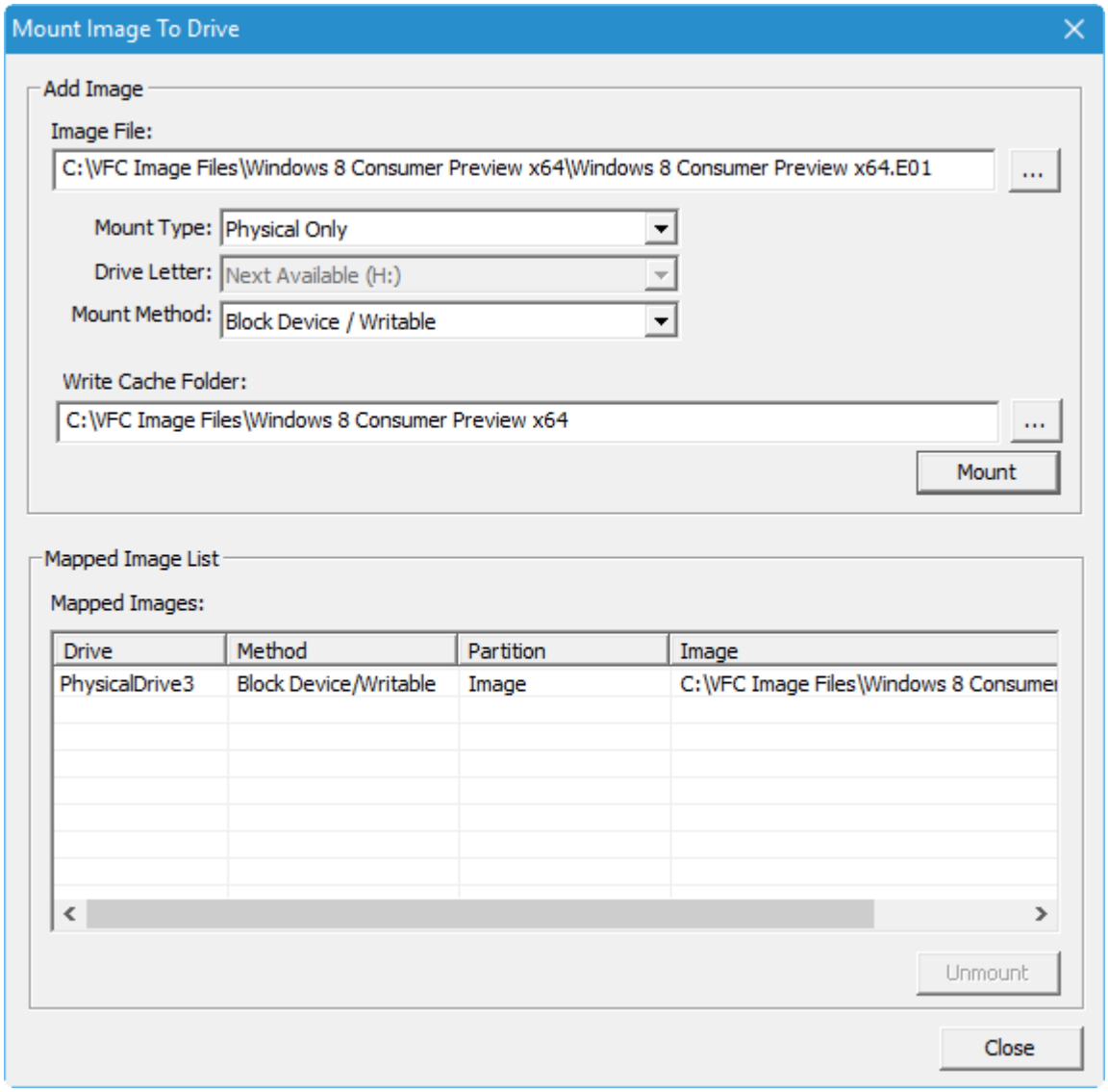
For the most consistent results, if mounting a disk image from Windows 7 or above, the mount method should be ‘Block Device / Writeable’ to minimise issues but ‘Block Device / Read Only’ should still work.



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

NB1 *If using either Encase PDE or the FTK Imager mount function, closing either of these applications will cause the image to dismount. The MIP GUI can be closed but will minimise the application to the system tray whilst maintaining the mounted status of the image, similar to the behaviour of VFC Mount, as described in the section above.*

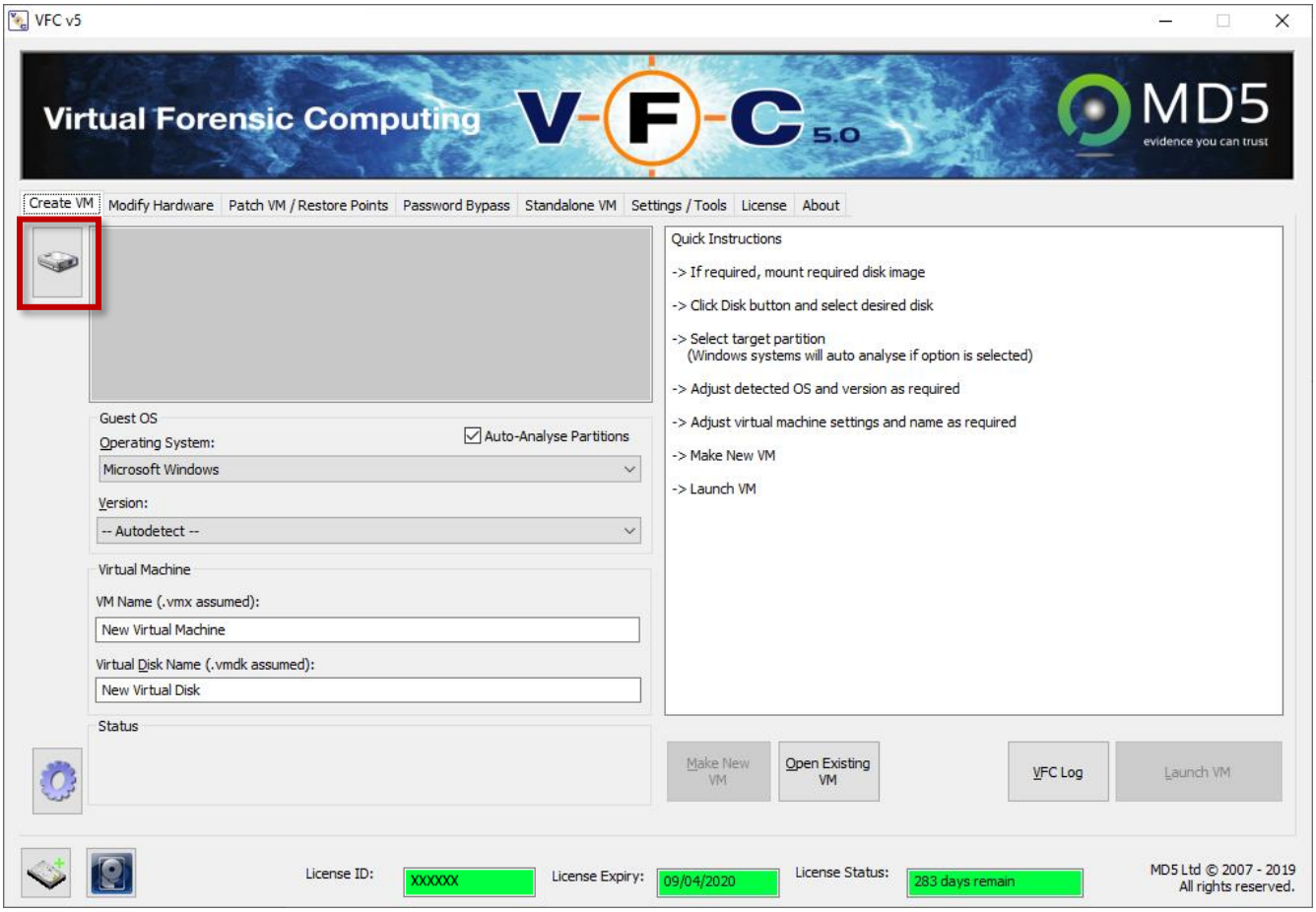
NB2 *If you need to select the OS folder using the Options screen in VFC you may need to mount the drive as Physical AND Logical.*



As can be seen from the above, the Windows 8 Consumer Preview x64.E01 image has been mounted as PHYSICALDRIVE3 and is now available to the system. This window can now be closed. From this point, the FTK Imager GUI is no longer directly required by VFC and can be minimised.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

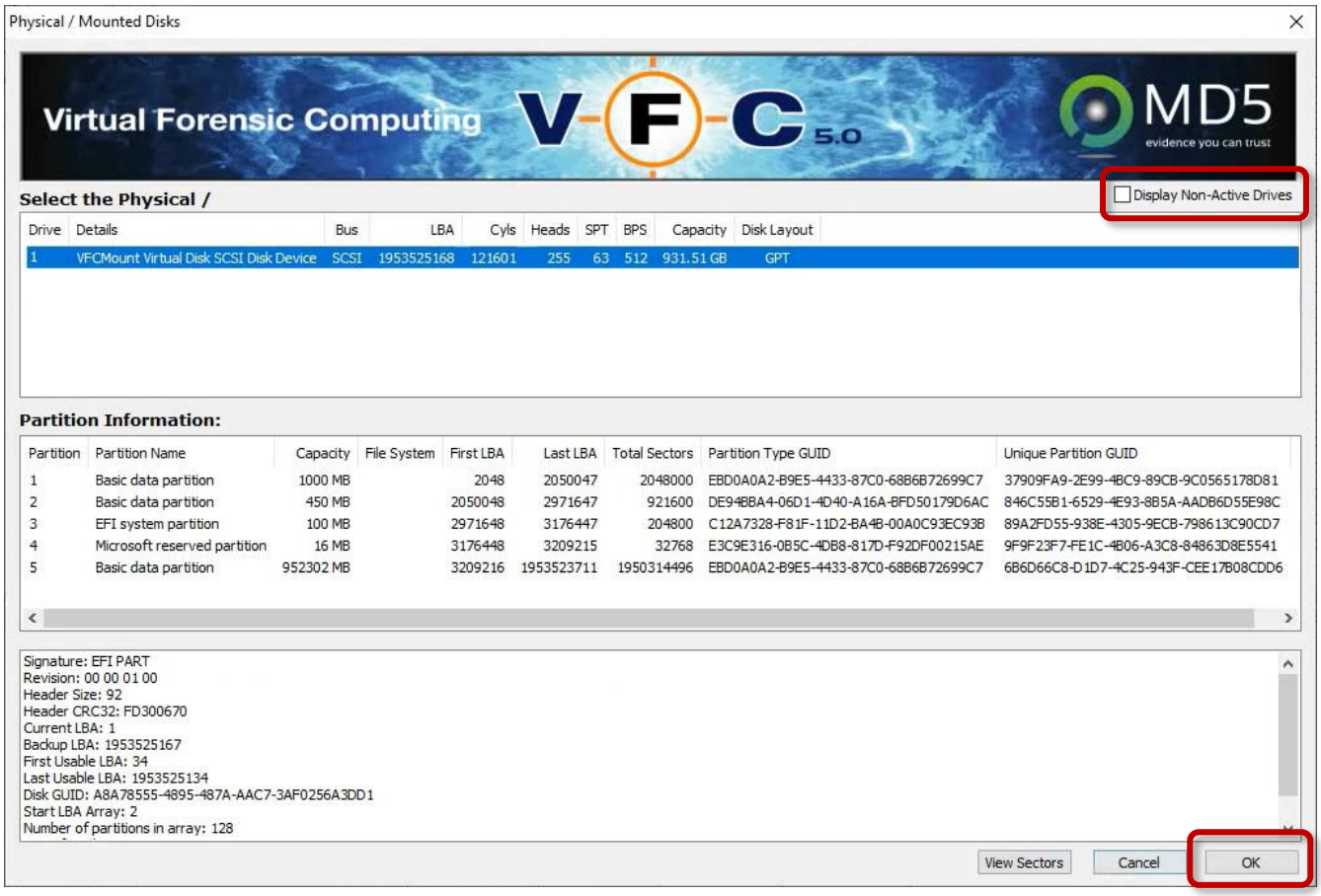
Enumerate Drives (Select Source Device) – Mounted Hard Disk



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

This process will enumerate all physical storage devices attached to the system – whether mounted or physically connected via a tangible interface.

Once enumeration is complete, VFC lists all the available drives in the drive selection dialog. You can 'double click' to quickly choose and load a specific disk into VFC or highlight it to view more information (such as the partitions or the sectors). Once you are happy you have the right disk, click "OK":



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, or with disks that do not have a standard MBR (such as Mac OS X GUID Partition systems).

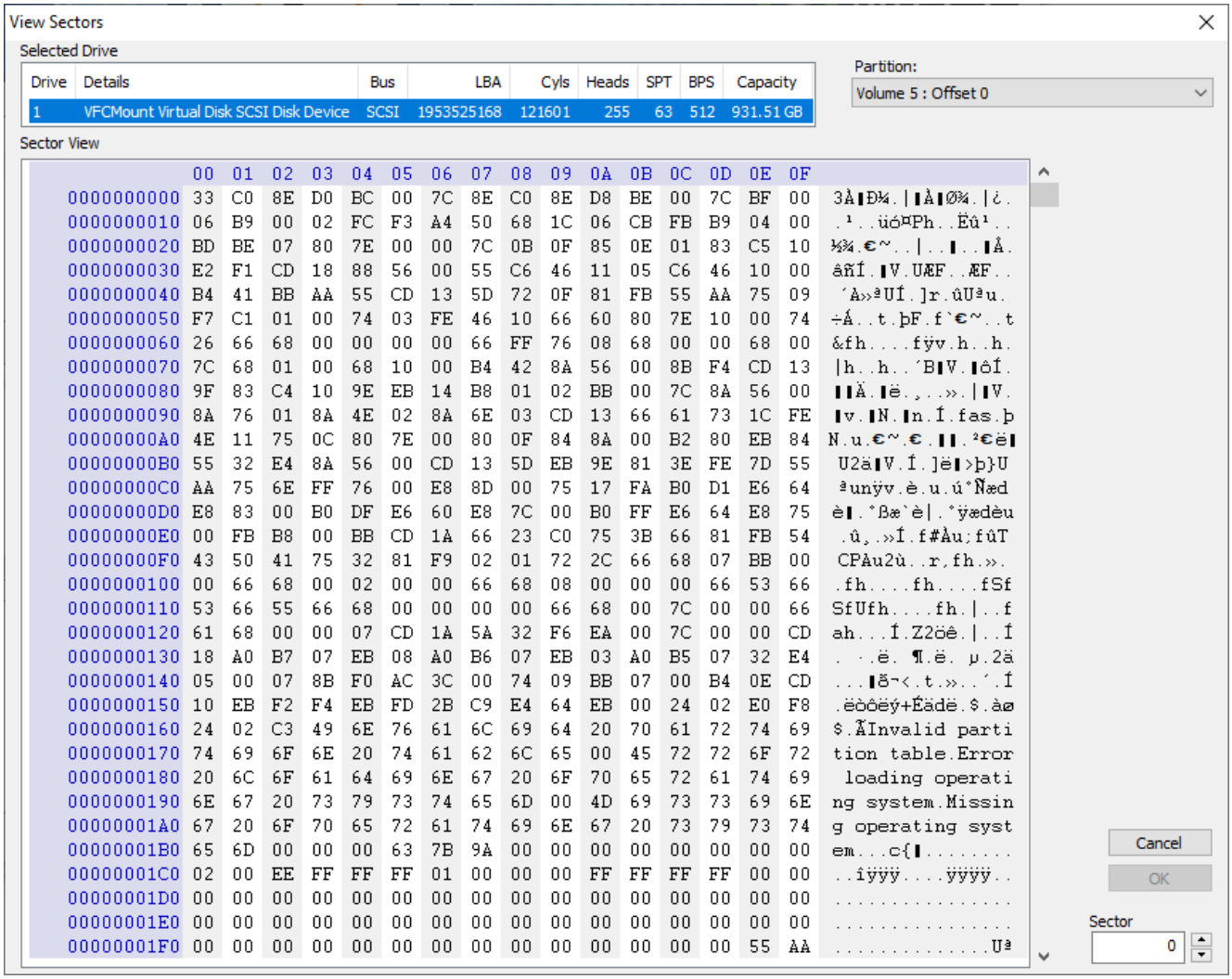
To display non-bootable drives, simply tick/check 'Display Non-Active Drives' located in the upper right of the drive selection dialog.

NB *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.*

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

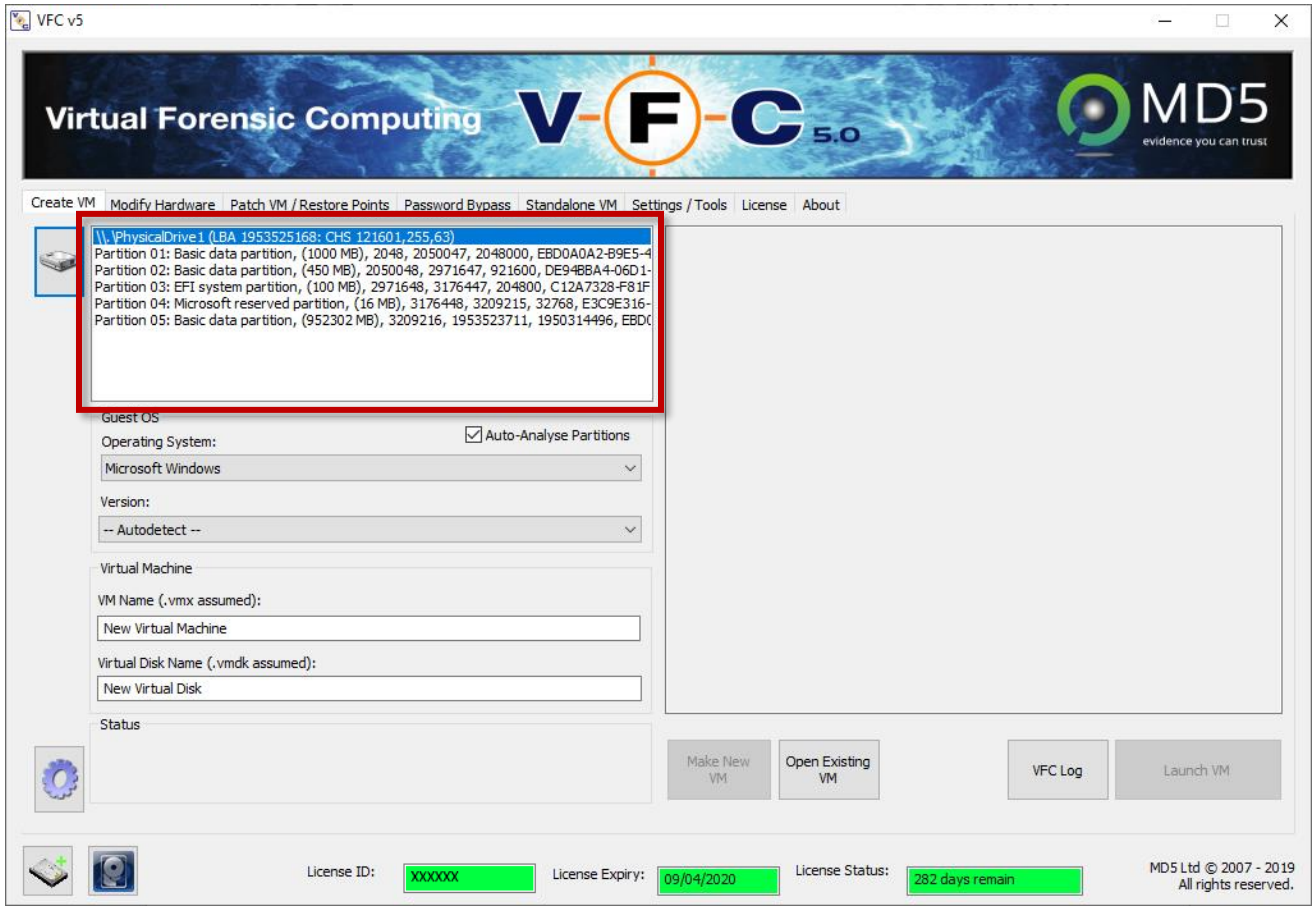
View Sectors

The 'View Sectors' dialog 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 the Target 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.

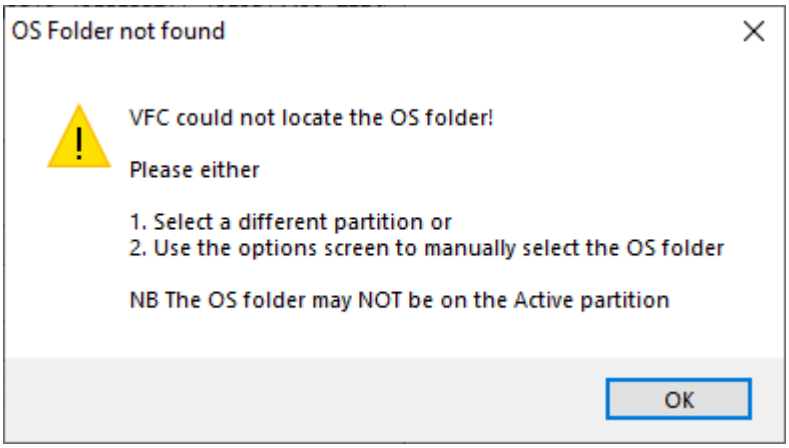


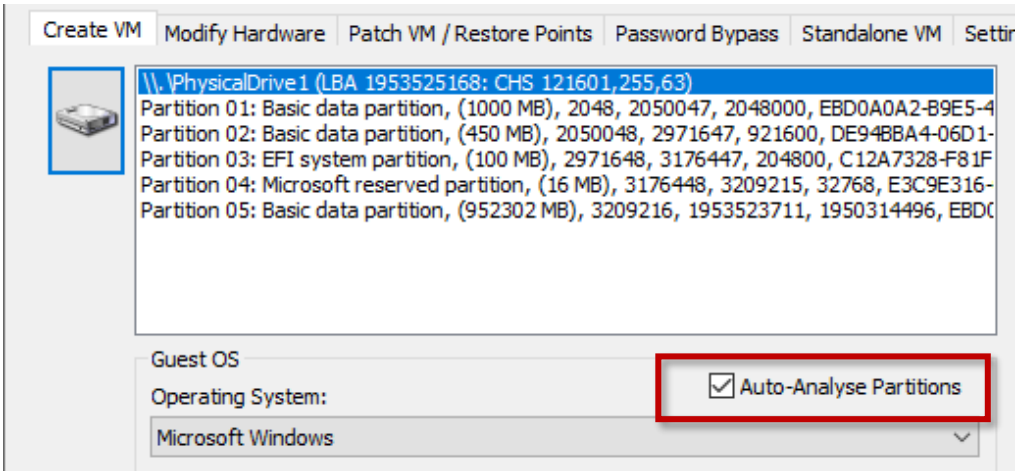
.

You will now need to select the appropriate 'boot' partition.

The boot partition may not always be the partition marked '(Active)', but it should be noted that on systems such as Windows Vista and above, the boot partition may actually be the second volume listed. The same would also be true for multi-boot systems, where the OS required to be VFC'd is on a different partition than the boot code for the drive.

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 version. This analysis will also try to extract relevant information relating to the installed Windows OS version from the registry and system files, and also information about the User accounts from the SAM file. This collected data will then be displayed in the upper right section of the main dialog. If the OS is not found then the following message will be displayed asking you to select a different partition.



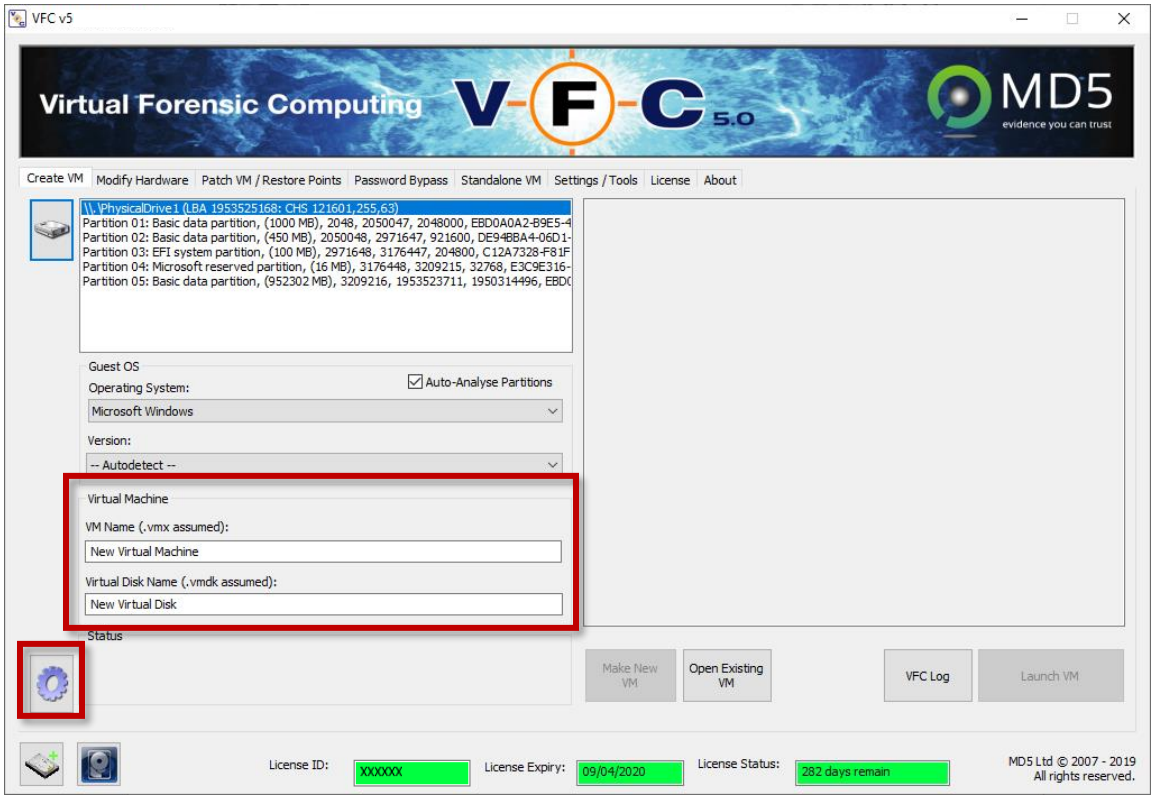


The 'Auto-Analyse Partitions' feature can be disabled if required and the OS version can be manually selected.

By disabling 'Auto-Analyse Partitions', this will preclude the extraction of any of the aforementioned system information.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

If required, various options which affect the generation of the Virtual Machine can also be altered as desired (see Options, later in this guide).

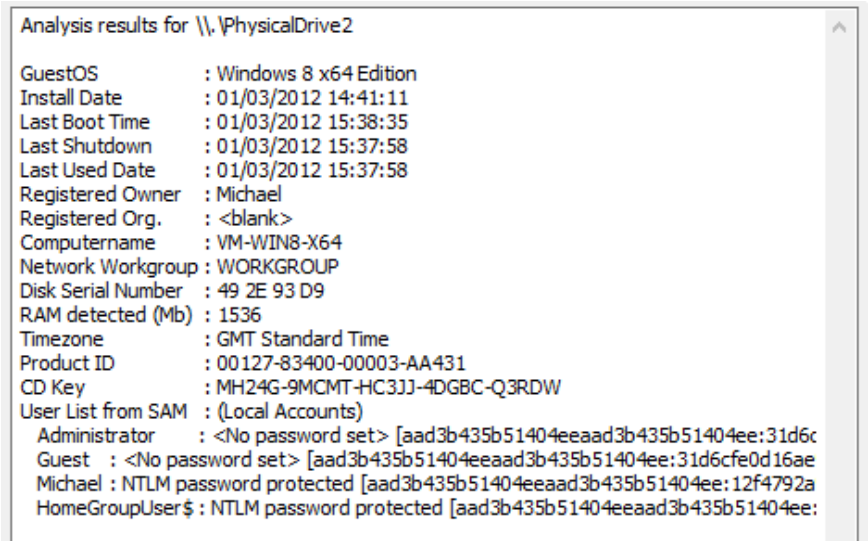


Once the analysis has been completed, you have the option of changing the Virtual Machine Name (default ‘New Virtual Machine’) and the Virtual Disk Name (default ‘New Virtual Disk’).

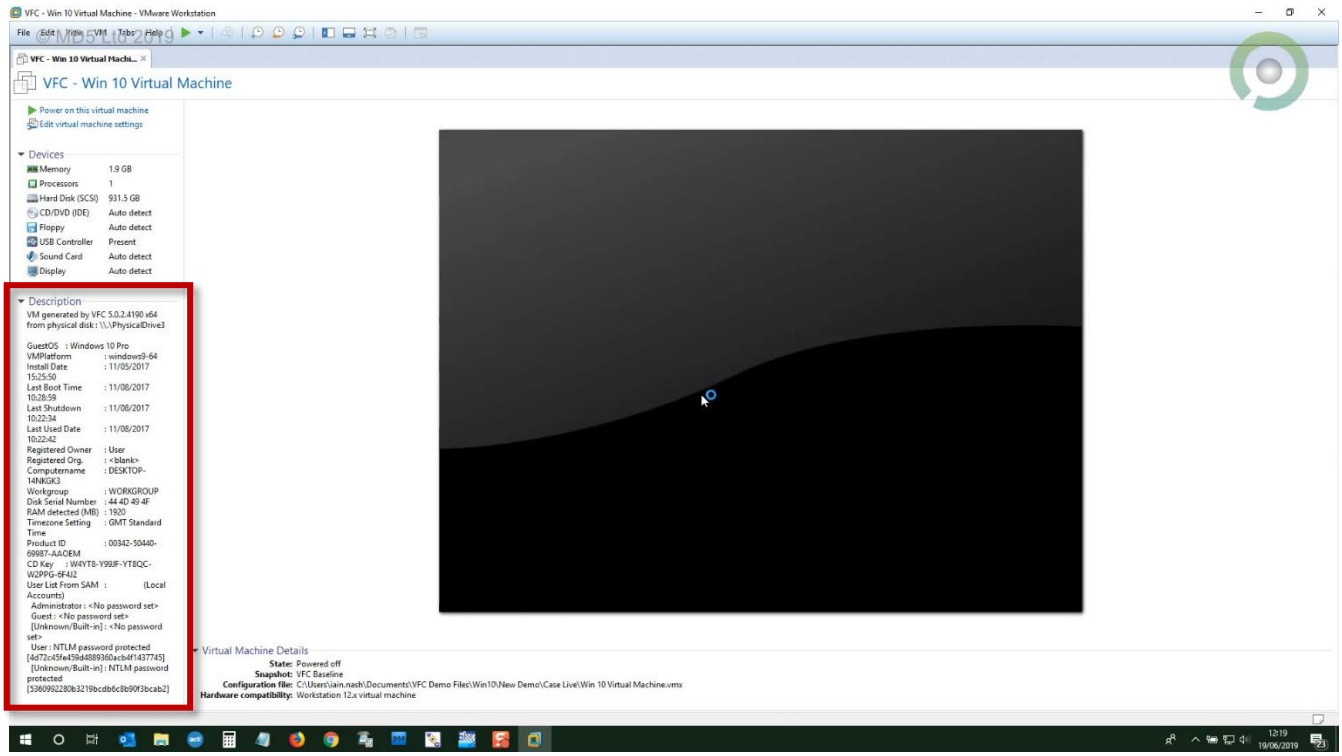
These values should be typically adjusted to reflect the details of the forensic image under investigation (e.g. Smith-PC1-HDD0). It can also help to name external drives (e.g. 8GB USB) so the bootable volume is easily recognisable when applying e.g. the Password Bypass routine.

Target System Information (TSI)

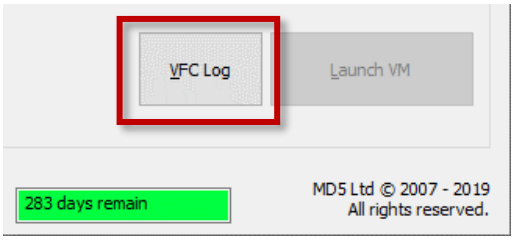
Key data pertaining to the Target System is displayed in the splash-screen on the home-screen of VFC, from where it can be highlighted with a mouse and copied and pasted into an electronic report. This information serves multiple purposes to the forensic investigator; from triage (via date of last use) through to identifying the presence of user access control features (User Account passwords):

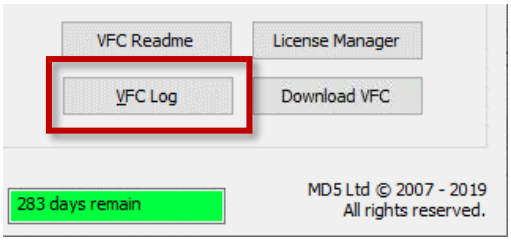


VFC5 also embeds the TSI in the annotation of the generated VMX file:



This TSI is also stored within the Log File which can be accessed via the "VFC Log" button (accessible via the Create VM tab or the About tab:



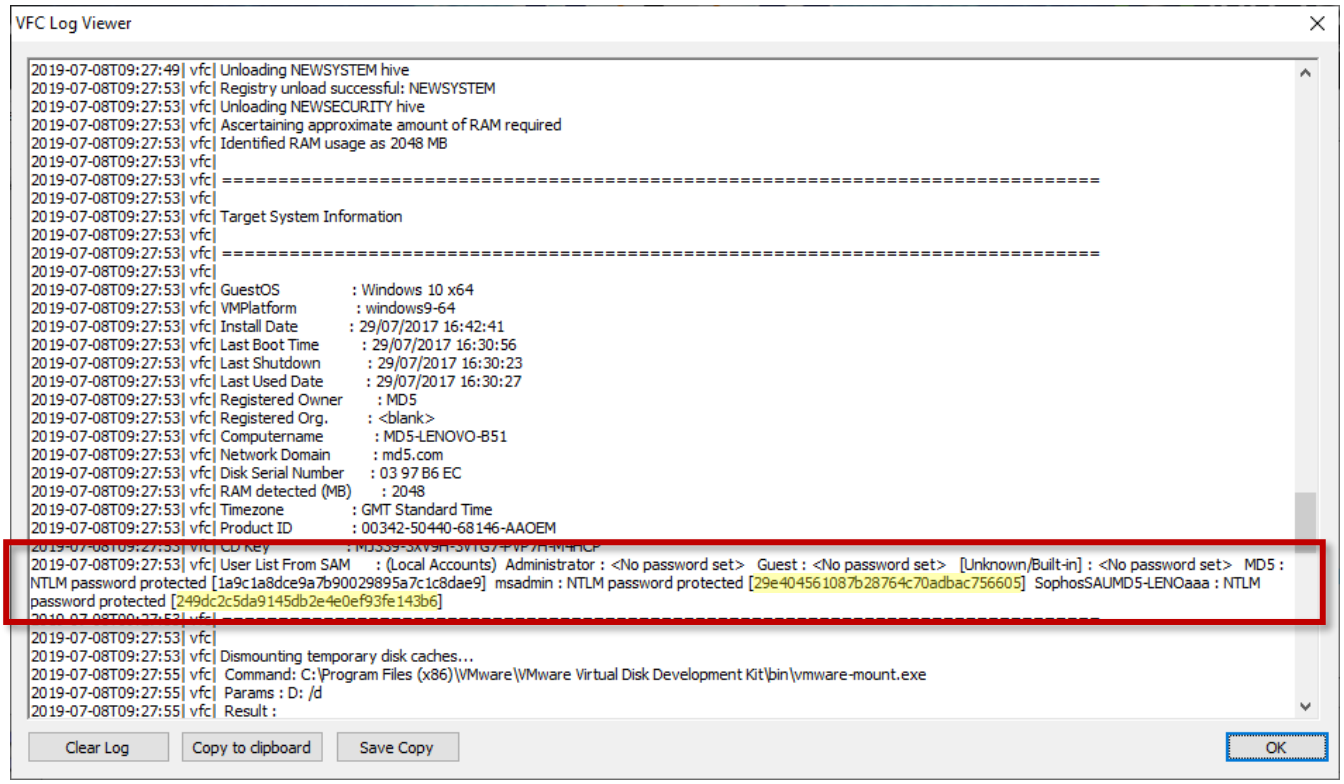


Using the TSI to Crack User Passwords

Using the user's original password to access a VM is always preferable where available, to avoid issues with user-encrypted data. The User's actual password can also offer clues to passwords used on websites or to access encrypted folders on the system and can also provide options to try on additional exhibits.

VFC collects TSI which includes the NTLM hash values for the passwords of password-protected User accounts. These NTLM hashes can be run through cracking tools to retrieve the original passwords.

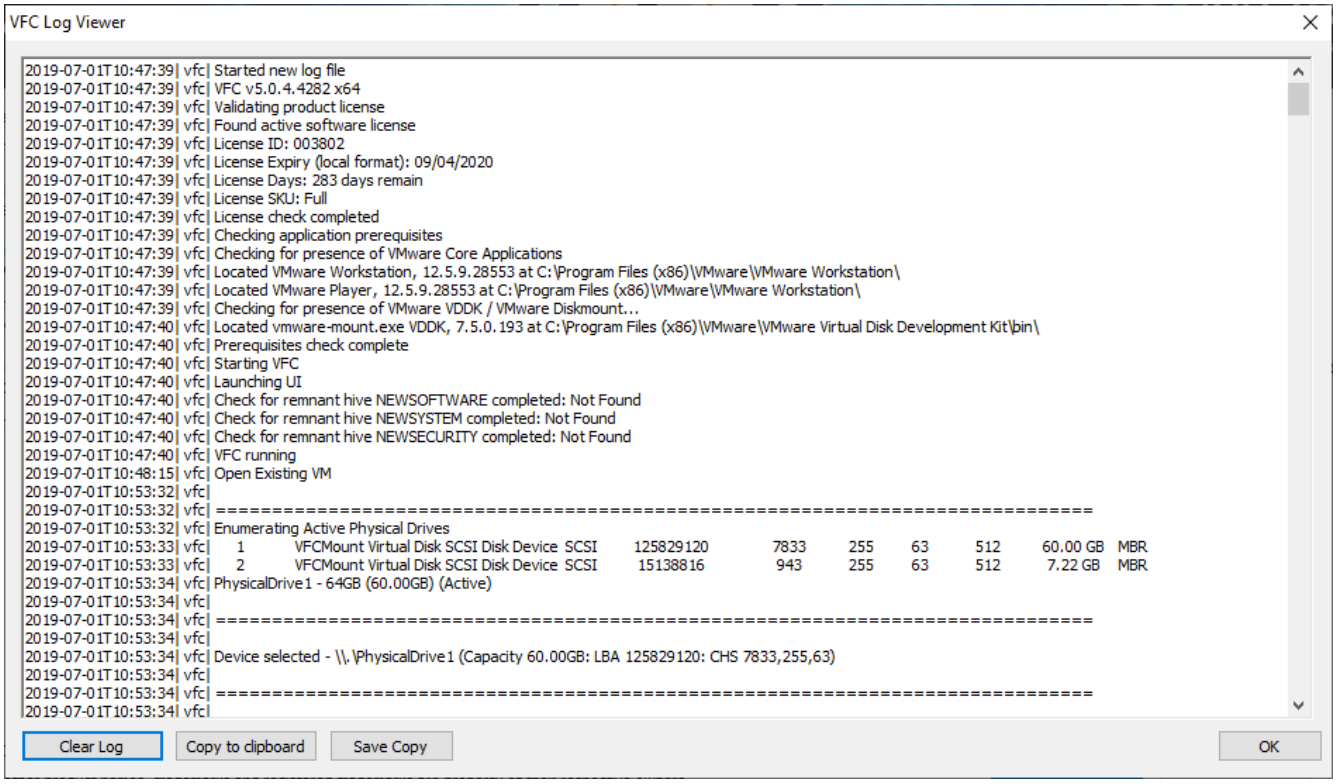
Recommended cracking options include offline rainbow tables and online solutions such as *www.hashkiller.co.uk* or the paid-for *www.crackstation.net*. Copy and paste the hash value from the end of the respective line (after the semicolon) and use your tool of choice to attempt to decrypt it.



The VFC Log File

For each session of VFC, a log file is created that records details about host software variants, host hardware and OS details and connected drives so that the VFC process can be replicated. When the log file is open, a copy can be saved at any time via the File Menu.

The log file can act as contemporaneous notes, to support an investigation and can also help with validation and verification for the international laboratory standard, ISO 17025. The log file records each step of the VFC process with time- and date-stamps, (measured against the internal clock of the host system). We recommend saving a copy of the Log file for each VFC VM generated.



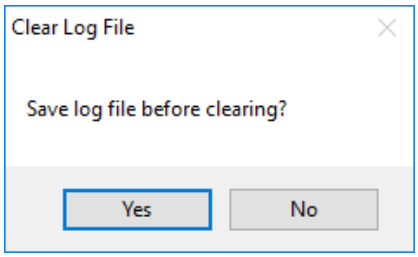
It is worth noting that unless the log is manually cleared, VFC creates one continuous log file for each session. It does not differentiate between cases or VM's.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Saving and Clearing the VFC Log File

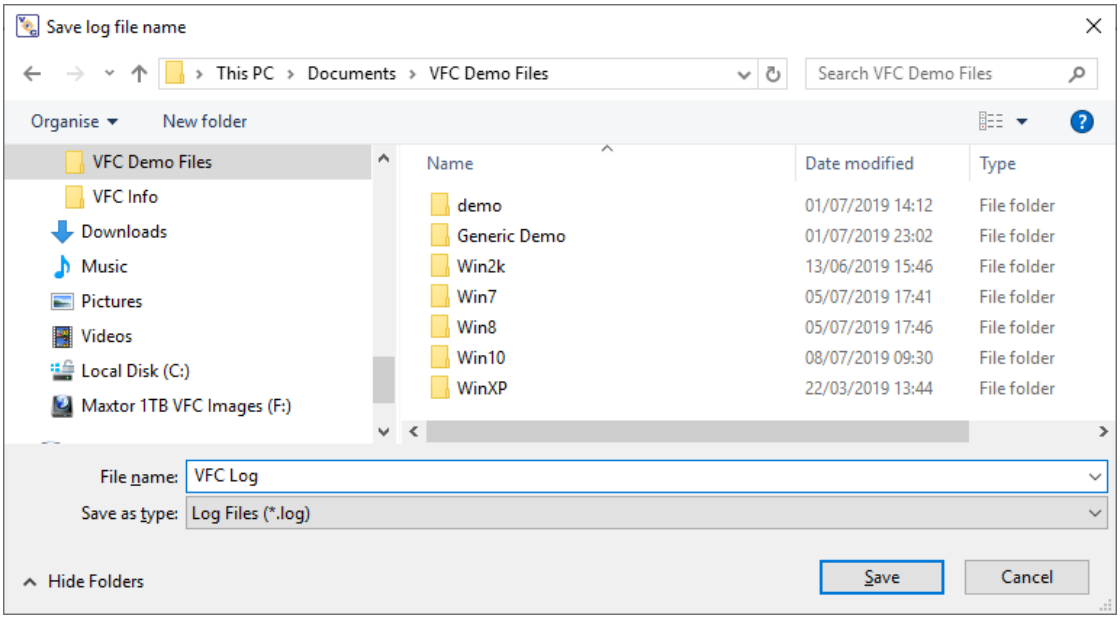
To avoid cross contamination of data from different cases or VMs, use the “Clear Log File” button within the log itself:

This will prompt you to choose if you want to save the log file or not*:



* … Click “Yes” to choose to save the previous log file (Recommended):

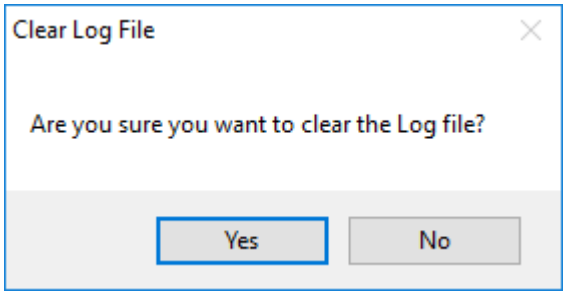
VFC will open File Explorer. Please confirm your save location, give the log a name and save the old file.



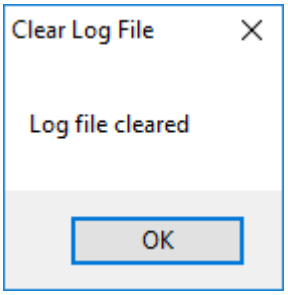
When you next open the log file, all details pertaining to any previously analysed disks will be missing.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

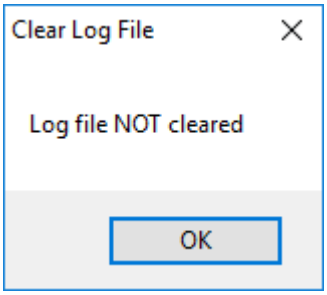
* … Clicking “No” will prompt you to confirm that you want to clear the log file:



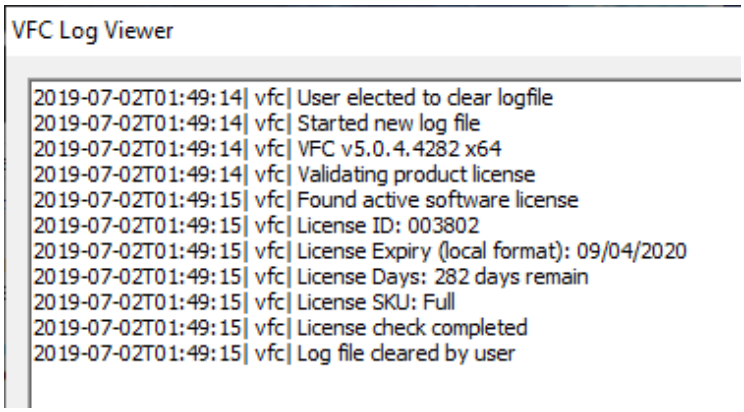
This will then deliver one of the following messages depending on your choice. Click “Yes” to clear the log file:



If you clicked the button in error, just click “No” and VFC will leave it as it is:



VFC will cleanse all data related to past virtualisations and just leave the basic system information pertaining to software variants etc:



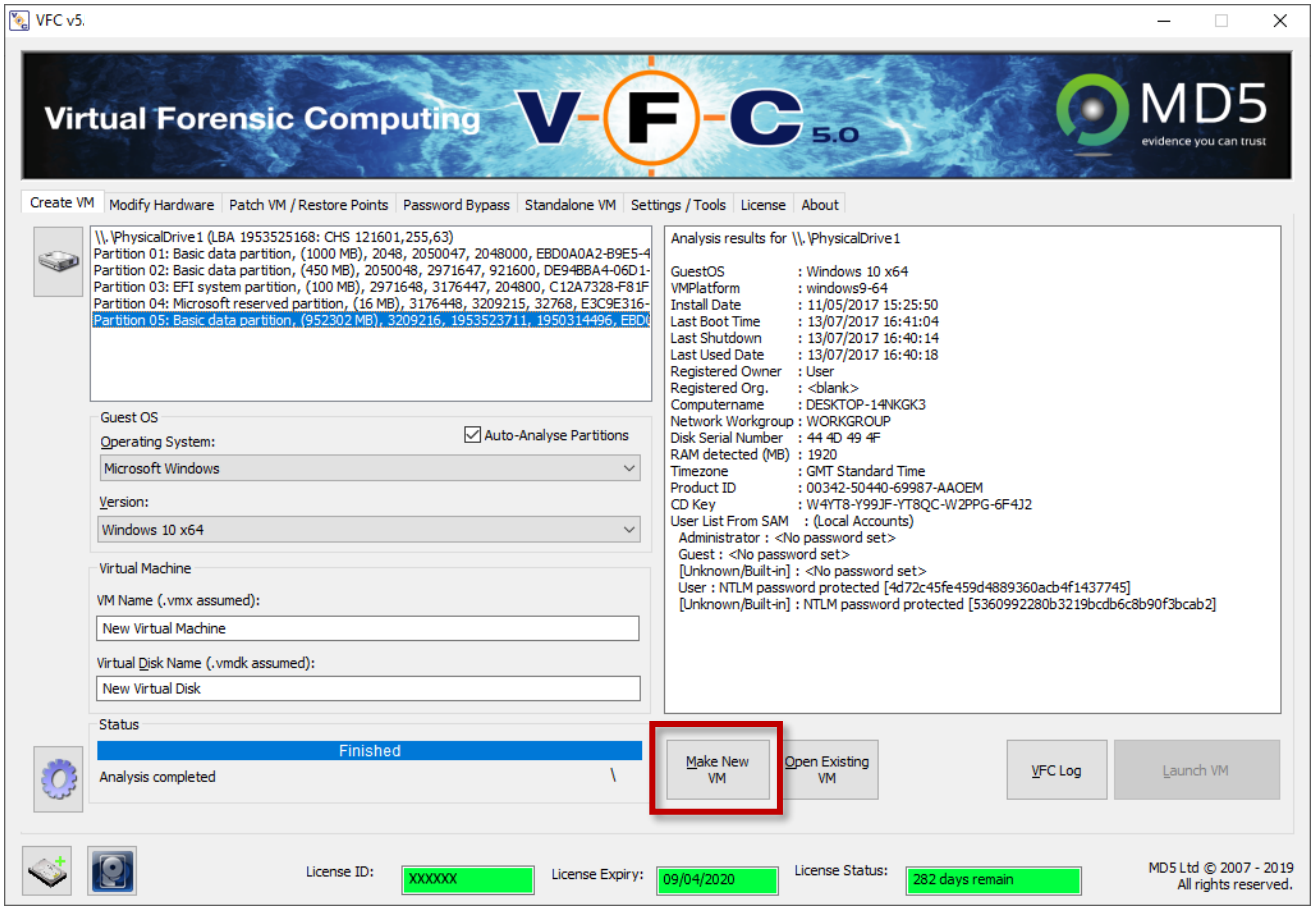
NB

The log file is a working document. VFC needs to write to it constantly to maintain the forensic audit trail of what has been done to the target system. If the log file is open, VFC will not work (you’ll see a blue circle instead of a cursor). As it says at the foot of the log file, “Please close the log file before continuing to use VFC”.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Generating the VFC VM

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.

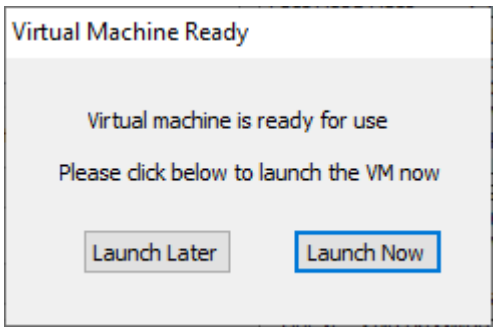


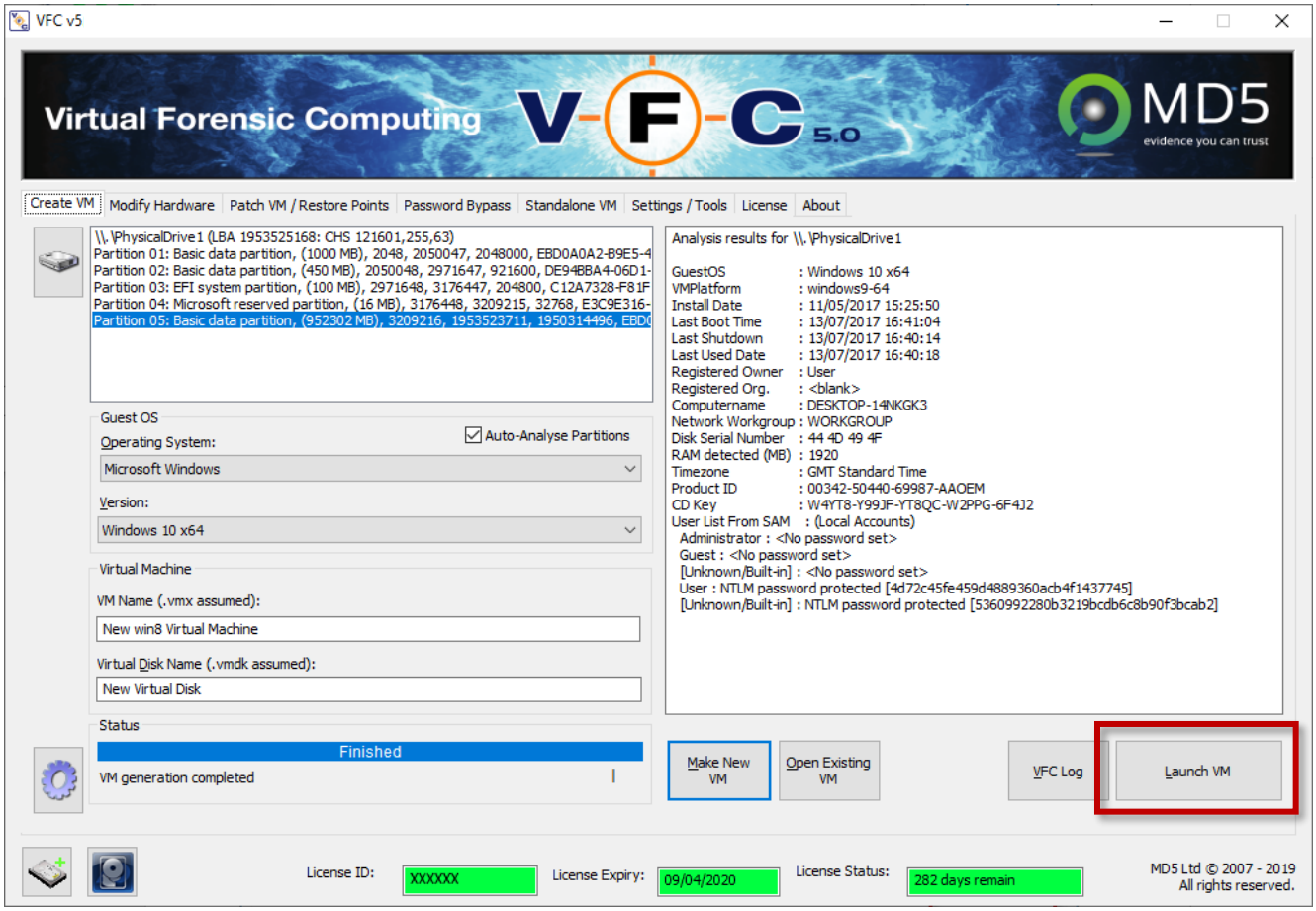
Click the 'Make New VM' button, select your Save destination, rename the VM if you wish to (if you haven't already) and wait for VFC to build the virtual machine.

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.

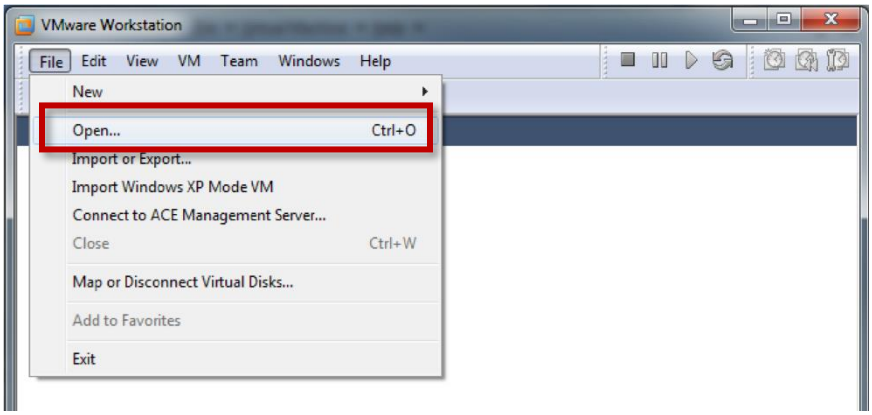
You can now choose to Launch your VM immediately or later:

The Option to Launch later was added so that users can add additional hardware into the VMX prior to booting it up. The Launch Now option removes one more mouse click from the VM generation process.



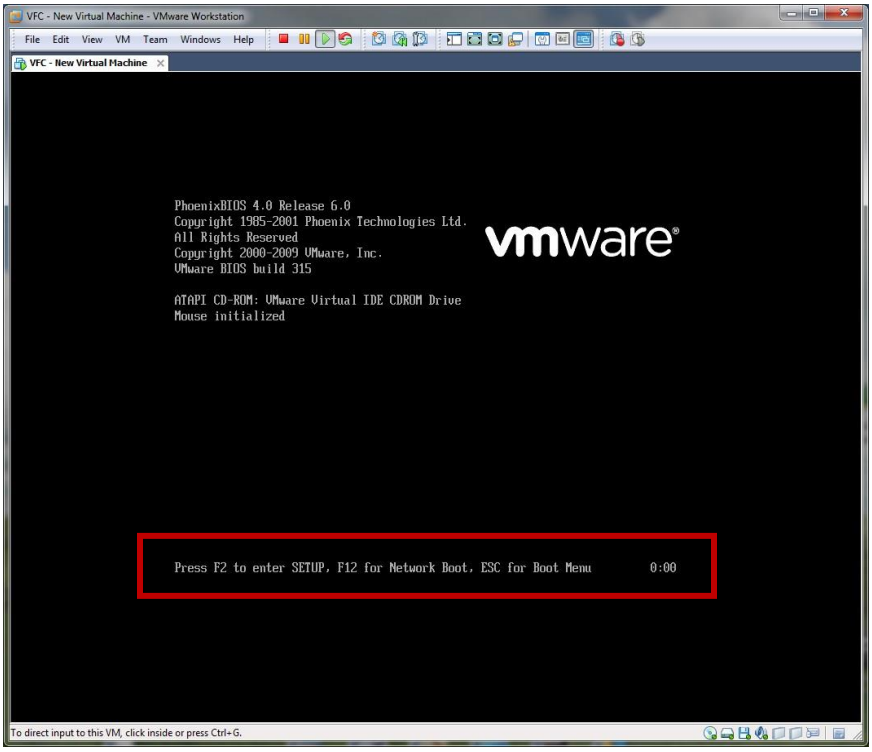


Alternatively, the machine can be launched manually, typically by either double-clicking the generated .VMX file via Windows Explorer, or by starting the VMware application and using the various options to Open a Virtual Machine.



Once the Virtual Machine has been manually opened, it will be necessary to 'Power On' the virtual machine (launching the VM via VFC will automatically power it on).

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 where 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 (e.g. make the mouse and keyboard work with the guest VM instead of your host machine).

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. You can also use the keyboard shortcut “Ctrl + Alt” to switch between inputs. Once you are focused on the VM, access to the virtual keyboard will be enabled and pressing the ‘Esc’ key will display the Boot Menu.

The Keyboard shortcut ‘Ctrl + Alt’ can also be ued to switch between VMware application key-entry (the main VMware window) and interacting with the VM itself.

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’.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Once the desired boot option has been selected (this is done 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.

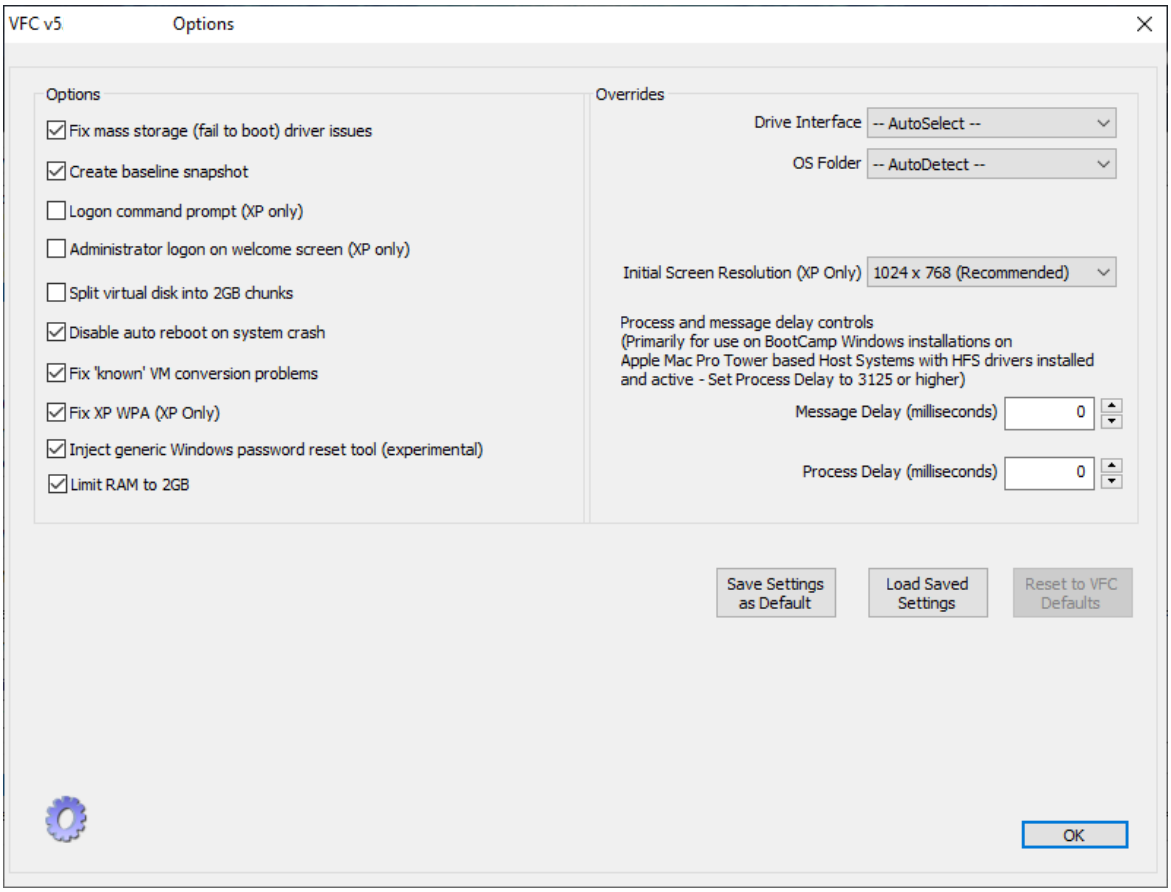
If the user account is password protected, it is possible (on Windows NT & above) to bypass the logon password by utilising the Password Bypass feature.

You can also use the Generic Password Reset tool to set the Password to a known value (including a blank value).

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Changing Default Behavior via the Options Button

On the home-screen, there is an “Options” button which will take you to a separate pop-up menu where you can tweak a number of settings within VFC:



If you are working with an encrypted drive (e.g. BitLocker) or your VM is stuck in a boot-loop repair cycle, you may need to tinker with these options.

Changing the drive interface can make a real difference. If the drive is encrypted, or VFC is struggling to communicate with it effectively, VFC won’t be able to read or make changes to the registry of the VM.

Many of the automatic fixes that VFC performs require access to the registry so to prevent them trying to run (and failing, resulting in a system crash), please untick the options on the left to e.g. “Fix ‘Known’ Errors” and select the correct Drive Interface then re-generate your VM based on these new parameters.

Please note as well, the Process Delay can safely be set to 0 to speed up the program. This was only ever implemented for some obsolete Mac hardware which could not handle the processes VFC was asking for while running Boot Camp Windows.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Password Bypass (PWB)

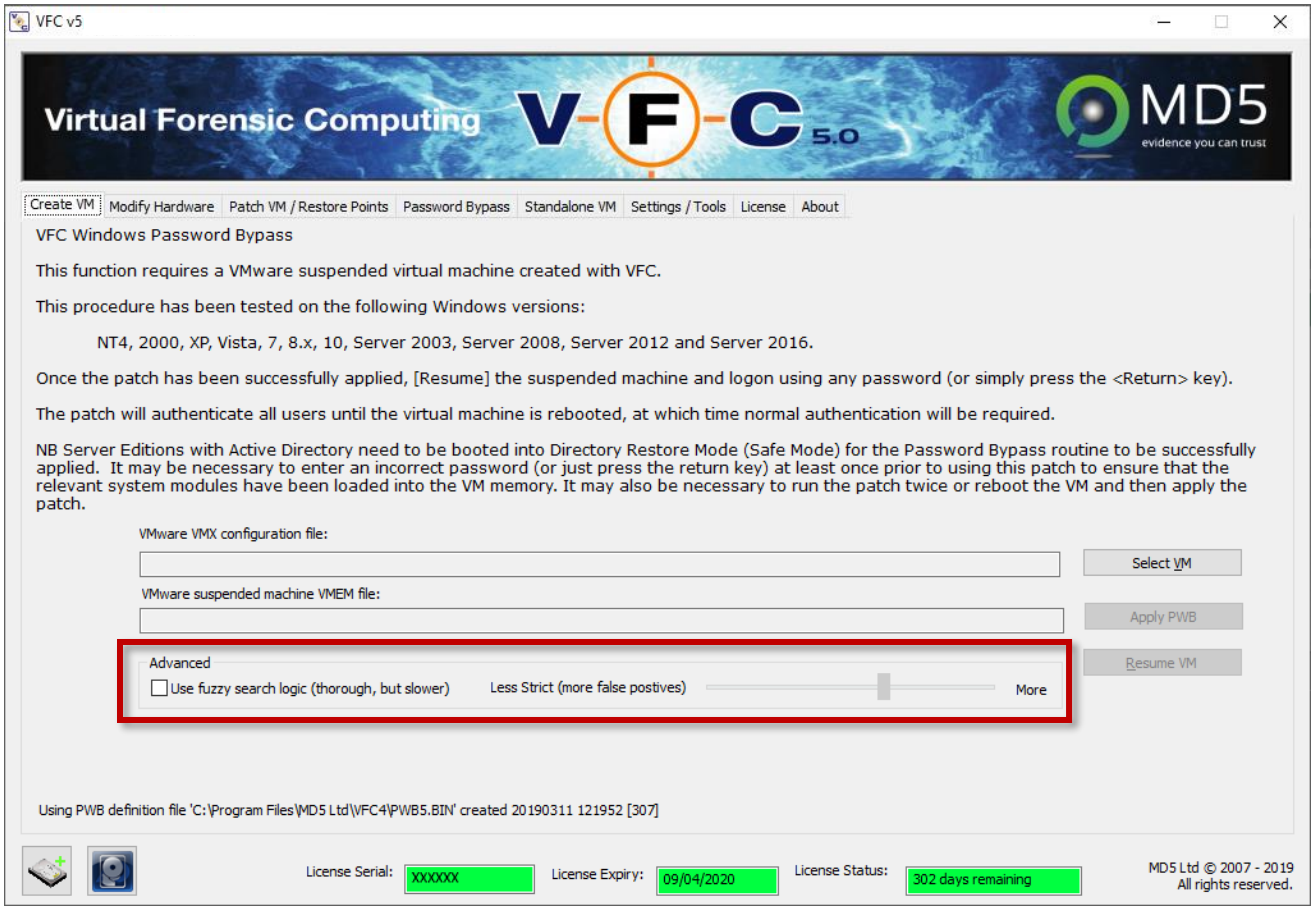
VFC incorporates a simple way to gain access to multiple local Windows User Accounts in a virtual environment via the enhanced Password Bypass (PWB) feature.

Please note, the VFC PWB routines ONLY work on Windows systems. We do not currently offer a PWB routine for Mac OSX User Accounts however tools and methods for bypassing them do exist.

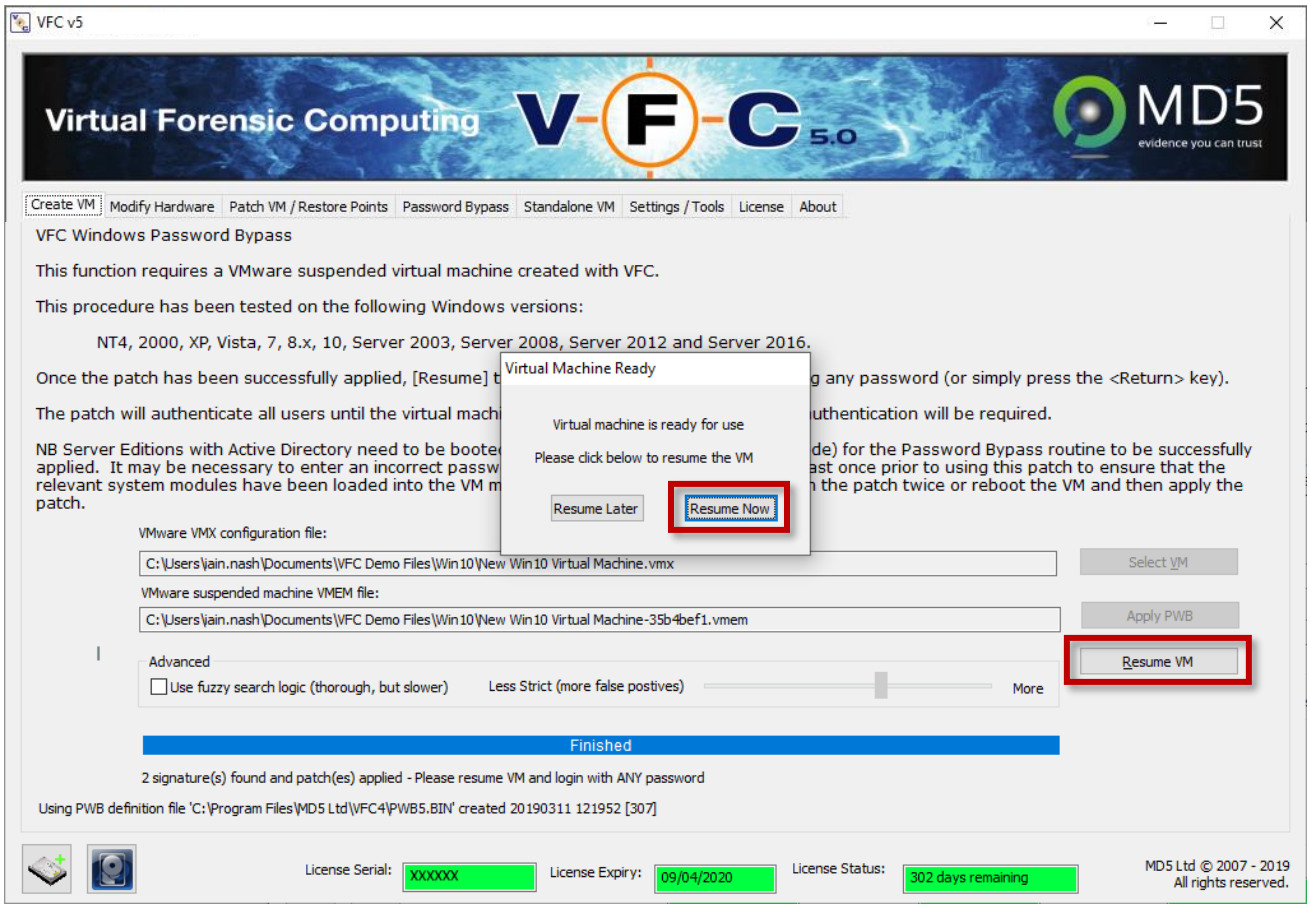
To use the PWB feature, when at the logon prompt of the VM (the VM must load completely for the PWB process to work), simply suspend the virtual machine in VMware (using the suspend button in the top menu – looks like a pause button), then open VFC and switch to the Password Bypass tab. Click "Select VM" and use VFC to select the required VMX file and then click "Apply PWB".

If the process fails to find a routine, you can open it up using the advanced "fuzzy search logic" slider to adjust the accuracy. PWB will then attempt alternative routines from other windows builds. It is more likely to have success but could take considerably longer.

To use this feature, tick the checkbox on the left and choose the level of focus you want to give to the routine using the slider:



Once the authentication routine is completed, click “Resume VM” and the virtual machine will ‘unpause’ and you will be able to access the user account without the need of a password. As the message states, you can also enter ANY password of your choosing and the VM will accept it.



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.

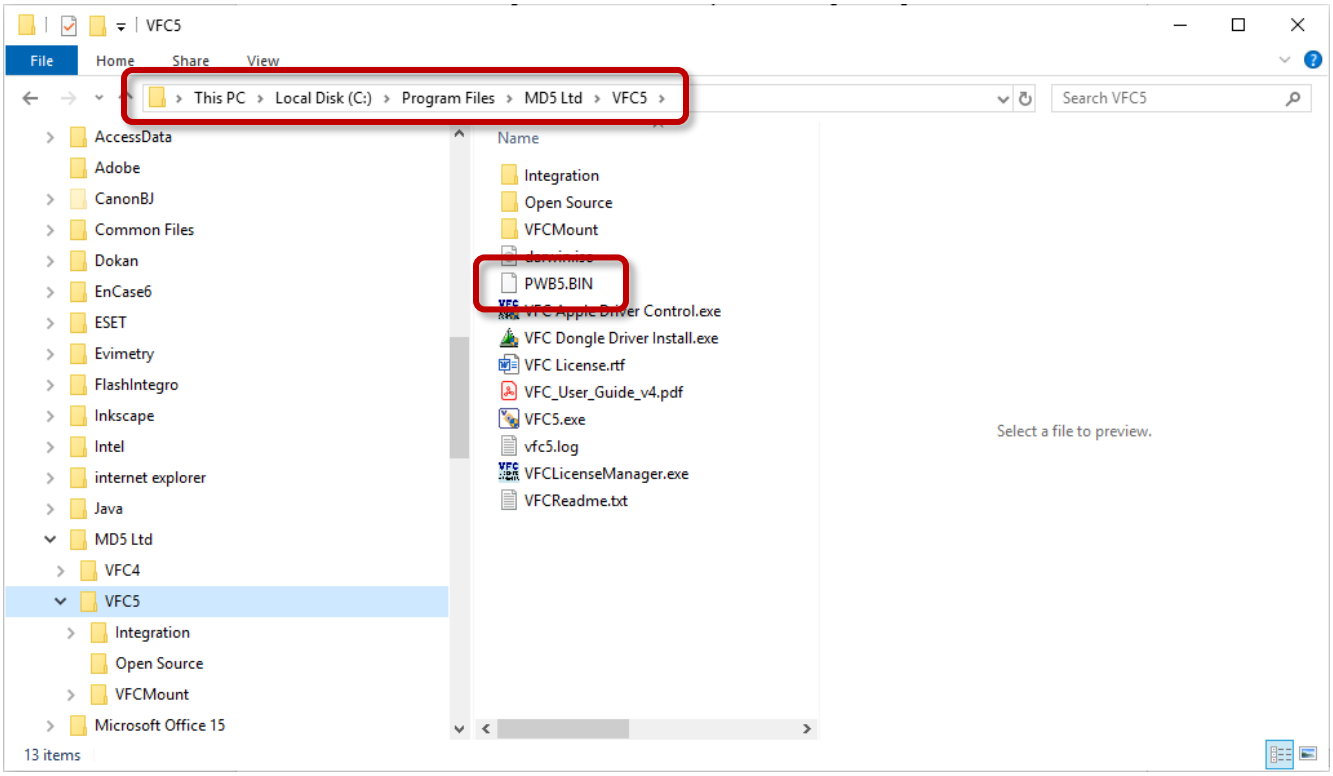
If the virtual machine is rebooted, memory will be reset and either the password must be utilised or the Password Bypass must be re-applied. No disk files are altered and the effect is transitory.

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.

If the PWB routine fails, you have 3 main options:

1. Check that the PWB5.BIN database is up to date (download updates from our website)
2. Use the Generic Password Reset (GPR) feature which is enabled in the Options screen
3. Crack the hashes listed in the Target System Information section, found both on the Create VM (home) tab and in the VFC Log file.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8



The Password Bypass (PWB) routine database is externalised for easier updates. VFC5 relies on PWB5.BIN updates. You will find the most up-to-date version of the PWB5.BIN file and other useful downloads online at:

http://md5.uk.com/vfc-downloads/.

Simply replace the PWB5.BIN file in your installation folder with the latest version to ensure you always have access to all available VFC PWB routines.

VFC5 supports Password Bypass on more than 2,000 different Windows OS Editions/combinations, subject to limitations created by encryption (e.g. BitLocker) and online logins (Live ID).

The VFC Password Bypass feature is under constant research and development. Updates to the PWB5.BIN file are released as often as possible and the latest version is always available to download from our website.

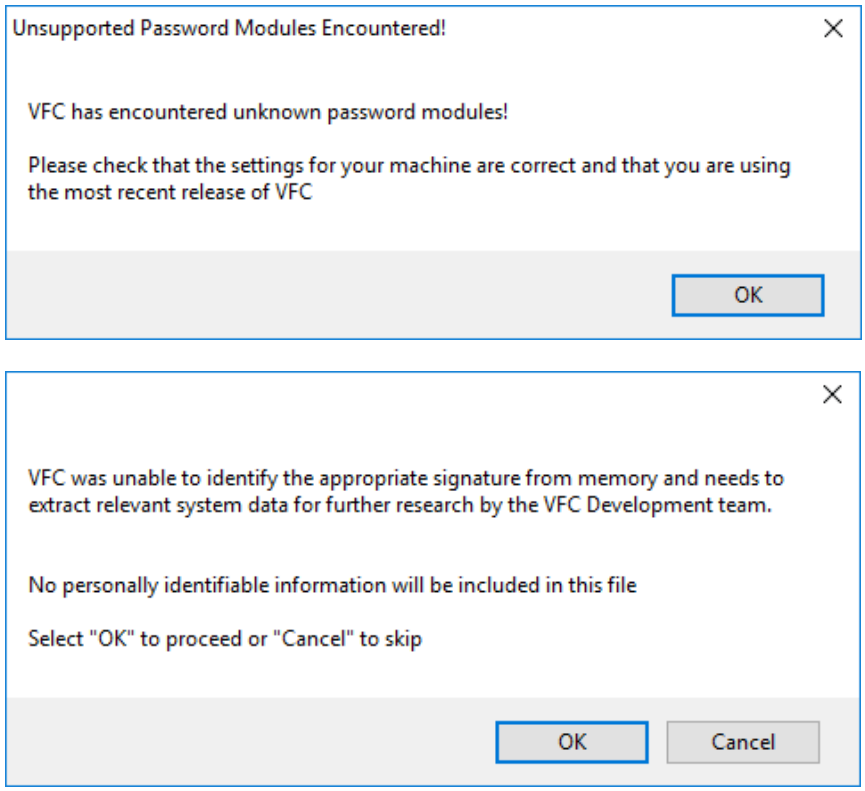
NB Older PWB.BIN files will not work with VFC v4.50 and upwards.

The Password Bypass feature does NOT work with online-authenticated accounts such as Windows Online (Live ID), which are linked to an email address or Live account.

The Generic Password Reset (GPR) feature can be used to access 'Live ID' accounts.

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 VFC.PWB file for return to the MD5 Development Team such that additional research can be undertaken. No user identifiable information is stored within the PWB file.

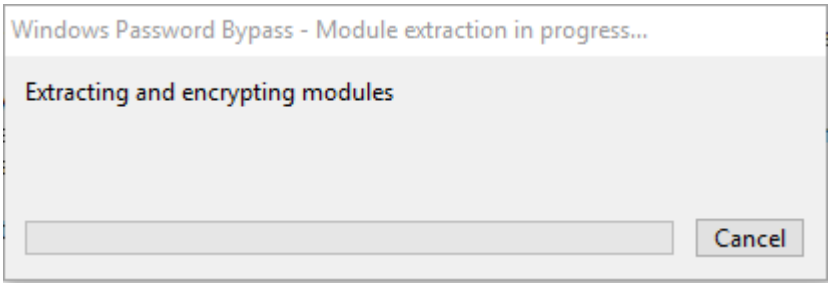
If the existing PWB.BIN does not contain the necessary patch, you will see the following message:

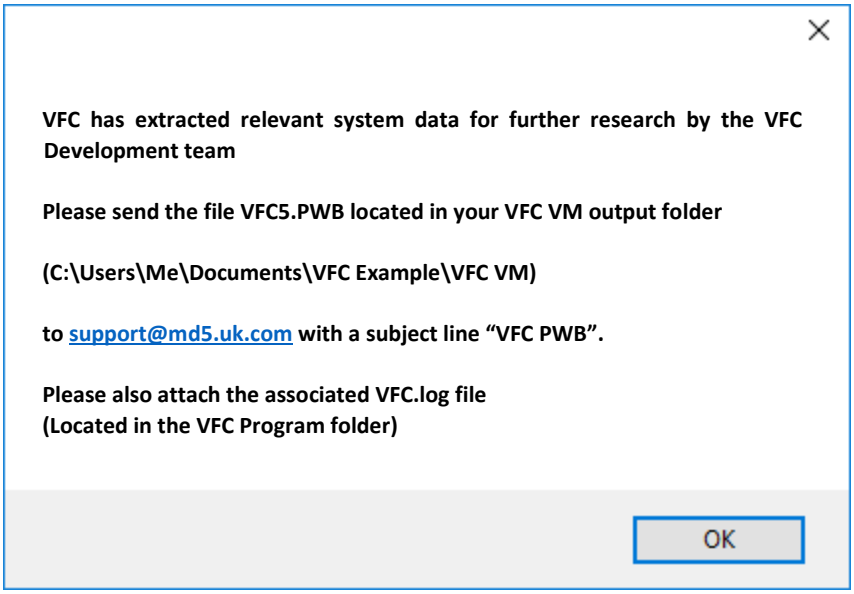


NB – If you run the password bypass routine when it isn't required, then this error message will still be shown. It will not affect the function of the VM.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

It will either be successful:

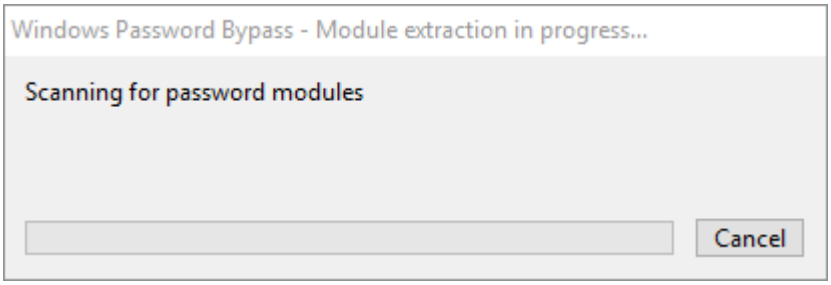


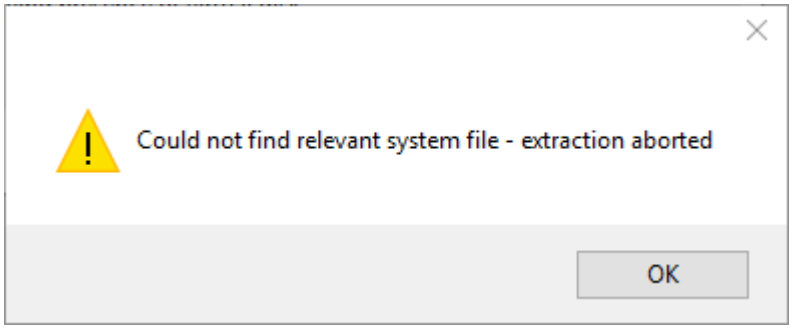


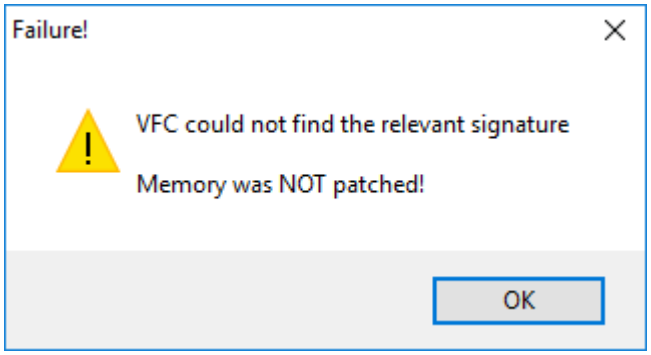
Please note the request for both the VFC5.PWB file **and** a copy of your VFC log file. This can be found in the VFC installation folder as guided, but can also be accessed from the either the "Create VM" or "About" tabs of VFC (click on "VFC Log" and then use the buttons to save a copy – don't forget to close the log file before continuing to use VFC). For more information on the Log File see here.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Or not:







This result can sometimes happen with a corrupted VM or if the image mounting has not been set up correctly. It is worth restarting the process from scratch if the process fails completely – or using the Generic Password Rest (GPR) tool.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

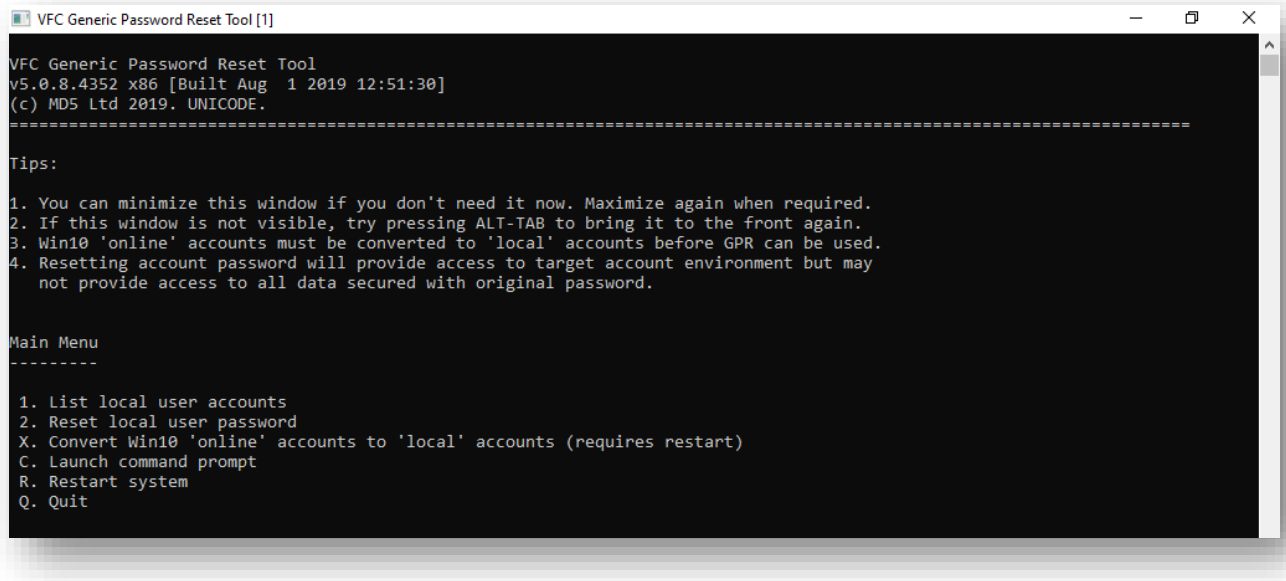
Generic Password Reset (GPR)

Includes Exploit for Windows Online (Live ID) accounts

New to VFC5, the Generic Password Reset (GPR) allows a user to:

- Change Windows Online (Live ID) user accounts to local user accounts
- Reset a chosen local Windows user account password to a known value
- Launch a Command Prompt with SYSTEM-level privileges

The GPR feature is completely separate to the legacy Password Bypass (PWB) feature and is very powerful. GPR is enabled by default in the "Options" screen (and can be disabled from here too). It works by injecting a proprietary VFC component directly into the VM. It launches as a console window on the login screen, which will normally appear a few seconds after the logon screen has loaded:



If the GPR features are not required (e.g. the password is known), it is recommended that you minimise the console window, in case it is required later.

The window can be resized to view more information and the scroll bars can be used to review information that may not fit on the screen.

The initial options presented are:

1. List local user accounts
2. Reset local user password
X. Convert Win10 'online' accounts to 'local' accounts (requires restart)
C. Launch command prompt
R. Restart system
Q. Quit

List the local user accounts and their password status(es) by pressing "1":

```
-------------------------------------------------------------------------------------------------------------------
User#          : 0
Username       : Administrator (Admin)
Display name   :
Password reset : Not set
Last logon     : Not set
Properties     : (Account disabled) (Password never expires)
-------------------------------------------------------------------------------------------------------------------
User#          : 1
Username       : DefaultAccount (Guest)
Display name   :
Password reset : Not set
Last logon     : Not set
Properties     : (Account disabled) (Blank password permitted) (Password never expires)
-------------------------------------------------------------------------------------------------------------------
User#          : 2
Username       : defaultuser0 (User)
Display name   :
Password reset : 2019-08-02 10:35:11
Last logon     : 2019-08-02 10:30:38
Properties     : (Account disabled) (Password never expires)
-------------------------------------------------------------------------------------------------------------------
User#          : 3
Username       : Guest (Guest)
Display name   :
Password reset : Not set
Last logon     : Not set
Properties     : (Account disabled) (Blank password permitted) (User cannot change password) (Password never expires)
-------------------------------------------------------------------------------------------------------------------
User#          : 4
Username       : virtu (Admin)
Display name   : virtual forensic
Password reset : 2019-08-02 10:33:18
Last logon     : Not set
Properties     : (Password never expires)
-------------------------------------------------------------------------------------------------------------------
User#          : 5
Username       : WDAGUtilityAccount (Guest)
Display name   :
Password reset : 2019-08-02 10:31:57
Last logon     : Not set
Properties     : (Account disabled)
-------------------------------------------------------------------------------------------------------------------

6 user accounts found
```

Display name is included as this will sometimes differ to the system-allocated default Username (see User # 4, above).

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Change a password to a known value by pressing "2":

Option 2 lets you change the password for a specific (single) user account. Please note, you need to enter the system name so this is the value given for "Username" not "Display name":

Hopefully it will work first time:

```
Reset Password
--------------

Username (ENTER to exit): MD5
Password: Password1
Password successfully changed to "Password1" (9 characters)
```

If it fails, you may need to try a more complex password:

The new password must meet the security requirements defined by the local Windows security policy. Typically, this could mean the password needs to be a minimum length and contain a variety of characters. If the local security policy demands a specific mix of characters and/or a certain number of characters, unless all these parameters are met, the reset feature may not work first time.

With this in mind, VFC will prompt you to try a more complex password – e.g. alphanumeric or with a mix of cases or including some symbols etc:

```
Reset Password
--------------

Username (ENTER to exit): MD5
Password: Password
Password "Password" (8 characters) does not meet requirements. Try a more complex password.
```

```
Reset Password
--------------

Username (ENTER to exit): MD5
Password: Password1
Password successfully changed to "Password1" (9 characters)
```

Depending on the security policy settings, you may need to try a number of times to enhance the security of your replacement password before the VM will accept it.

GPR may identify that the account is a domain account or online "Live ID" account:

GPR can only reset local Windows user accounts (just like PWB will only bypass local accounts). If it fails, it will highlight that the target account could be an online account:

```
Reset Password
--------------

Username (ENTER to exit): virtu
Password: 1234
The system is not authoritative for the specified account and therefore cannot complete the operation.
Is the account a domain or 'online' account?
Suggestion: Try converting 'online' accounts to 'local' accounts and try again.
```

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Change 'online' (e.g. Live ID) accounts to local accounts by pressing "X":

If the target account is an 'online' account, you can convert this to a local account by pressing X:

```
Converted 1 'online' user account(s) to 'local' account(s).
Please restart before attempting to login.
```

After making system level changes to change an online account to a local account you need to restart the guest system for the changes to take effect. Once this change has been made and applied, the normal GPR process (or the legacy PWB process) can be applied:

```
Reset Password
--------------

Username (ENTER to exit): virtu
Password: 1234
Password successfully changed to "1234" (4 characters)
```

Launch a Command Prompt from the GPR window by pressing "C":

The Command Prompt gives you access to powerful system-level administrator functions.

Restart the system by pressing "R":

GPR includes a simple solution to a quick reboot – just press "R".

```
Preparing to restart...Please wait
```

Exit GPR and disable the feature by typing "Q".

You can then utilise the legacy PWB process in the manner described above. Clicking the red X will only close the window temporarily. To quit, press "Q".

It is recommended that if you don't want to use the GPR tool, you minimise the window.

GPR can be used to permanently reset or remove passwords from standalone clones prior to export.

NB *The appearance of the GPR window is not the application of the legacy PWB bypass routine but a totally separate and new process, run entirely within the VMware environment.*

It should be noted that GPR is a proprietary routine that is permanently applied to the VM it is injected into. If the virtual machine is rebooted, the new password must be utilised or the Password Bypass must be re-applied. Virtual disk files are altered and the effect is permanent.

Please note, neither PWB nor GPR currently support bypass of domain authenticated passwords. This is a key focus of current research and we hope to provide a simple solution in the near future.

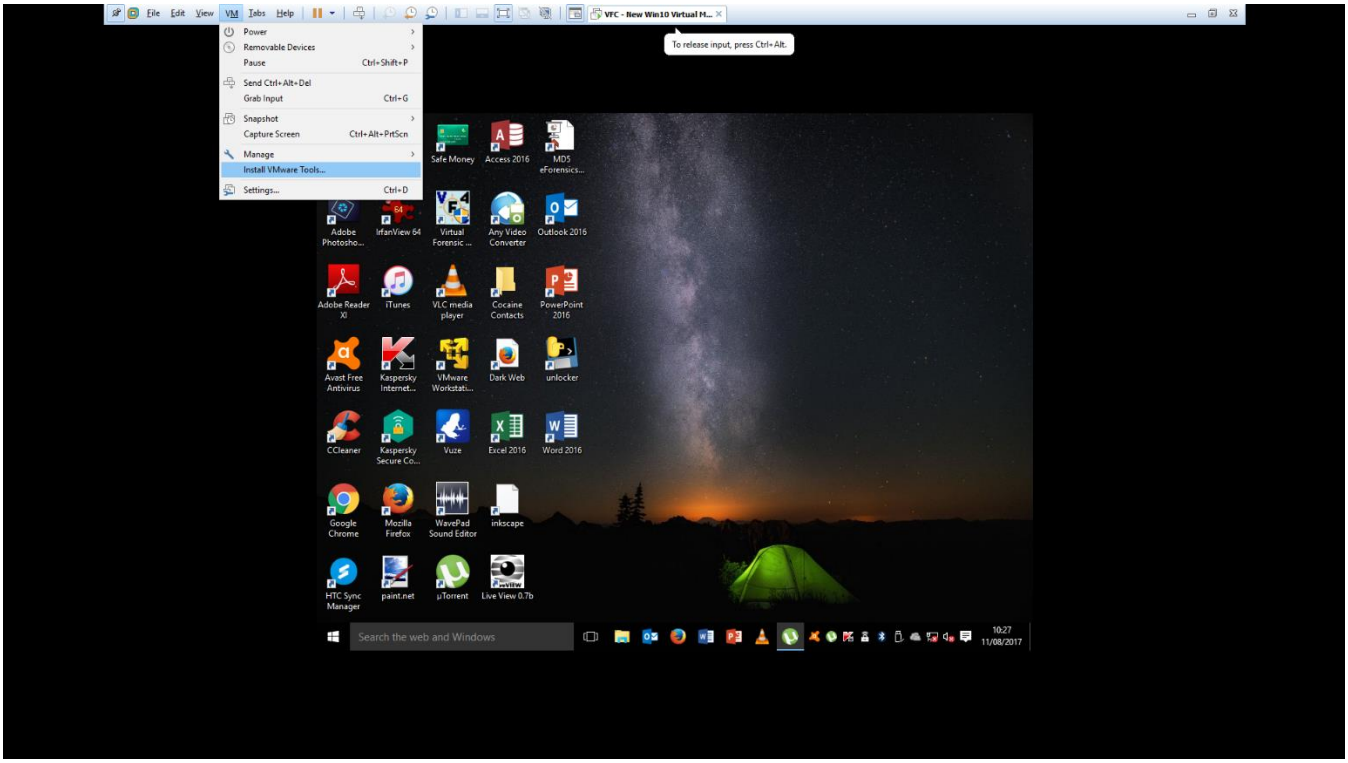
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Experiencing the User's Desktop

Once you have successfully accessed the desired account, depending on the OS and the hardware employed on your host system, the installed Guest 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). It is also likely you will need to reboot the VM at least once before it is completely functional.

Some drivers will become available after the installation of the VMware Tools package (see next page), others (e.g. Sound on Windows Vista) may require additional manual intervention. VMware Tools will also fix a number of other irritating things like screen resolution settings and jumpy mouse tracking and will also enable features for advanced interaction with the guest system (more on next page).



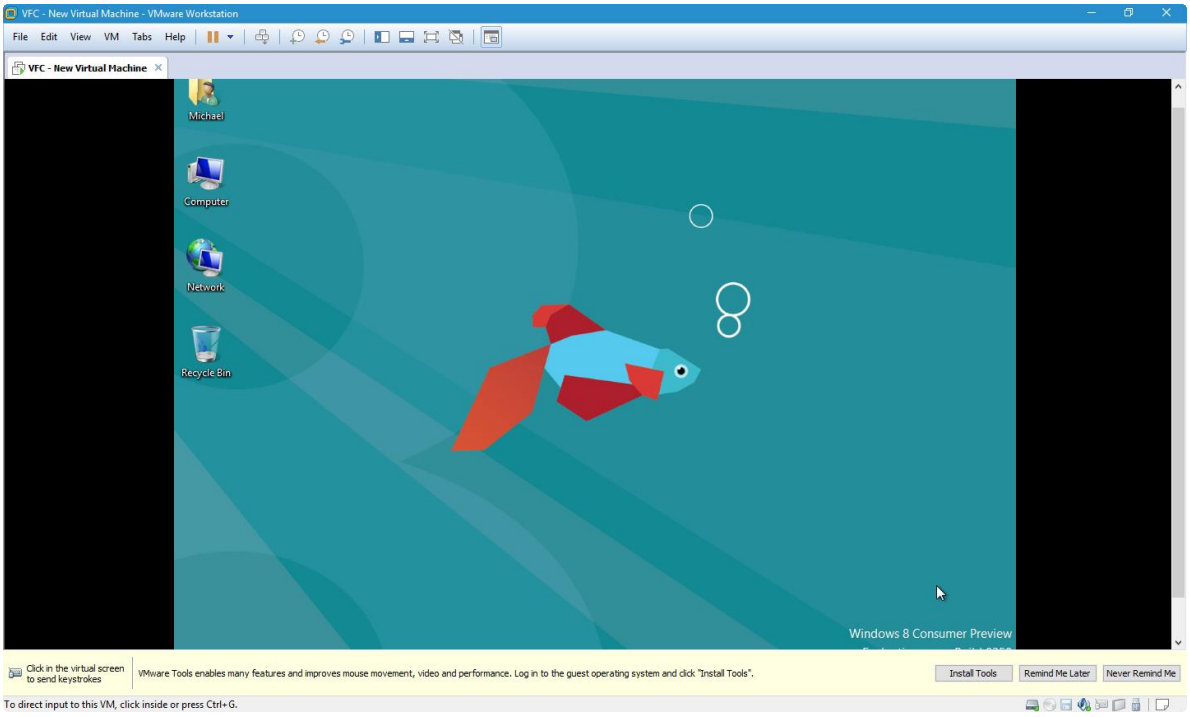
VMware Tools Installation

In most instances, we recommend the installation of VMware Tools. The time taken for this will vary depending on the guest OS and the host hardware. Follow the onscreen prompts or drop down from the VM menu in VMware to start the installation wizard.

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 recreate the original environment), it should be noted that the installation procedure will most likely generate a System Restore Point event.

Equally, if you are planning on rewinding the machine to an earlier point using System Restore functionality (and the VFC Restore Point Forensics patch), this will effectively remove the installed Tools from the system and they will need to be installed again anyway.



Once the VMware Tools are installed, it is necessary to restart the machine for configuration changes to take effect. During the reboot process, 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 using the options available within VFC (Currently applicable to Windows XP only). Pre-adjusting resolution may avoid unwanted desktop icon relocation.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

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 this icon 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.

(https://docs.vmware.com/en/VMware-Workstation-Pro/15.0/workstation-pro-15-user-guide.pdf)

Modify Hardware (add additional hard drives, network cards etc.)

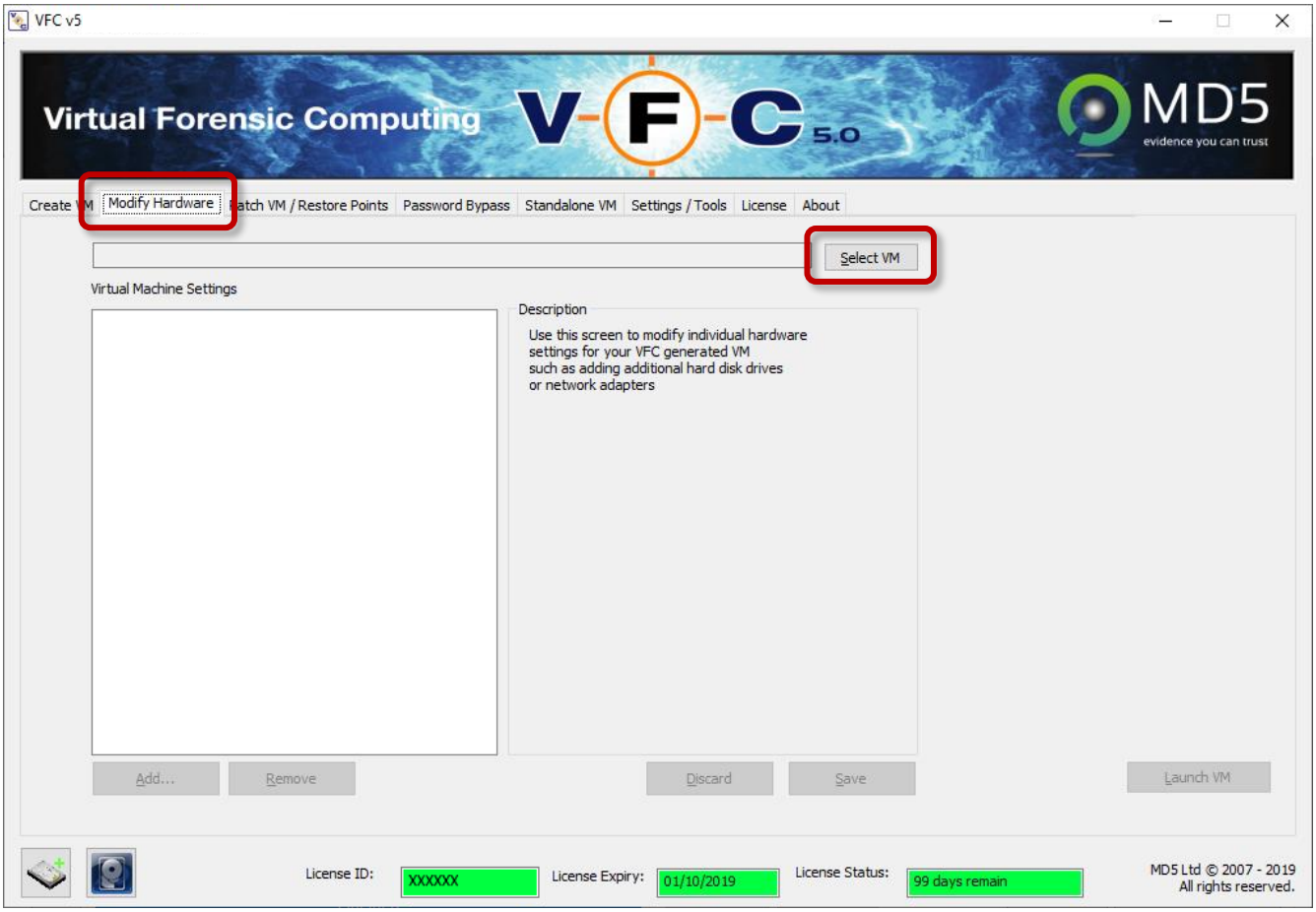
VFC enables you to add hardware and rebuild a complete physical setup as a single virtual system. You may have seized a tower PC with multiple drives or a laptop with an external drive or USB flash drive attached. The Modify Hardware tab allows you to stitch these seamlessly into your VM, whether you're using VMware Workstation Pro or Player.

The Modify Hardware tab allows you to modify a VM you have already created. You can use this to add additional mounted drives or make other minor changes to the VM configuration directly from within VFC. Alternatively, you can make these (and more complex) changes from within VMware; the outcome will be the same.

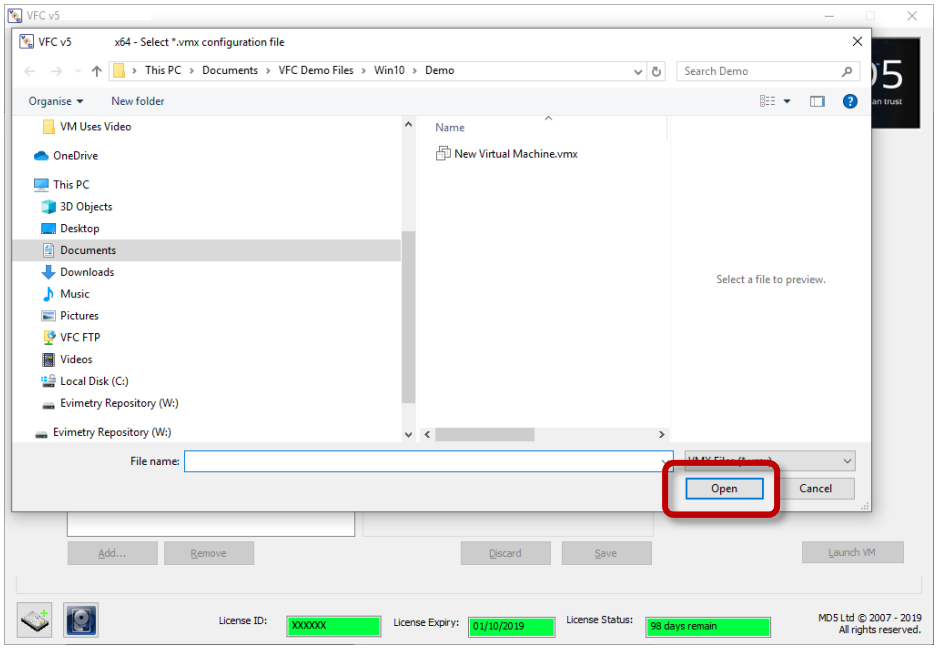
This feature works from physical drives, just like VFC itself when building a VM. Mount or attach any additional drives or hardware in the same manner you would to create a VM in the first place.

Best practice is to mount ALL drives before you begin to use VFC however if you run into problems, the Settings/Tools tab can be used alongside the mounting options in VFC Mount to mitigate further issues.

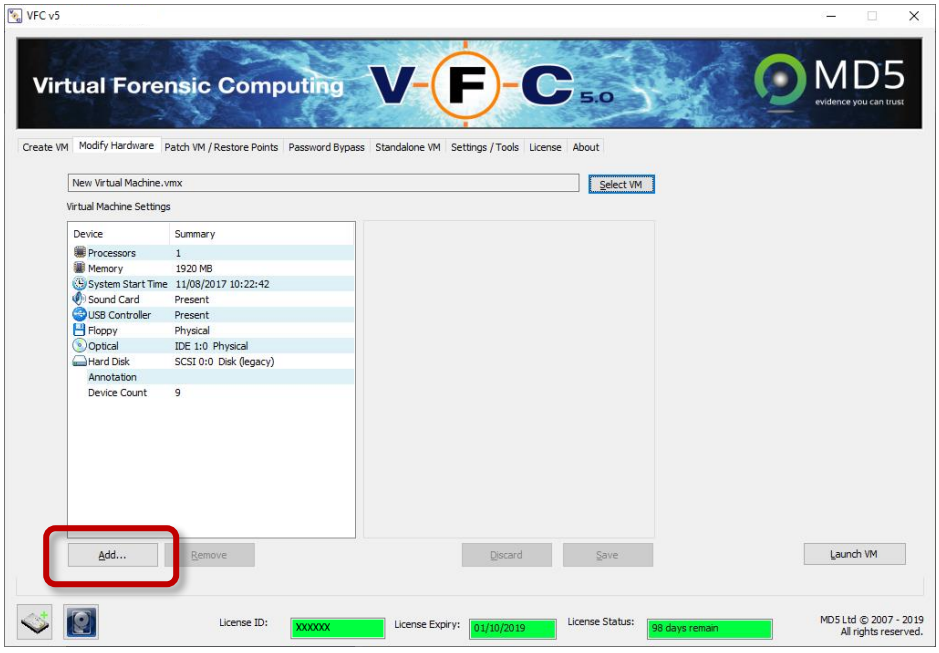
Navigate to the Modify Hardware tab and click on "Select VM" to choose the VM you want to add to:



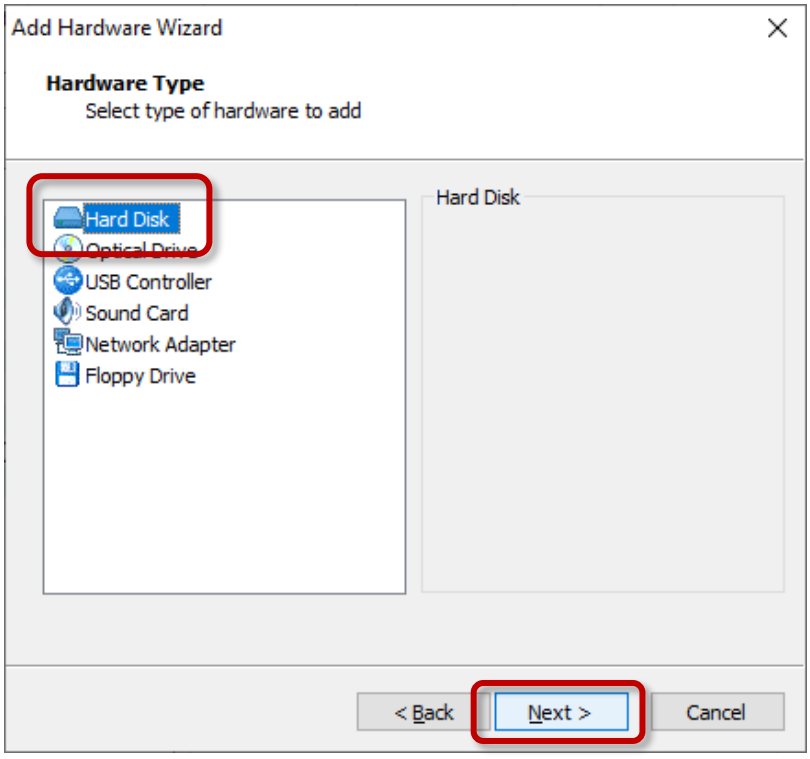
Browse to the VMX you need and click “Open”:



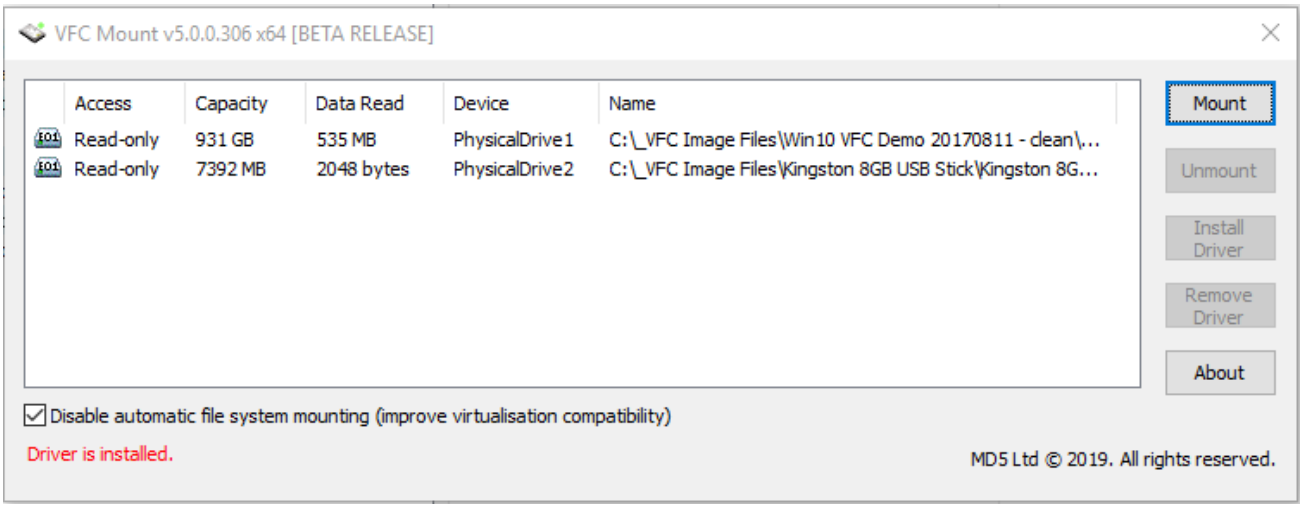
You will see a list of virtual hardware that is connected to the VM. To add hardware, click “Add…”:



Select the type of hardware you're adding (in this example, we're adding a Hard Disk) and click "Next":



If the drive you want to add is not mounted, VFC Mount (or your preferred mounting tool) can be employed to add the required image at this time:

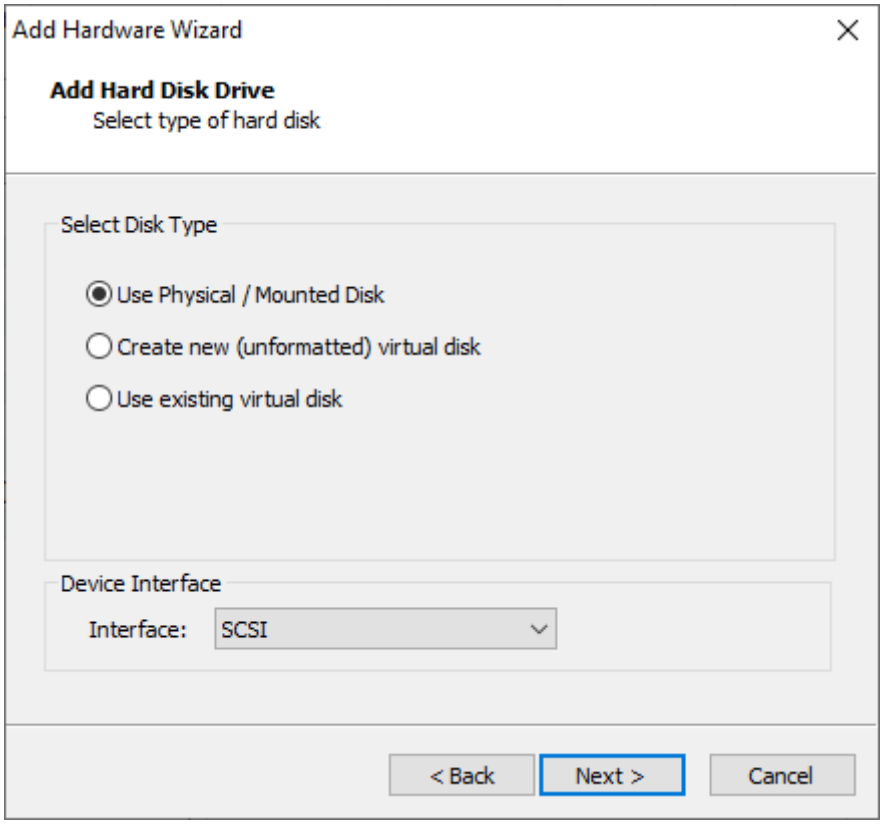


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Choosing the correct Drive Interface

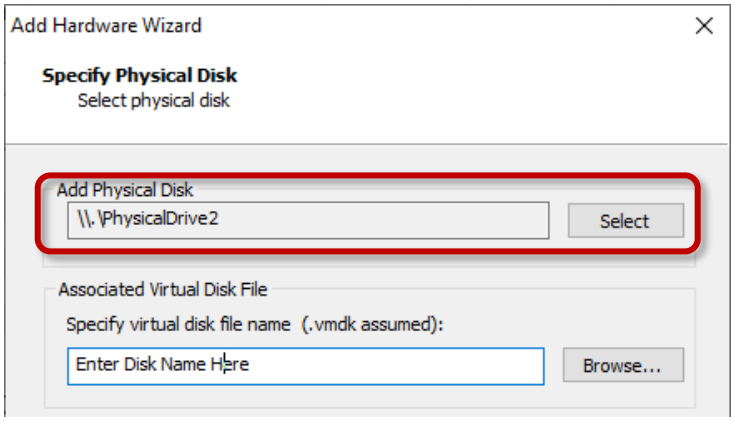
Once you've selected the hardware you want to add, the Add Hardware Wizard will prompt you to choose the type of drive (if applicable) and the Drive Interface.

We recommend that you use the SCSI drive interface in most cases. This is the default preferred by VFC and likely to cause the fewest problems. If this fails to work, we would recommend you select the drive interface used for the original physical disk (typically SATA for modern systems).

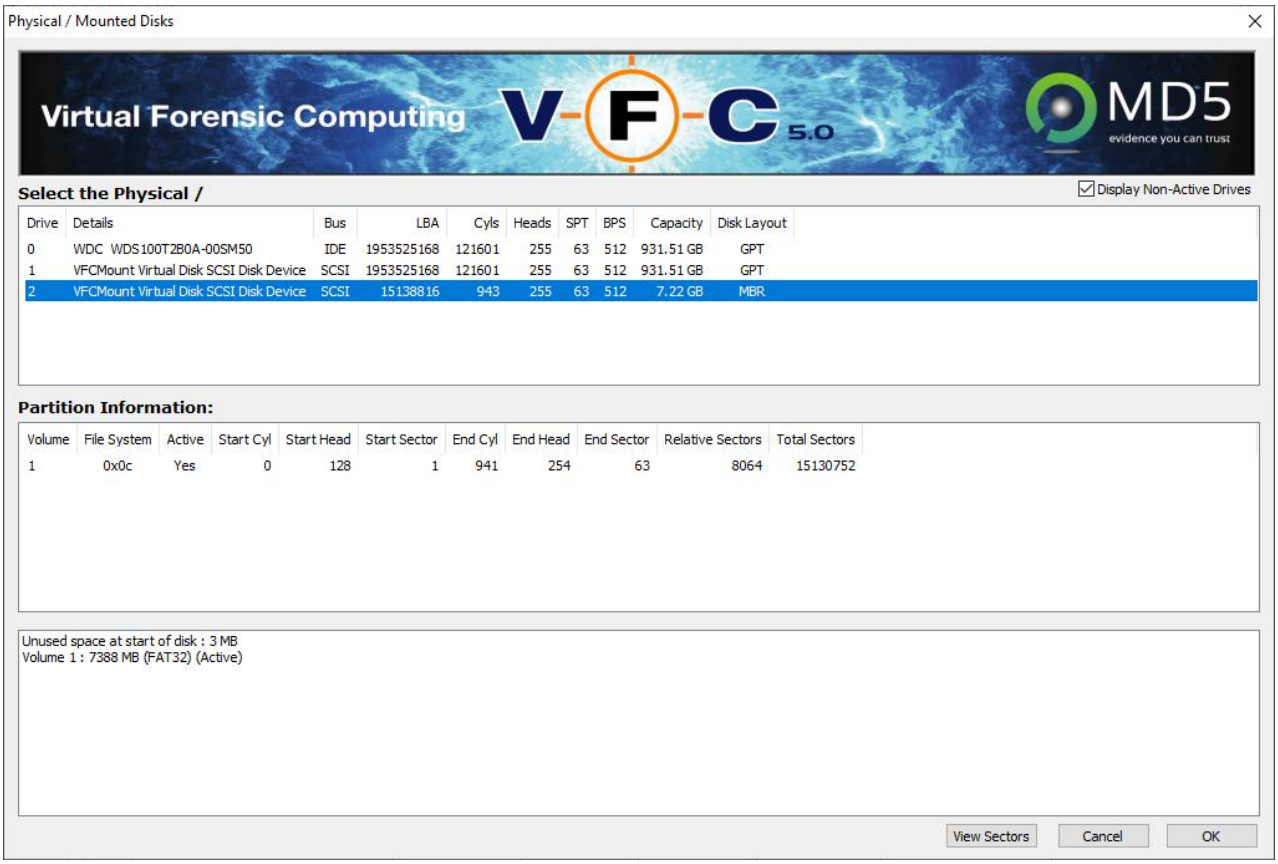


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

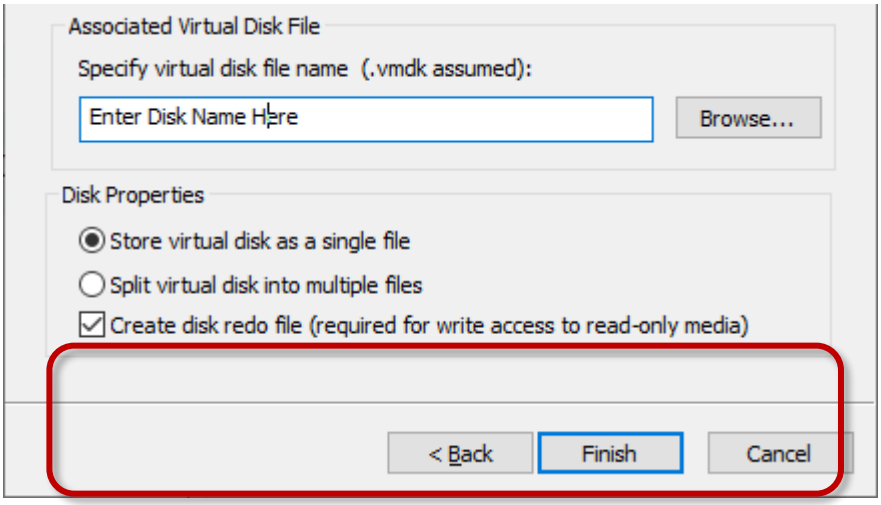
VFC will prompt you to select the virtual drive (VMDK) you want. Simply click “Select”:



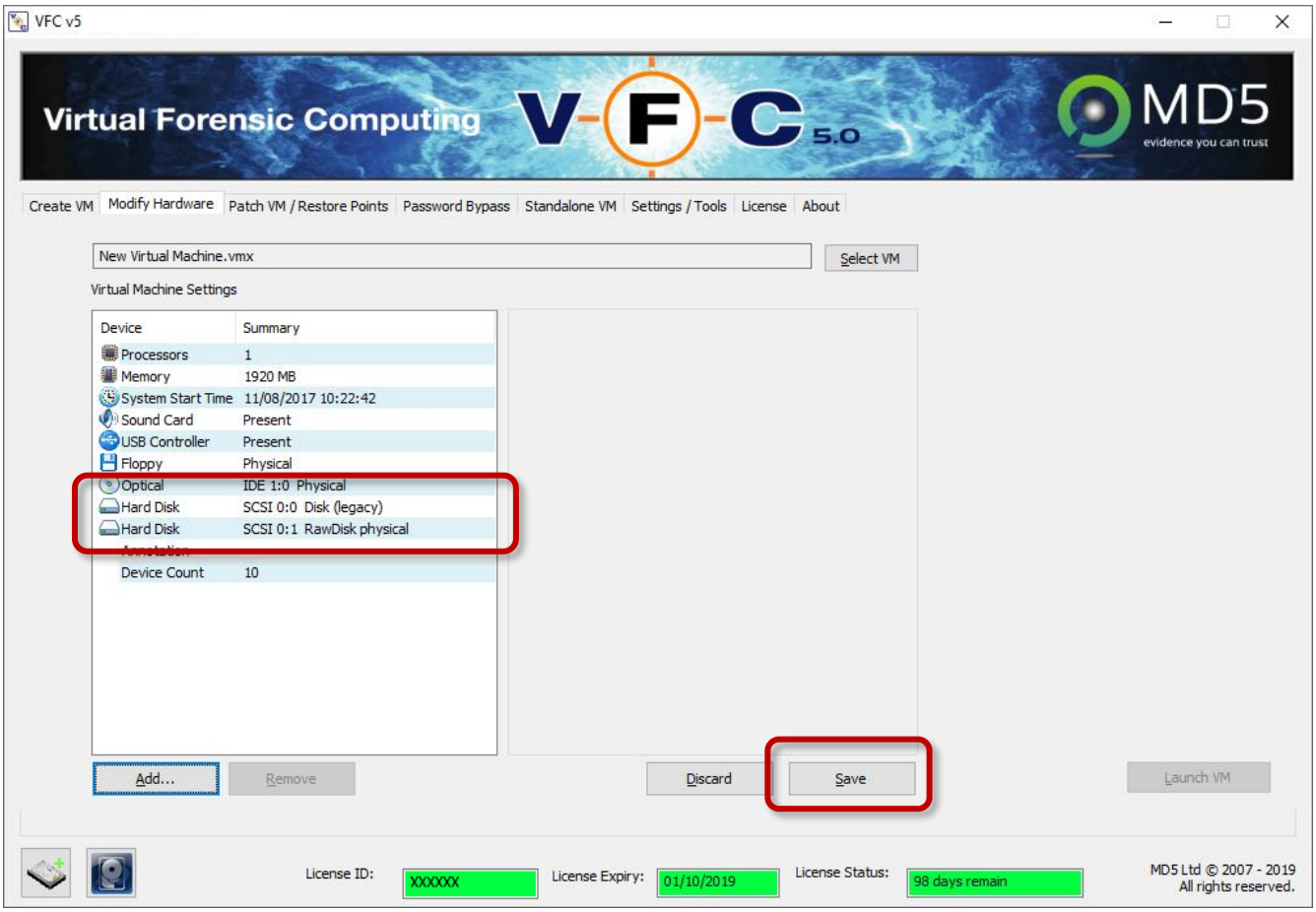
VFC will re-enumerate the connected drives. Select the option you want:



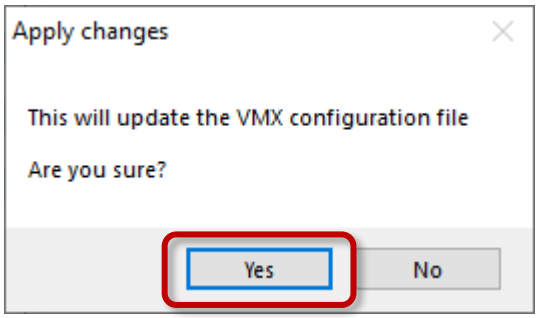
Next, give your new virtual disk (VMDK) a name and flick “Finish”:



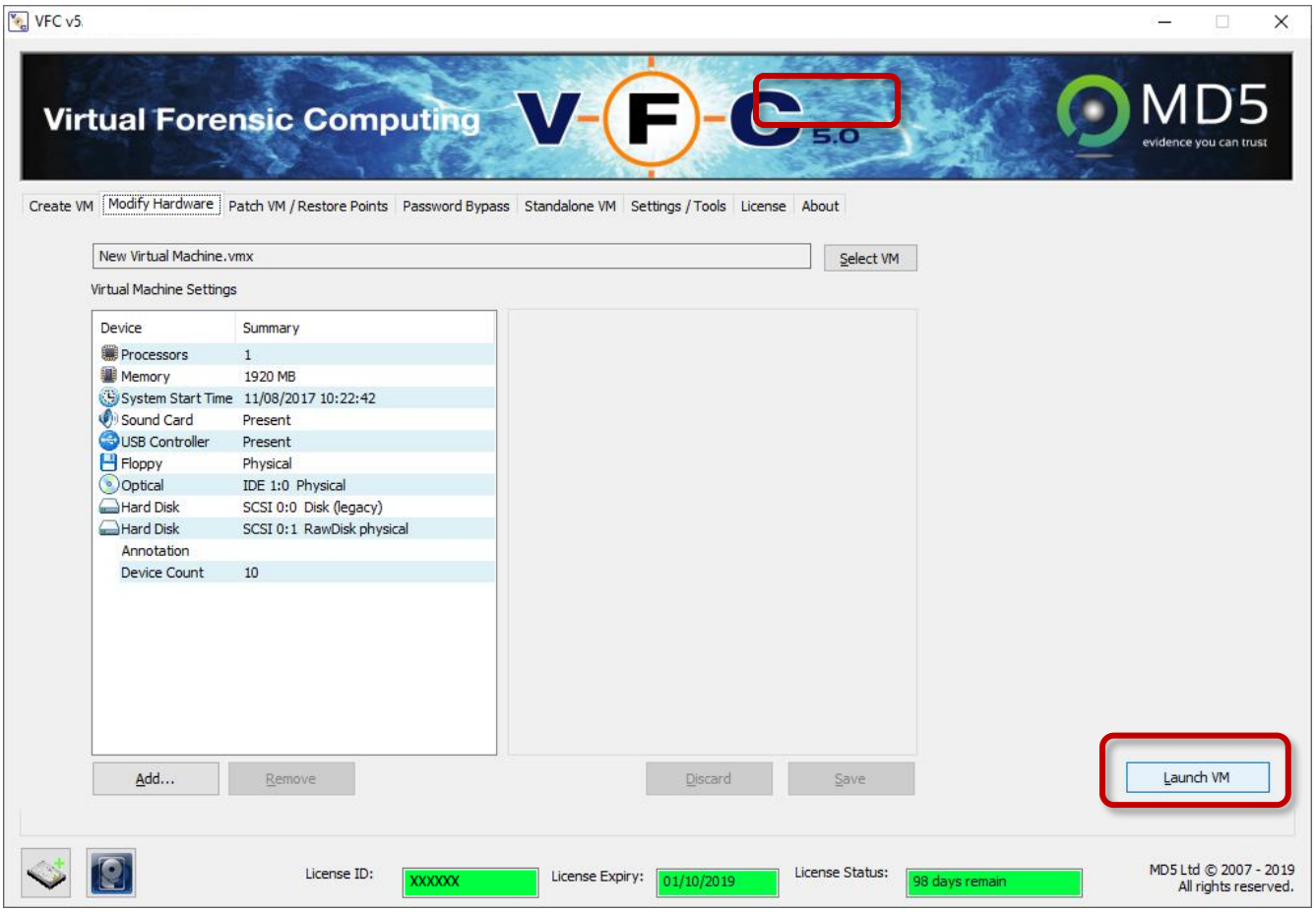
VFC will now display an updated hardware list which should now show multiple hard disk drives. You will need to click on “Save” to update the VMX configuration file before you can Launch the VM:



VFC will check you want to apply the changes. If you're happy, click "Yes" to accept. Alternatively, if adding more drives, you can do this before you update the configuration file to make all the updates in one go (in which case, select "No"):

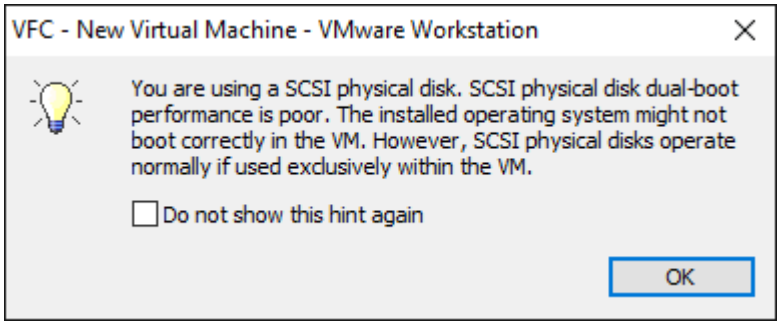


VFC will now give wake up the "Launch VM" button. Click this to launch the VM in VMware:



VFC will load the VMX into VMware and automatically power on the VM so that it boots up automatically. Alternatively, you could browse for and open the VMX directly or use the File>Open menu options within VMware but these will also require you to Power On the VM.

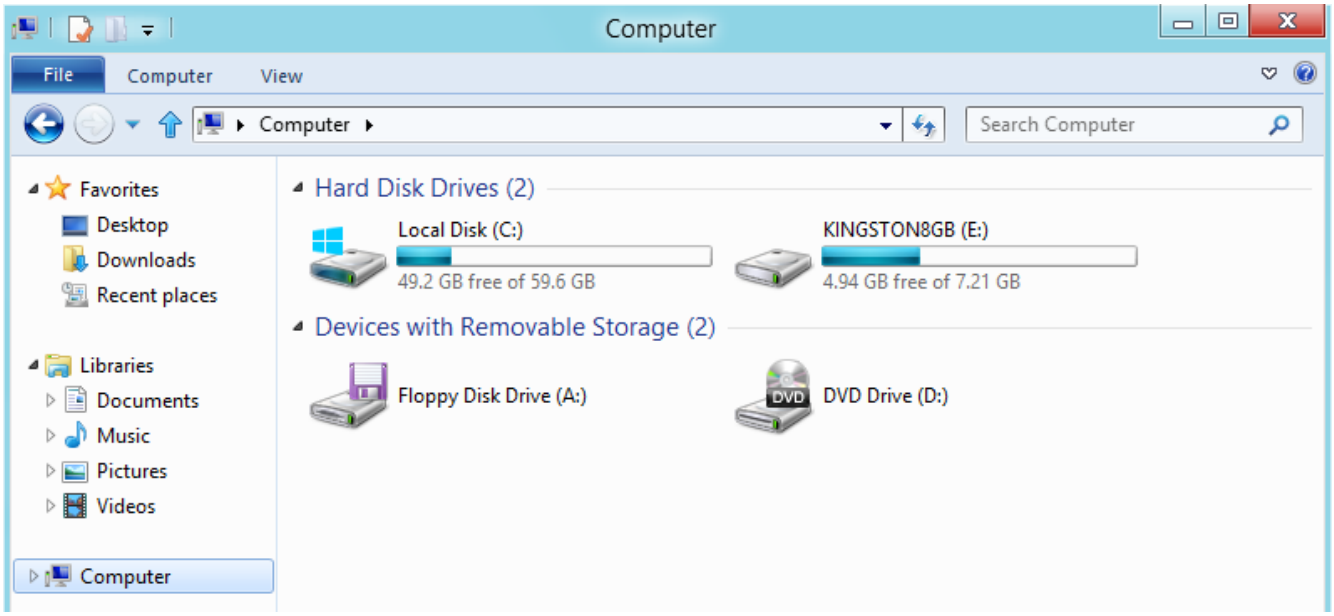
When the VM is booting up, you may see a message much like this:



This is related to the choice of Drive Interface selected when adding the hardware. We have found that SCSI is the most reliable and forgiving interface when dealing with unknown VM connections so the checkbox can safely be checked to prevent the message appearing again.

Please heed the warning relating to dual boot systems.

When you then enter My Computer on the VM, you will see any additional drives listed under File Explorer and will be able to navigate them as if they were connected to the computer.



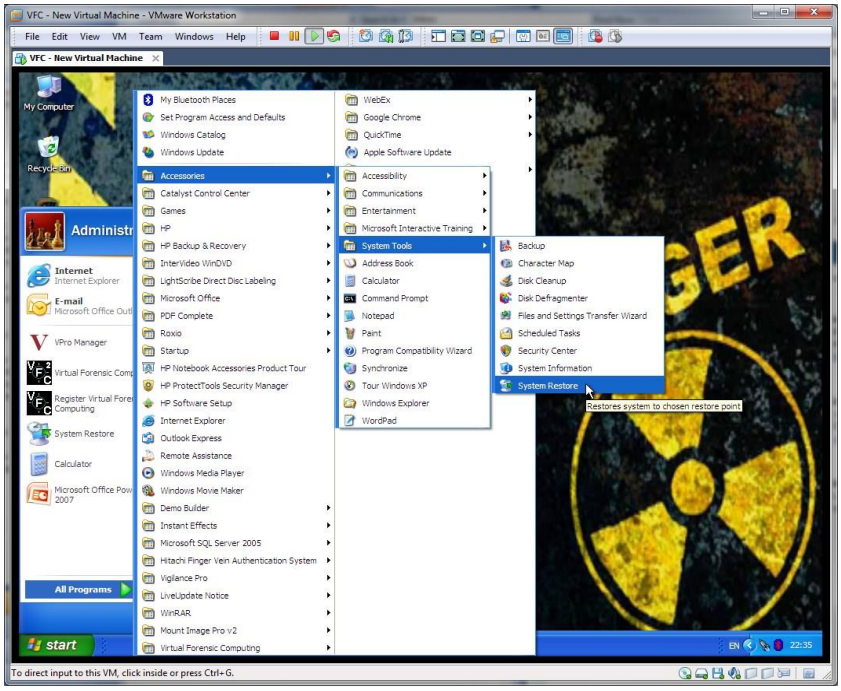
If the VM does not fire up or the hardware you've added does not appear in the list, please double check how you mounted your drives. All E01 files should be mounted as Physical Only.

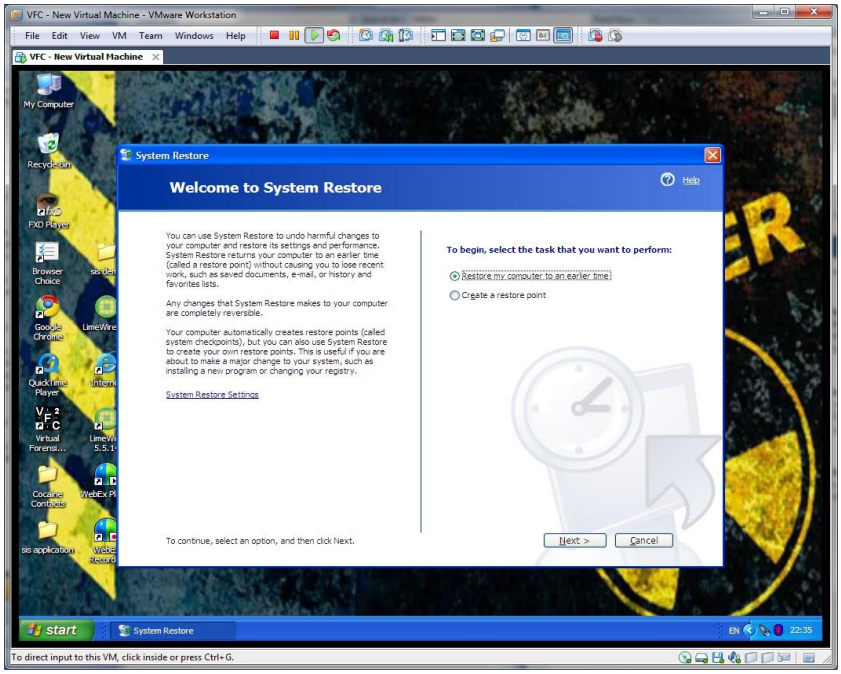
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

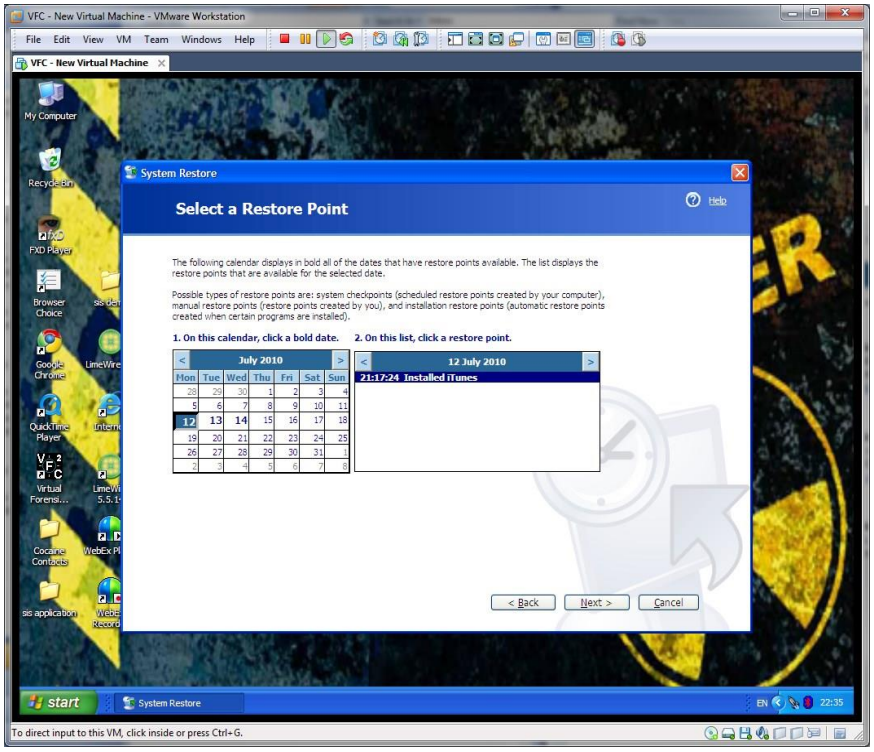
Restore Point Forensics / Patch VM

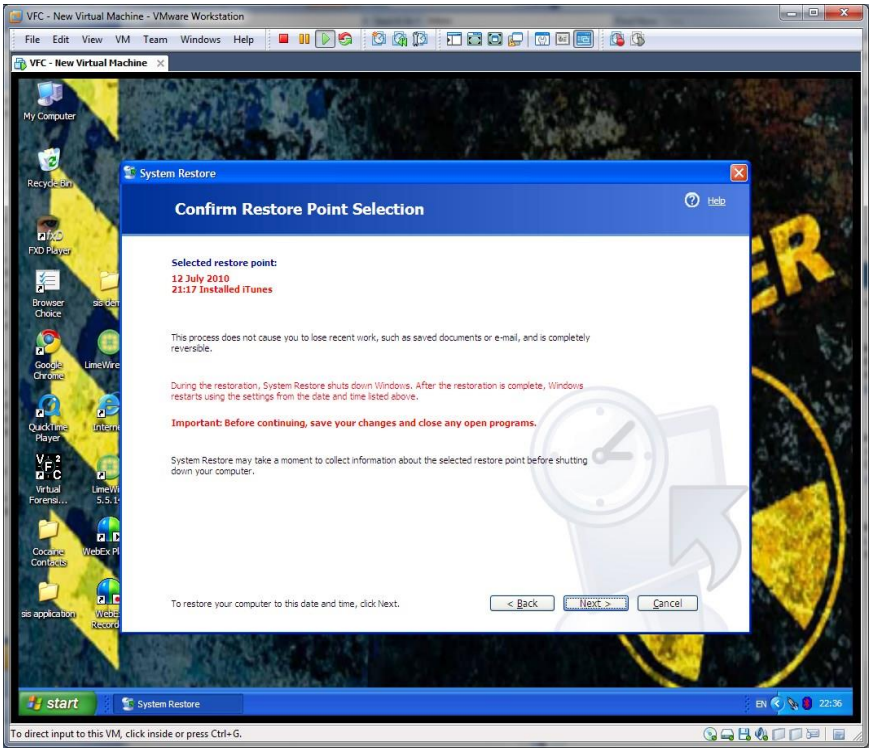
System Restore

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



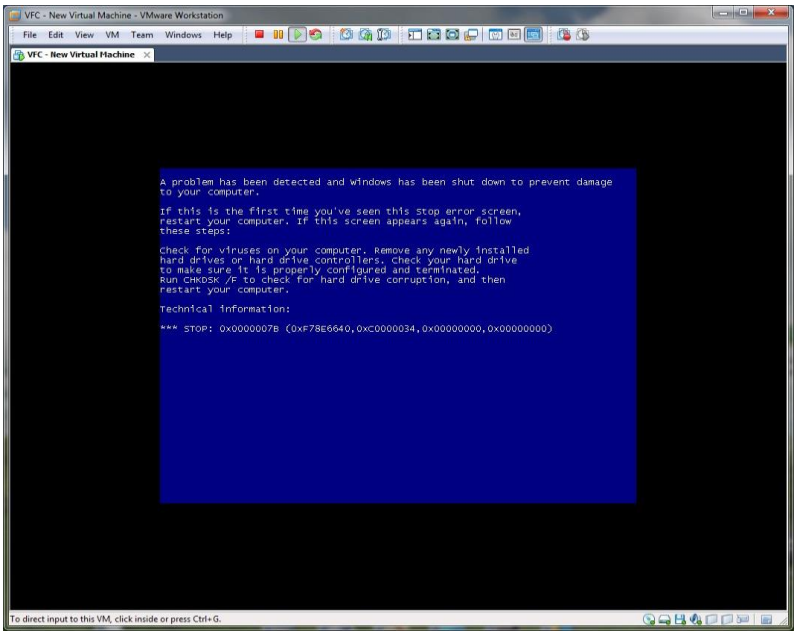




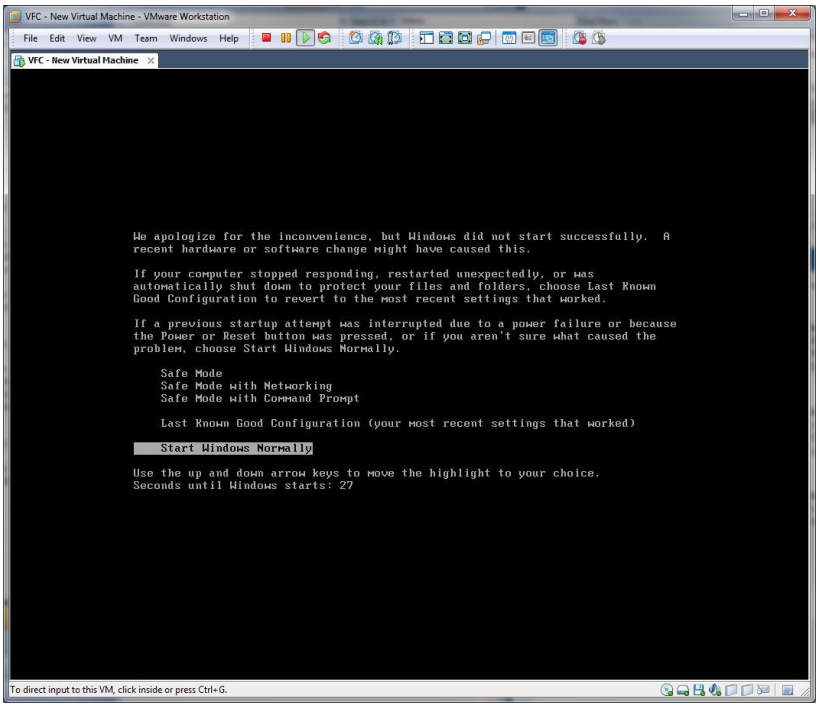


When utilising this functionality, any changes (including fixes and patches) made to the system by VFC and any subsequently installed applications (such as VMware Tools) will be removed.

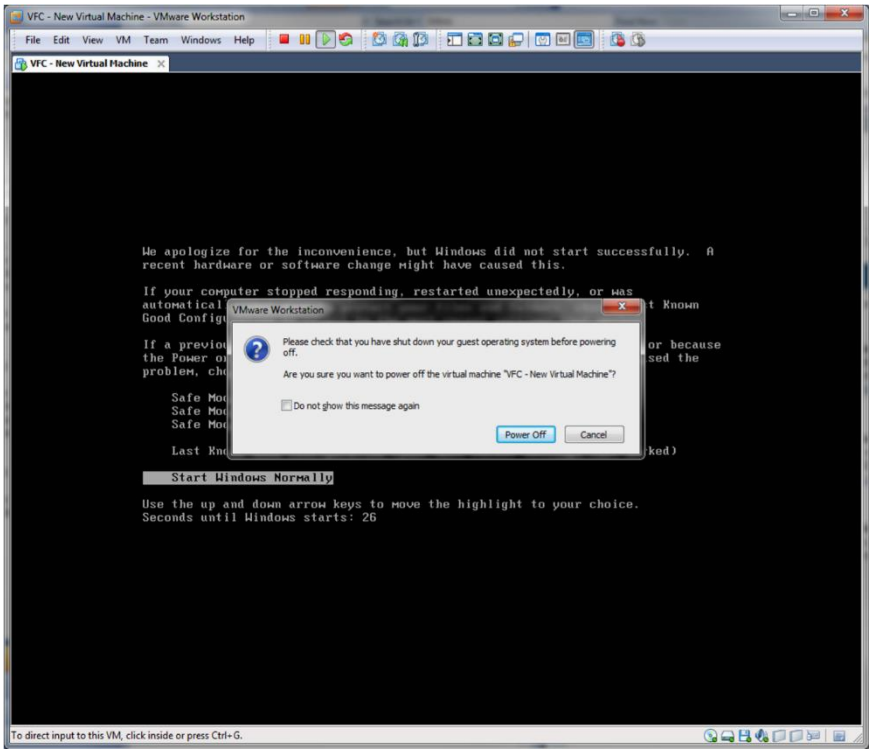
Undoing the VFC changes will typically result in the VM failing to successfully boot or entering a reboot loop. On older systems, this can result in a 0x7b BSOD (Blue Screen of Death) STOP message part way through the process:



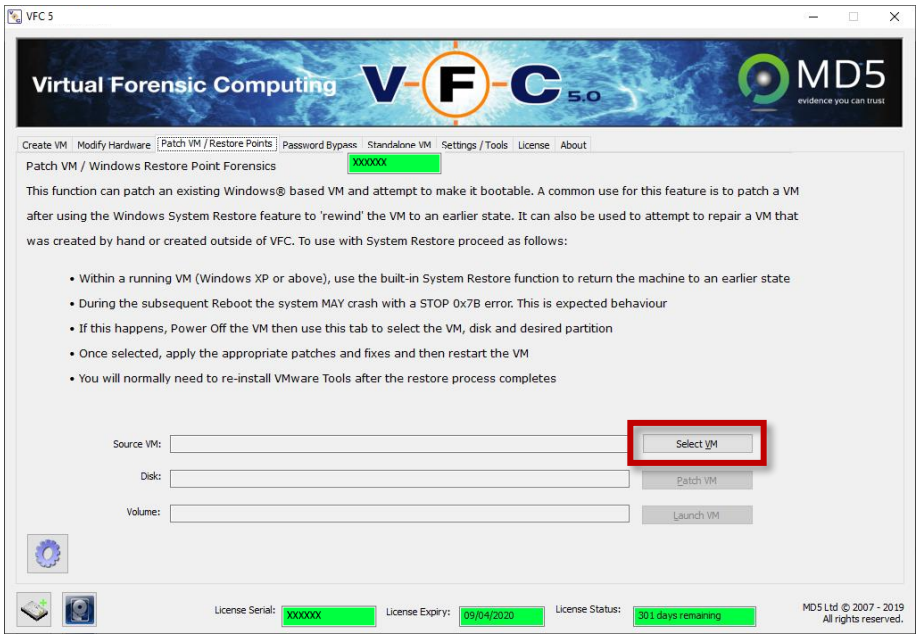
This is expected behaviour. When the system crashes, it will likely go into a cyclical reboot.



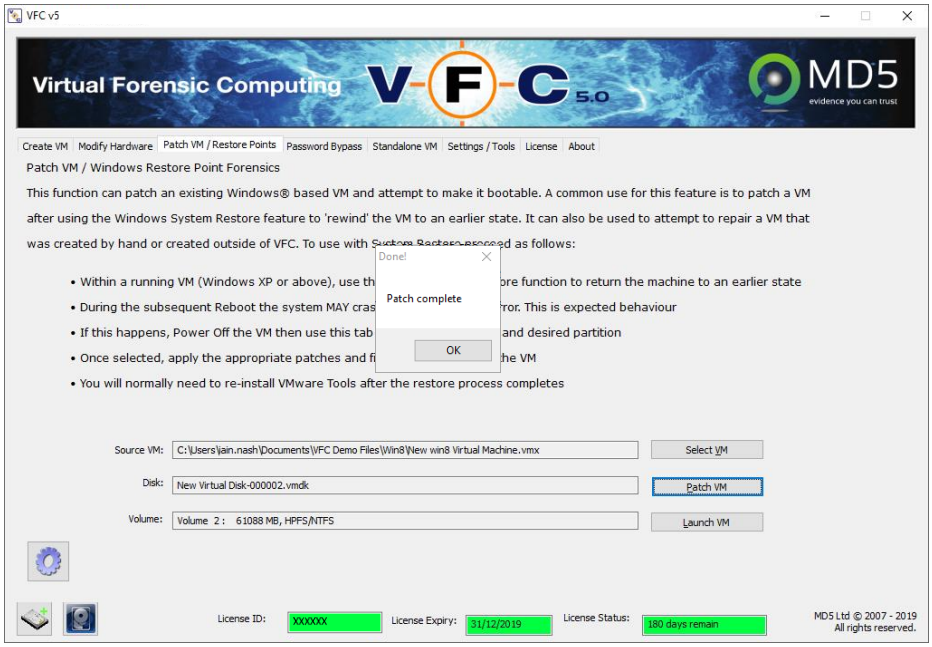
When this happens, Power Off and then close (rather than suspend) the Virtual Machine in VMware (or close VMware).



Once the VFC VM has been closed, you can utilise the “Patch VM/Restore Points” tab in VFC to "repair the VM". The fix applied is very similar to the process used by VFC to create a new VM. Simply click “Select VM” and choose the bootable drive (from which the VM was initially created):



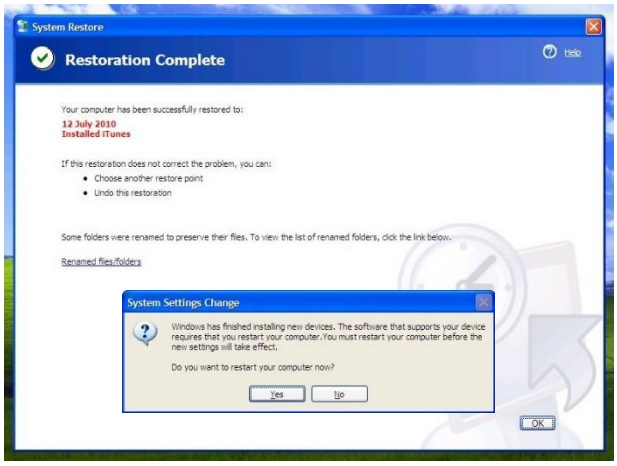
Select the VM you want to patch and click “Patch VM” then click “OK” when it’s finished. You should now be able to Launch the repaired VM and continue as before.



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

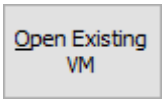
NB A full restoration to an available restore point may take some considerable time.

When the system completes its boot sequence you will need to run the Password Bypass (PWB) or Generic Password Reset (GPR) routine another time as any changes made by these will have been lost. You may again experience alert messages relating to hardware devices, including requests to restart the computer for new devices to take effect.



Open Existing VM

You will notice on the home-screen of VFC a button that says “Open Existing VM”:



This button is designed to save you a few seconds when revisiting a VFC VM you have previously generated. To use it, the same forensic image(s) used when the VM was created will need to be mounted and available as Physical disks.

Please note, THIS IS ONLY FOR VFC GENERATED VMs. It will only work for VMs with multiple VMDKs If you ensure they are correctly mounted first (e.g. in the same order and occupying the same Physical Disk locations).

VFC will not currently open VM files from other sources*.

When VFC creates a VM from a mounted E01 file, it leaves all the user data in situ inside the secure E01 wrapper. It does this for speed (it would take a long time to export all that data into e.g. a raw DD image) and for security and forensic integrity. Due to the nature of how VFC creates virtual machines, to re-use a pre-existing VM, you will need to mount the same image(s) upon which it depends.

If these mounted images happen to be allocated the same Physical Disk numbers as when the VM was first generated, it will boot up with no issues.

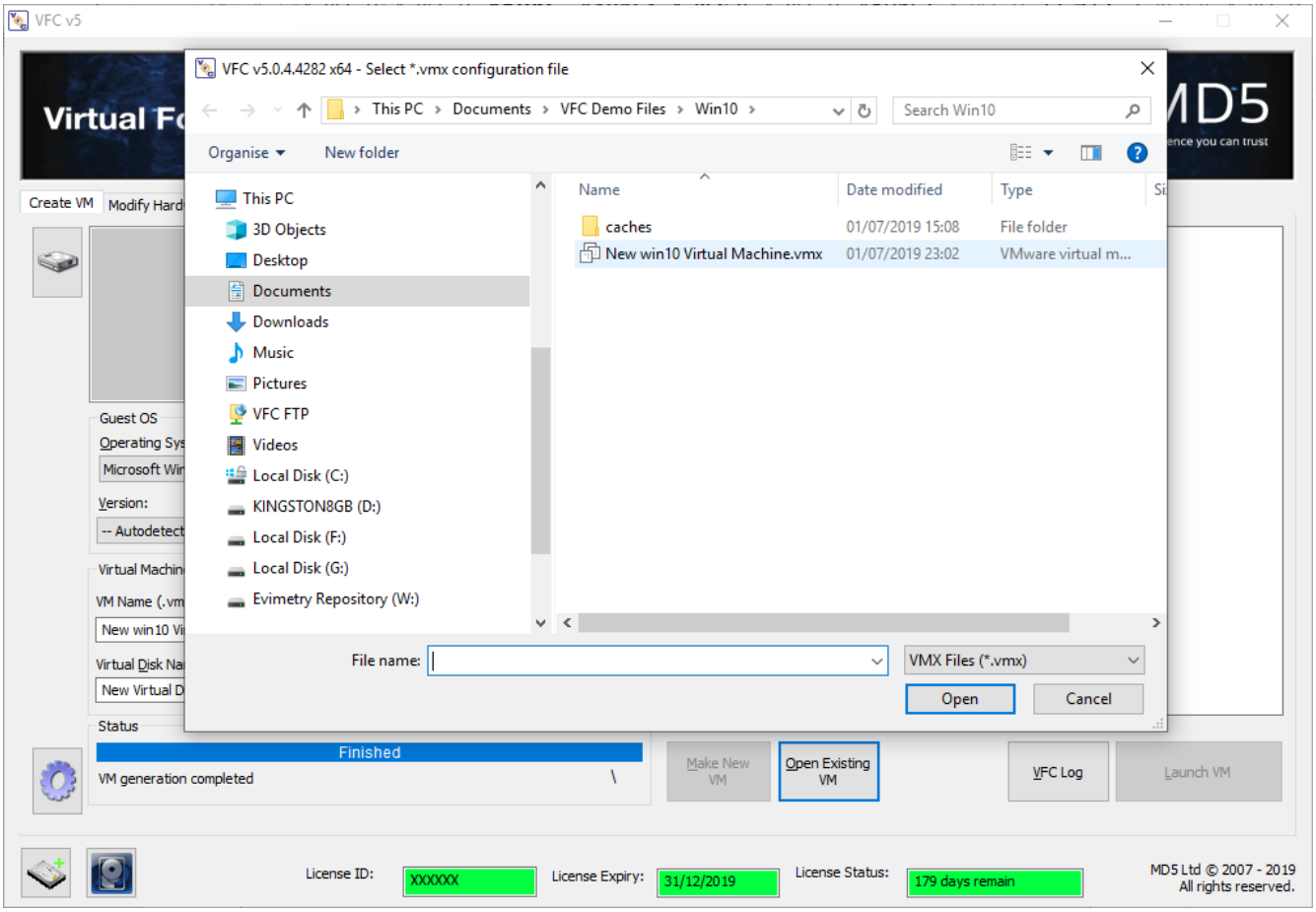
If the mounted images have moved, and Windows has allocated them different drive numbers, the Open Existing VM button gives you the option to scan all available drives for the original source data and automatically re-allocate the drive numbers and edit the VMX accordingly to make the VM boot up.

Please see next pages for detailed instructions.

* Correct at time of writing (05/07/2019)

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

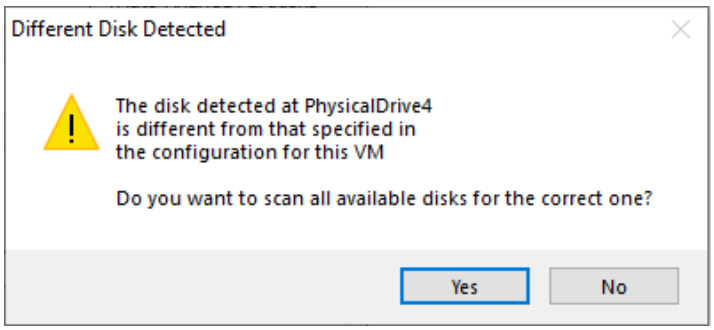
To start, click “Open Existing VM” and select the required VMX configuration file:



Browse for your desired VMX and click “Open”.

If the VM loads, then the mounted drives that this VM relies upon happen to be in the same location that they were in previously.

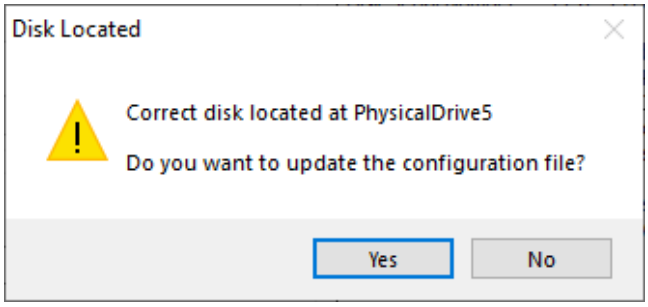
If, however you see the message below (or similar), click “Yes”:



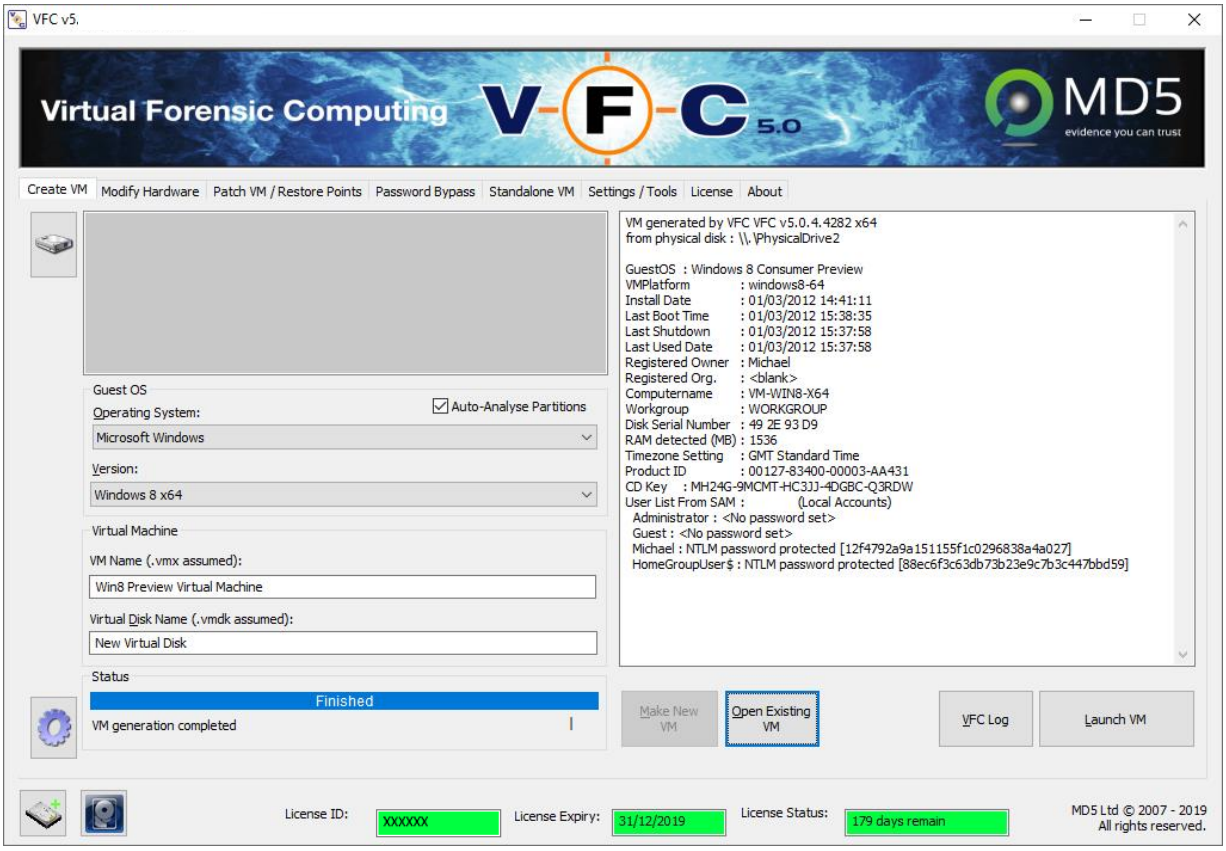
VFC should now look for the drive signature of the mounted image you used before. If found, it will notify you of the new disk location.

Click “Yes” again and VFC will attempt to redirect your VMX to the new mount location (by updating the VMX configuration file with the new disk location).

If successful, you should see this message (or similar):

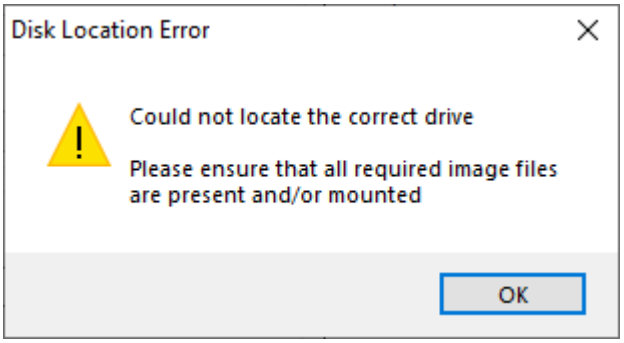


The VM should now load:



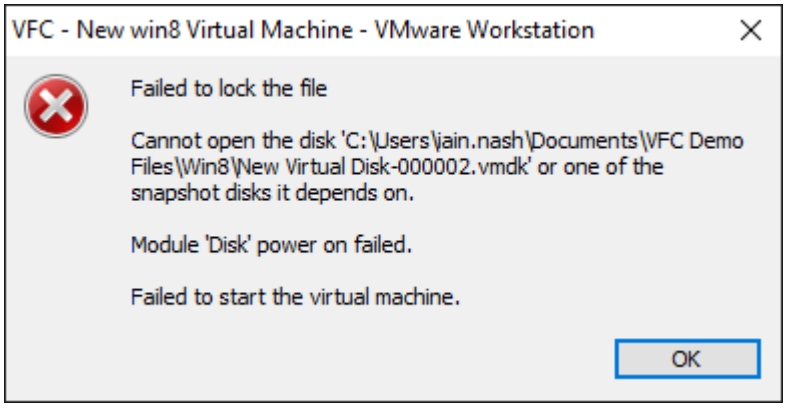
You should now be able to launch the VM.

Alternatively, if you see this message:



… then unfortunately, either the disk signature has changed or another problem has occurred.

Please note, if the VM has multiple disks, it will probably fail unless the images are correctly mounted beforehand:



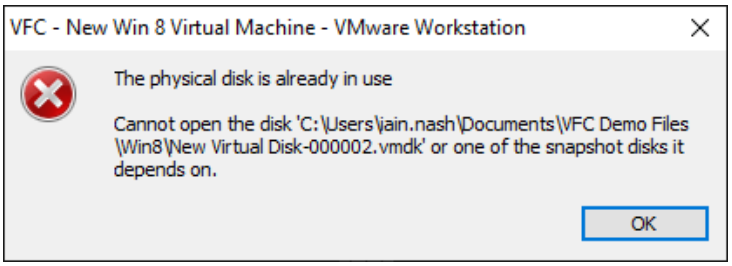
You could attempt to manually edit the VMX configuration file with the new disk locations however...

If the Open Existing VM option fails, you can simply rebuild the VM quickly from the original mounted evidence files, using the standard VFC VM creation processes.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

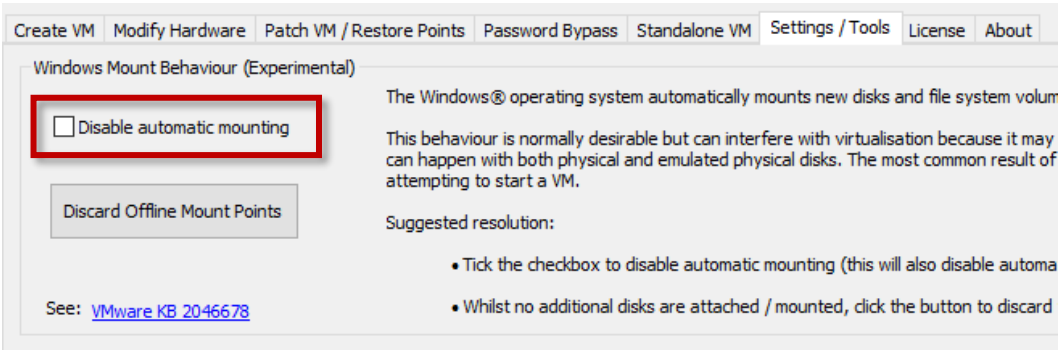
Settings / Tools

This new tab in VFC has been added to address the notorious “Physical Disk In Use” (PDIU) error in VMware. This error can occur because Windows has mounted file systems on the emulated/ physical disk and VMware is unable to gain exclusive access to that disk:



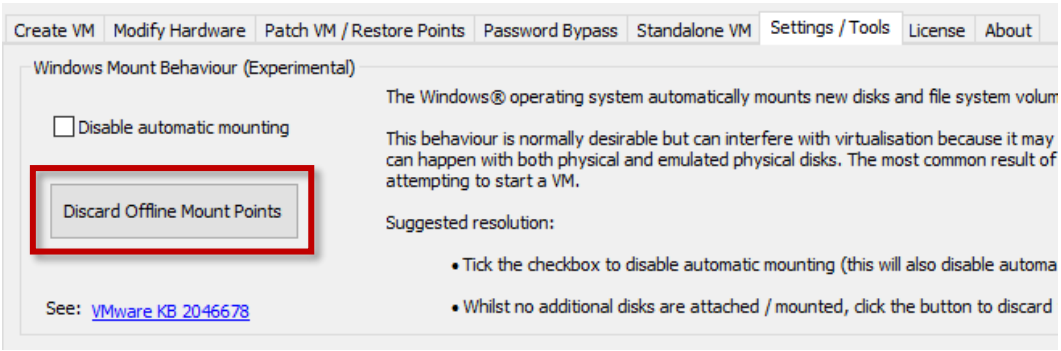
VFC v5 includes three new features to mitigate the PDIU problem. These should greatly reduce the number of times the problem occurs (but may not eliminate it entirely):

1. Disable automatic mounting checkbox on the Settings / Tools tab in VFC itself:



This stops the underlying Windows OS behaviour and clears out the Windows mount history.

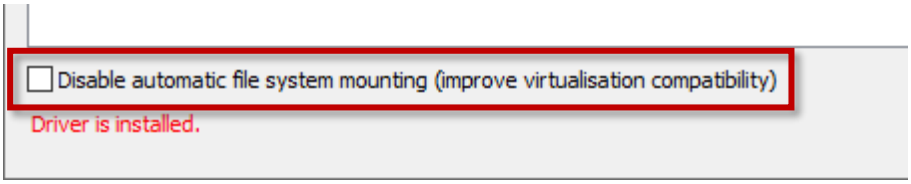
2. Discard Offline Mount Points button on the Settings / Tools tab in VFC:



This second part is necessary to stop the problem re-occurring with disks/images that were mounted before the checkbox was ticked. It is harmless to press the button (it just clears the mount history again).

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

3. Checkbox in VFC Mount:



This stops the underlying Windows OS behaviour (as above) AND also tells VFC Mount to mount the image in a way unique to VFC and developed specifically to address the PDIU issues that makes the problem less likely occur. We initially didn't expect this to be necessary but in testing found that PDIU still occurred quite often. The result with VMware should be superior to using FTK Imager or MIP.

The new feature mostly addresses the issue although frustratingly it can occasionally return, especially if your workstation has been running for a number of days. This article from VMware gives more technical information on the issue: https://kb.vmware.com/s/article/2046678

Please follow the checklist below to reduce the instances of this problem.

Checklist:

1. Make sure no images are mounted (unmount everything and then close FTK Imager and VFC Mount)
2. Start VFC
3. Open Tools/Settings tab – Tick box and press button
4. Open VFC Mount
5. Ensure box is ticked (it should be)
6. Mount image
7. Try to create VM again

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

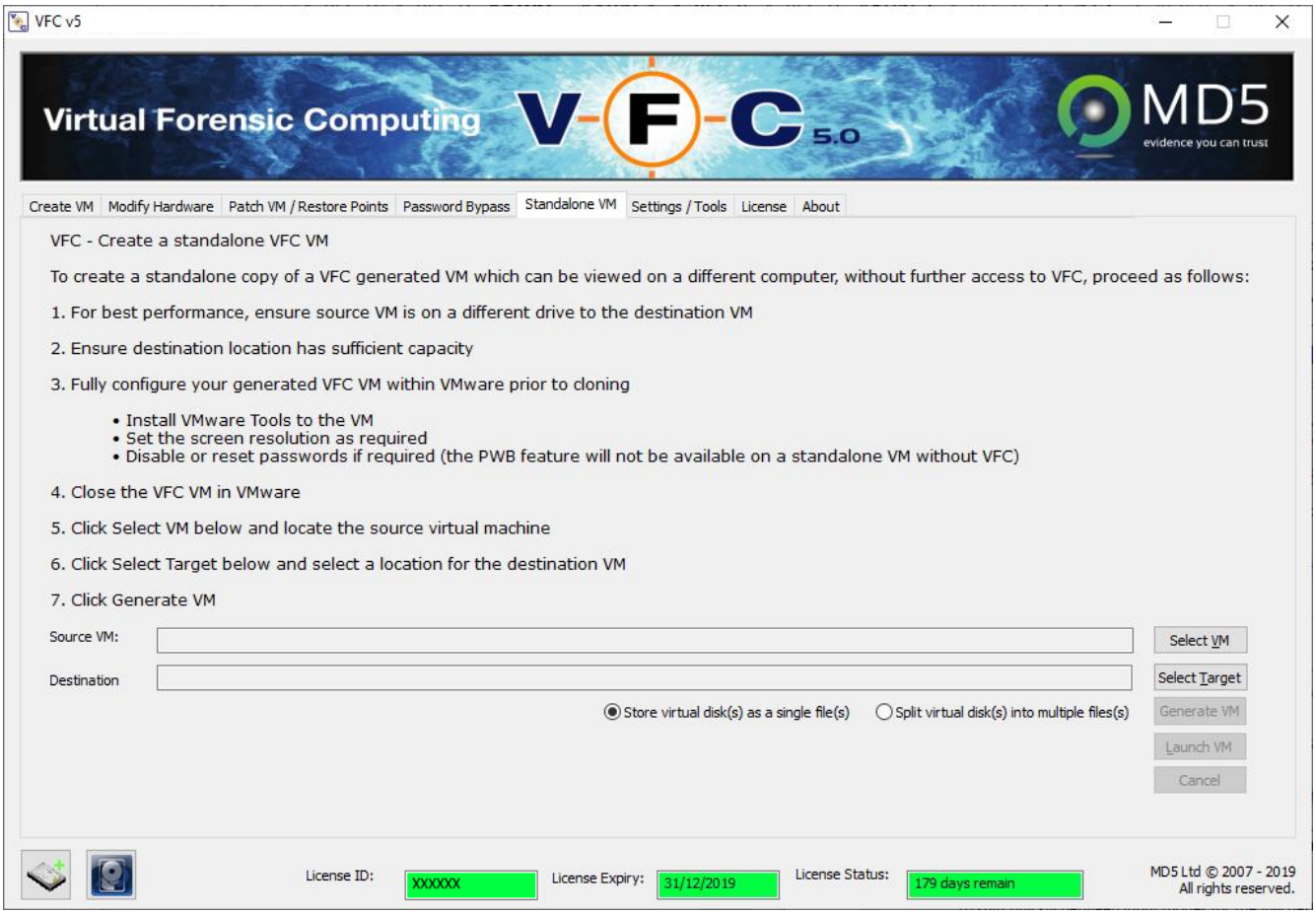
Creating a Standalone Clone Virtual Machine from a VFC VM

On occasion it may be necessary to create a standalone copy of a VFC VM for a client whom does not have access to mounting utilities such as VFC Mount, FTK or MIP – or the main VFC program (and associated license(s).

NB *When using the following method to create a copy VFC VM, unless snapshots are carefully used, the forensic integrity of the methodology will be compromised as the standalone machine cannot be readily recreated and returned to its initial state.*

Creating a Standalone VFC VM using the automated VFC process

VFC5 refines the standalone clone functionality that was present in previous releases of VFC. The feature automates the generation of a standalone clone. The UI looks like this:



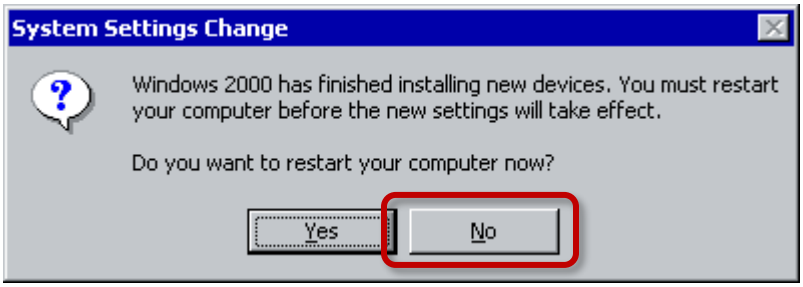
The instructions should be self-explanatory however we do recommend that you follow them closely.

NB *The Generate Standalone VFC VM Clone Copy feature will copy all the User data from the source image into a new destination so depending on the size of the source drive(s), the export process can take a significant amount of time.*

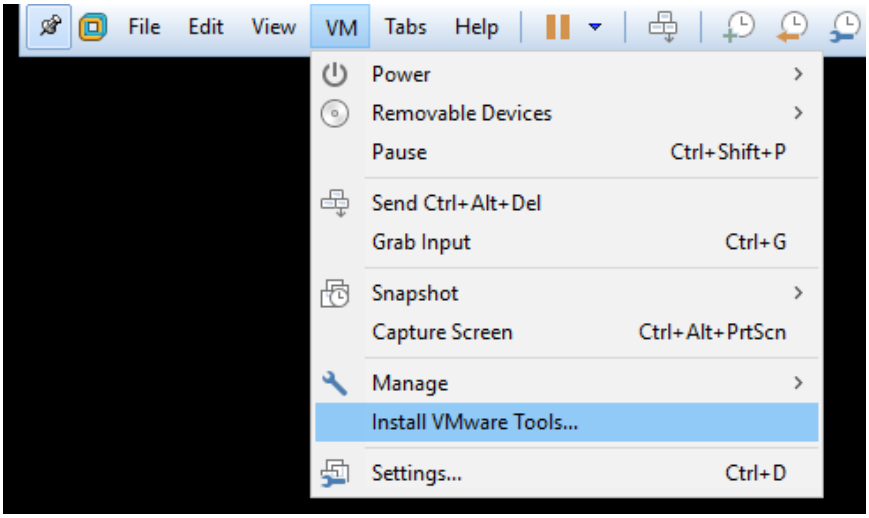
Preparing the VM for export as a Standalone Clone

When you first open your VM, you may find the system identifies new hardware and tries to locate the relevant drivers. When exporting a standalone clone, it is good practice to allow all these processes to run in full. If the drivers cannot be found, it can help the end-user of the Standalone Clone if you disable the feature.

Once all driver installation processes have run, the VM may prompt you to restart. Because you need to install VMware Tools as well, it can save time if you click “No” at this time:



Next, you need to install VMware Tools which can typically be done via a virtual CD drive within the VM or from the VMware menu:

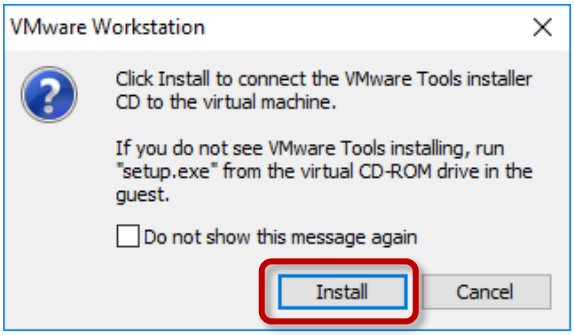


To shift quickly between input modes for the VM desktop and your host system (e.g. the VMware toolbar), use the keyboard shortcut (Ctrl + Alt).

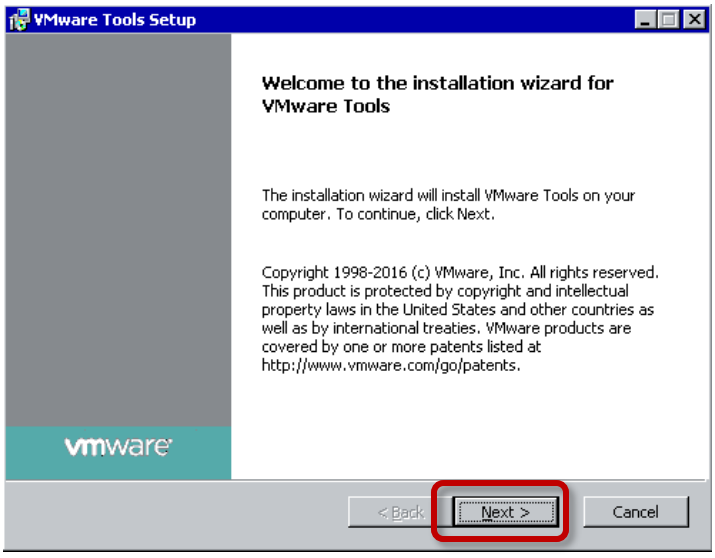
Select “VM > Install VMware Tools…” and follow the instructions below. More information is available in the section above titled “VMware Tools installation”.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

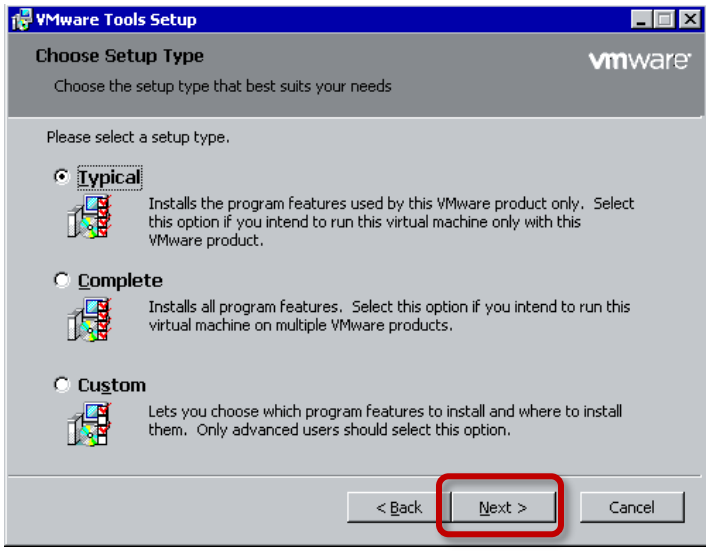
Click “Install”:



The VMware Tools Setup wizard will open. Click “Next”:

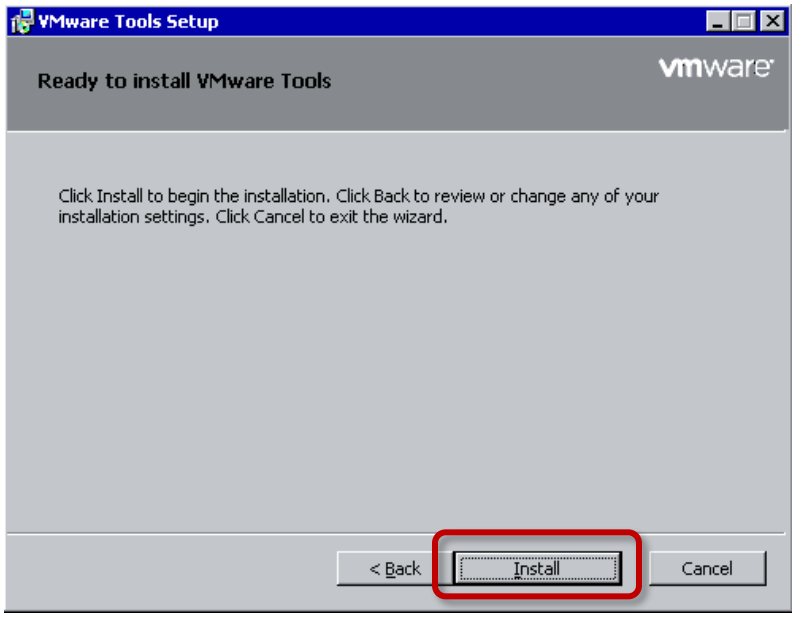


You can choose which setup to use but ‘Typical’ usually works fine so just click “Next”.

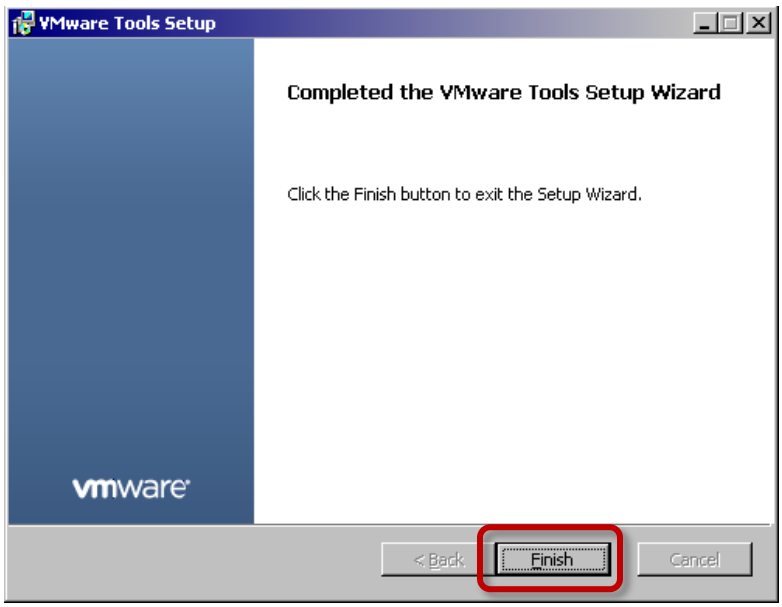


Unlike producing a clone in VMware where you need to pick 'Custom' settings, VFC will pre-prepare the VMX for export as part of the "Generate Standalone Clone VFC VM Copy" process.

Click "Install" to start the installation process:

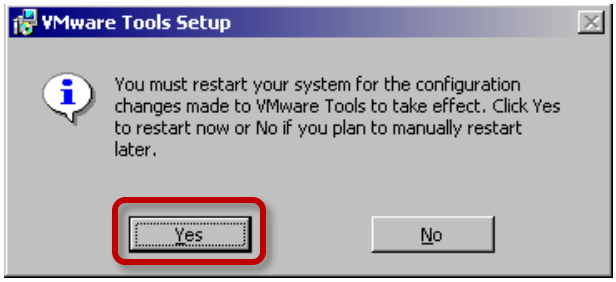


Once the installation is complete, click "Finish":



Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

You will now be prompted to reboot your machine again:



This time, click “Yes” and wait for the VM to power on again. This will ensure VMware Tools are correctly installed on your VM prior to exporting a standalone clone and will give the recipient or end-user better control of the VM and greater access to the files and data held within it.

Once the system has rebooted, you can reset passwords or change the screen resolution if required. Because the clone is designed to be opened without the need for VFC, the user will most likely not have the option of the password bypass feature so it is paramount that the password is either cracked and supplied, or reset/removed entirely.

It is worth noting that often the installation of VMware Tools will address issues with the screen resolution and map it to your own hardware… this means that the desktop of the resultant VM may not look exactly like that of the original evidence and you may want to set the value to that of the original system (see further details in the section above on VMware Tools installation).

You can then take a snapshot if you are running VMware Workstation Pro, which will allow the VM to be rewound back to this initial state.

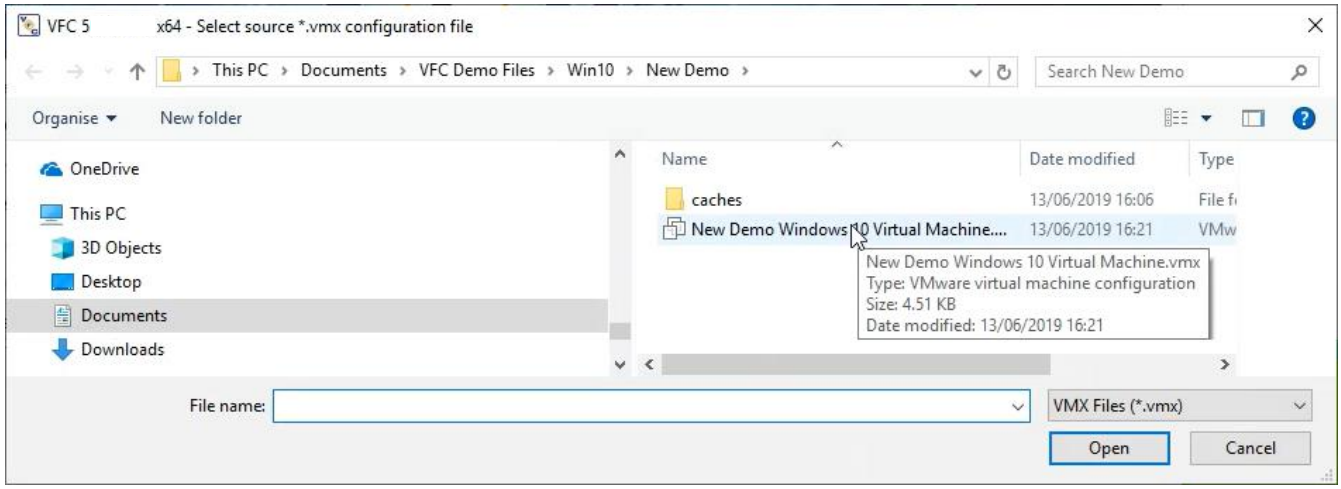
NB *You will need to close your VM in VMware before you can use the VFC Standalone Clone function*

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

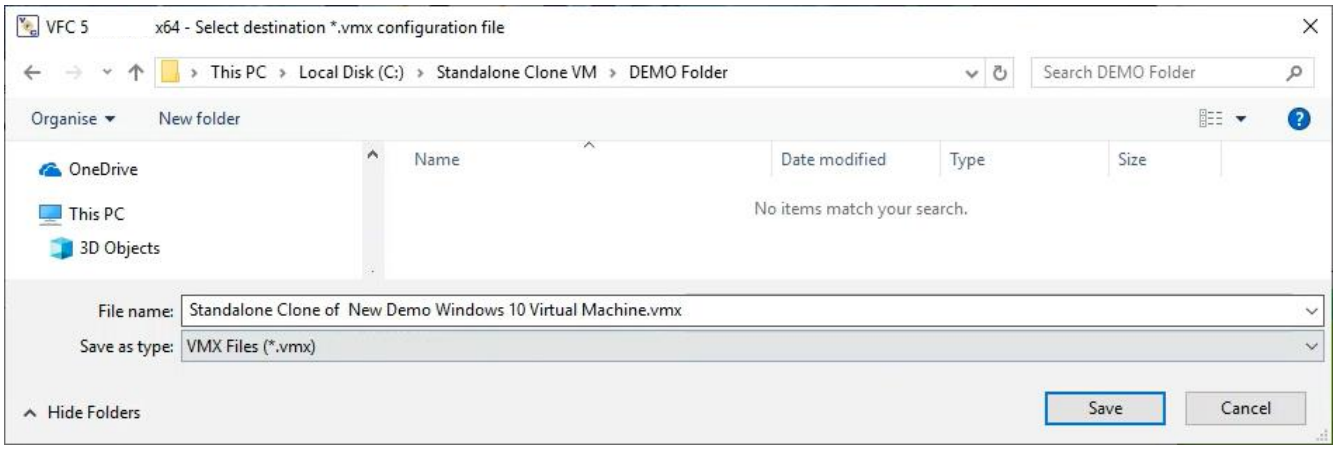
Exporting a Standalone Clone

To export your clone, set it up as above and then ensure that the VM you want to clone is not open in VMware (i.e. not suspended or powered down but closed completely). Depending on how the clone is to be used, you may prefer to power it off in the state it's in or shut it down properly. It will have to boot up fully when next launched, whichever options is chosen, so there is little difference between these two from this perspective.

Once you have done this, use the buttons on the VFC "Standalone VM" tab to choose which VM you want to export (click "Select VM" then browse for it and click Open):

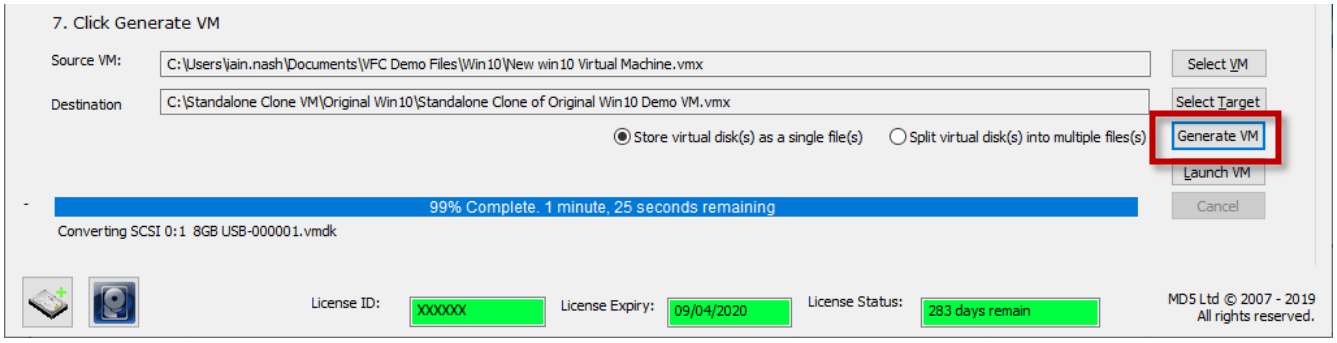


… and where you want to export it to (Click "Select Target" then navigate to your chosen folder):

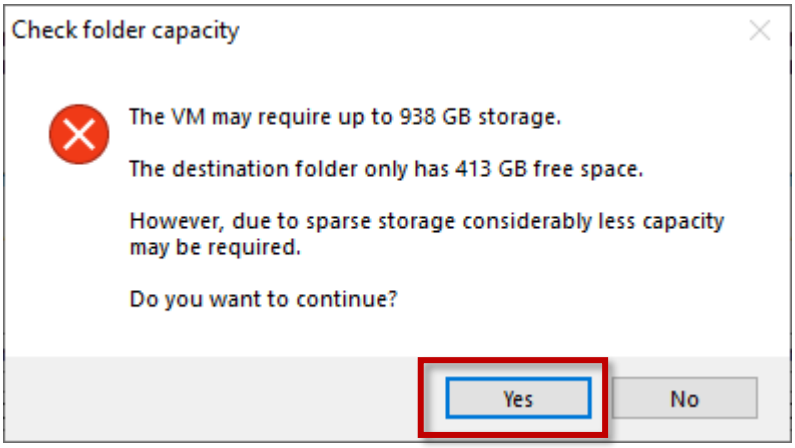


Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Next, click on “Generate VM”:

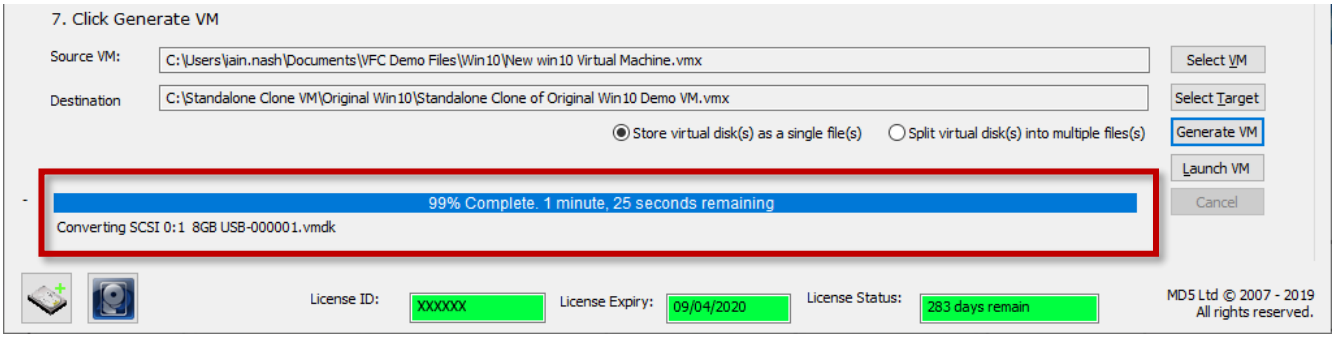


VFC will check the capacity of the target drive and notify you if there may not be enough space. If you choose to continue (by clicking “Yes), unlike earlier versions of VFC, if there is enough storage space in the destination to store the resultant clone, the process will still complete:



The source disk does not need to be big enough to take the entire drive volume any more – it will utilise sparse storage features and provided the final VM takes up less space than is available, a VM with e.g. a 2TB drive can fit on a disk with just a few hundred GBs of space.

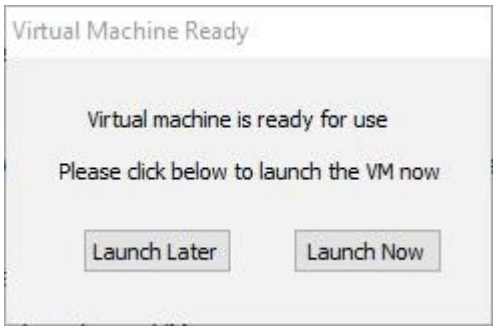
Click “Yes” and you will then see VFC exporting the data. A progress bar at the bottom of the VFC GUI will give an indication of how far through you are:



A padlock at the top will indicate that VFC has locked the program due to the ongoing process:

Please note, the more data you need to copy, the longer the process will take.

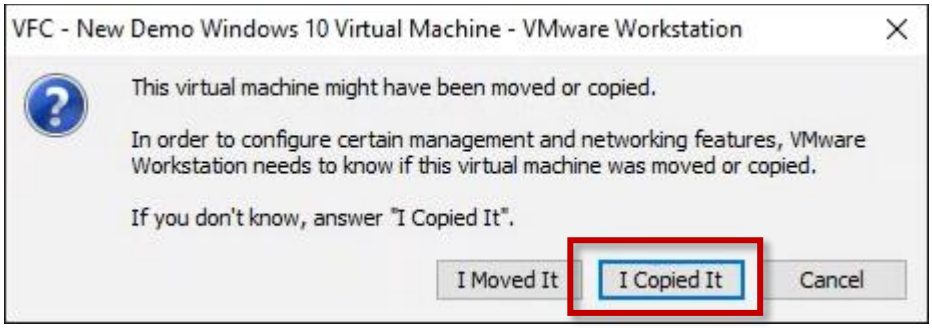
Also, the type of connection to your destination drive can have a huge impact on the speed of data transfer, e.g. USB 2.0, 3.0 or SATA.



When the export process has completed, you can either choose to “Launch Now” or “Launch Later”.

At this point, you can now open the VM clone on any computer running VMware Workstation without any mounting tools or the need for a VFC dongle.

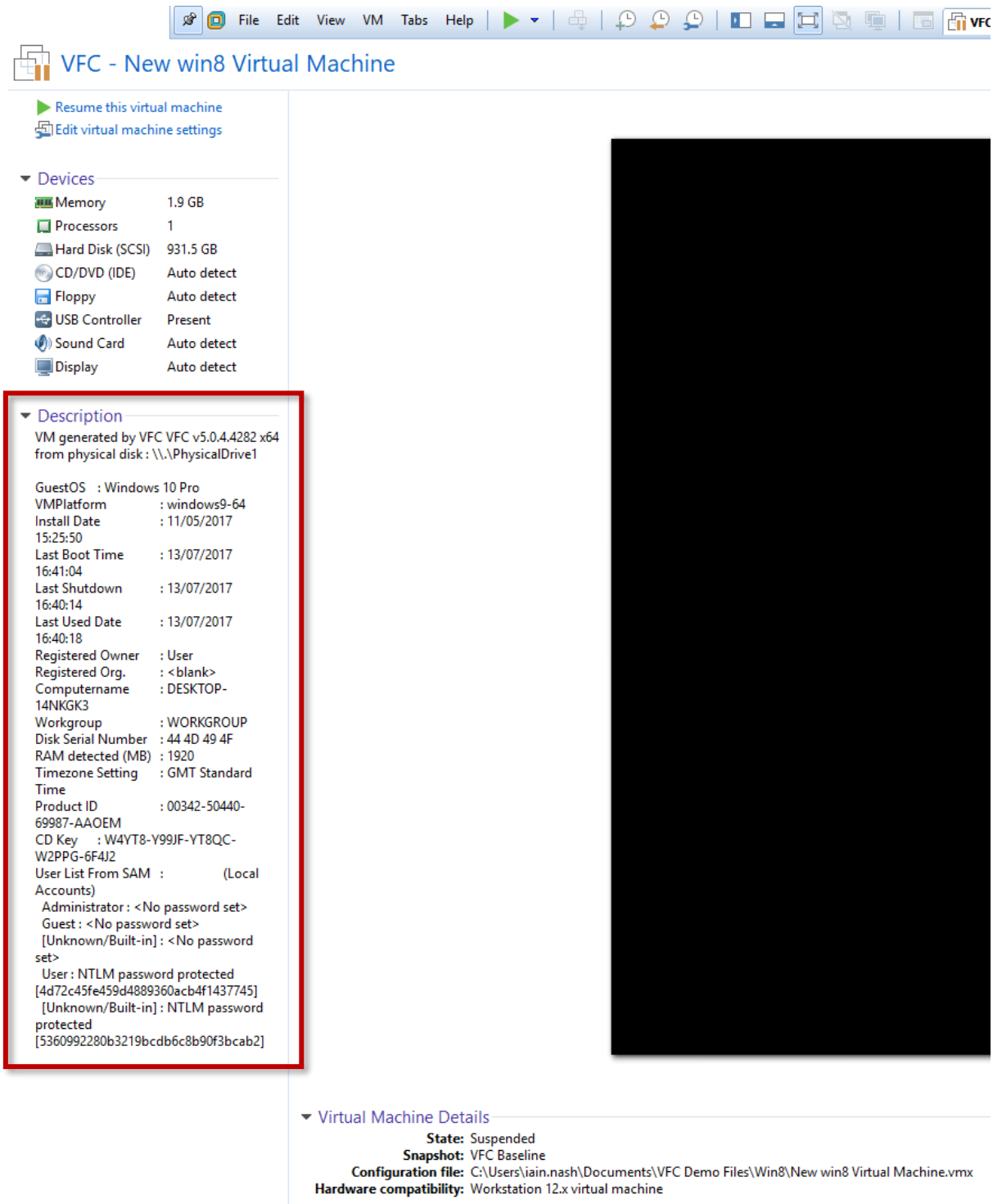
If you are planning on providing the clone to anyone else, it is worth launching the VM at least once to clear this message:



The message appears because the VMDK files it relies upon have moved. The correct answer is (as we know) “I Copied It” and it does instruct you to choose that option if you don’t know but to reduce confusion from other parties, if you launch it and choose this for them once, it won’t appear again.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

You can open the exported standalone clone VFC VM .VMX file from File Explorer or from the File > Open menu in VMware. You will notice the information from the splash-screen of VFC is embedded into the VMX annotation:



VFC Command Line Interface (CLI)

New to VFC5 is the option to run VFC via the new Command Line Interface (CLI). This can be used to script VFC and to automate common preparation tasks.

The interface does not currently allow the entire VM creation process to be automated but can significantly reduce the amount of manual interaction required. This is intended for automation/batch scenarios. The VFC Integration components for EnCase and X-Ways Forensics use the new CLI interface.

To view the supported syntax, use the command: **VFC5.EXE /?**

The following commands are currently supported:

- **/mounttool** – Launch the VFC Mount Tool.
    - We recommend you use this before other mount/unmount commands
- **/mount:filename** – Mount the specified image with VFC Mount Tool.
    - For example: VFC5.EXE /mount:"d:\mycase\image.e01"
- **/unmount:devicename** – Unmount specified device in VFC Mount Tool.
    - For example: VFC5.EXE /unmount:\\.\physicaldrive1
- **/unmountall** – Unmount all devices in VFC Mount Tool
- **/nosplash** – Do not display splash screen on start-up
- **/opentab:tabname** – Open specified tab on start-up.
    - For example: VFC5.EXE /opentab:pwb

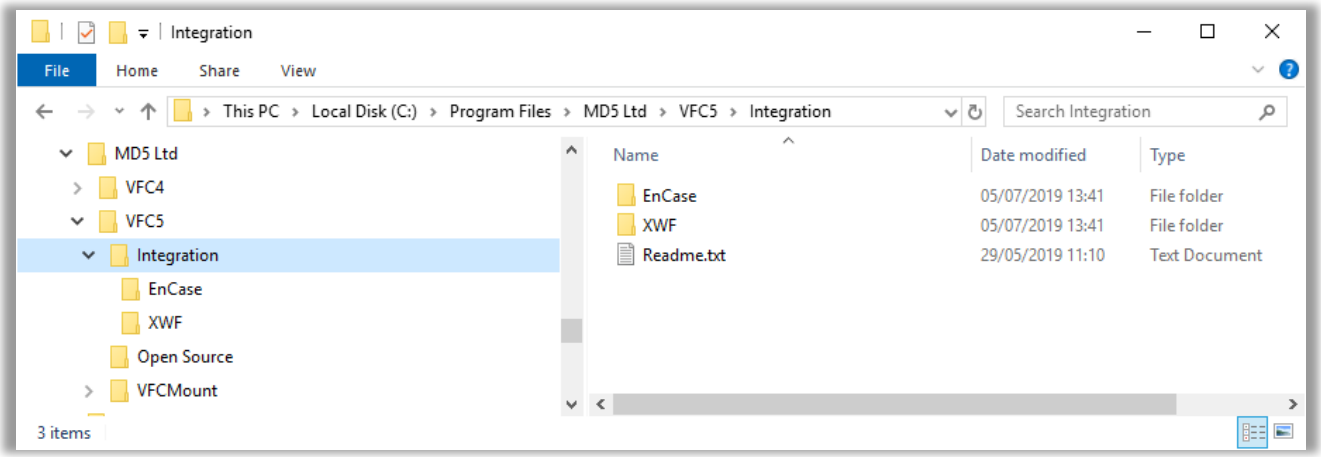
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

CLI Integration with Forensic Analysis Suite Software

When VFC is installed, it creates a subfolder in the installation folder called “Integration” where you will find pre-written scripts to integrate our software with some of the big names in digital forensics.

At launch, there are scripts for EnCase and XWF.

We have pre-prepared scripts for integration with EnCase v6, v7 and v8 and also X-Ways Forensics (XWF) v18 and later. The respective integration components are located in the "Integration" folder of the VFC installation:



The X-Tension and EnScript both behave in a similar way. They mount supported images from the current case (in XWF or EnCase respectively) using the VFC Mount Tool, and then launch VFC.

These scripts can be used to speed up operations and better integrate VFC into your forensic workflow. They determine the image file format using the file extension. The currently supported formats are:

.e01, .ex01, .aff4, .vmdk, .bin, .img, .raw, .dd*

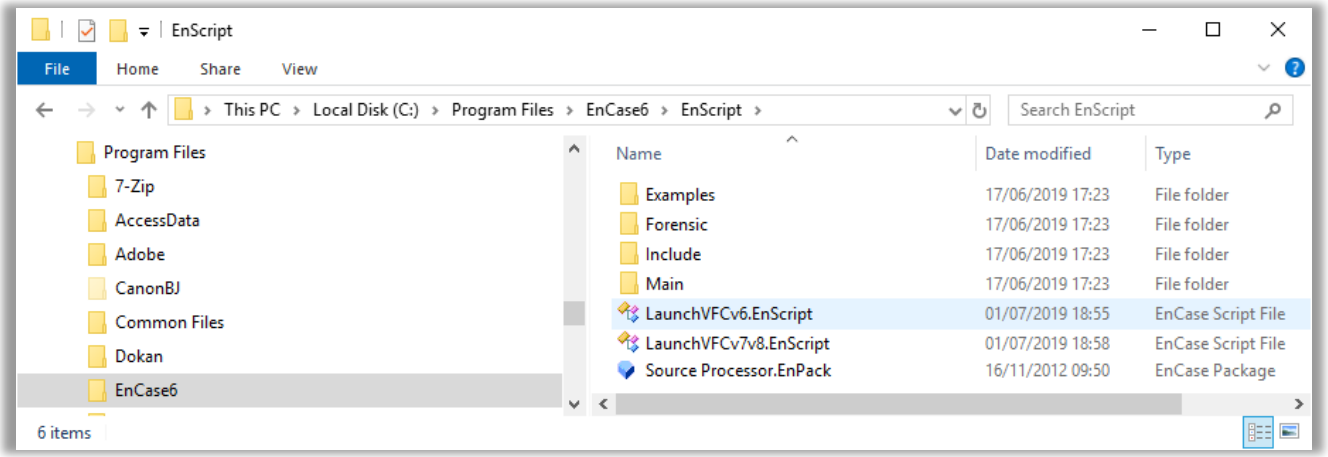
* Currently the EnScripts only support .E01 and .Ex01. The X-Tension (in theory) supports all of them but is limited by the fact the XWF itself doesn't support .Ex01 or .AFF4 without third-party extensions.

NB *Before attempting to use any CLI scripts, please ensure VFC v5.0.5 or later is installed correctly and has been launched at least once.*

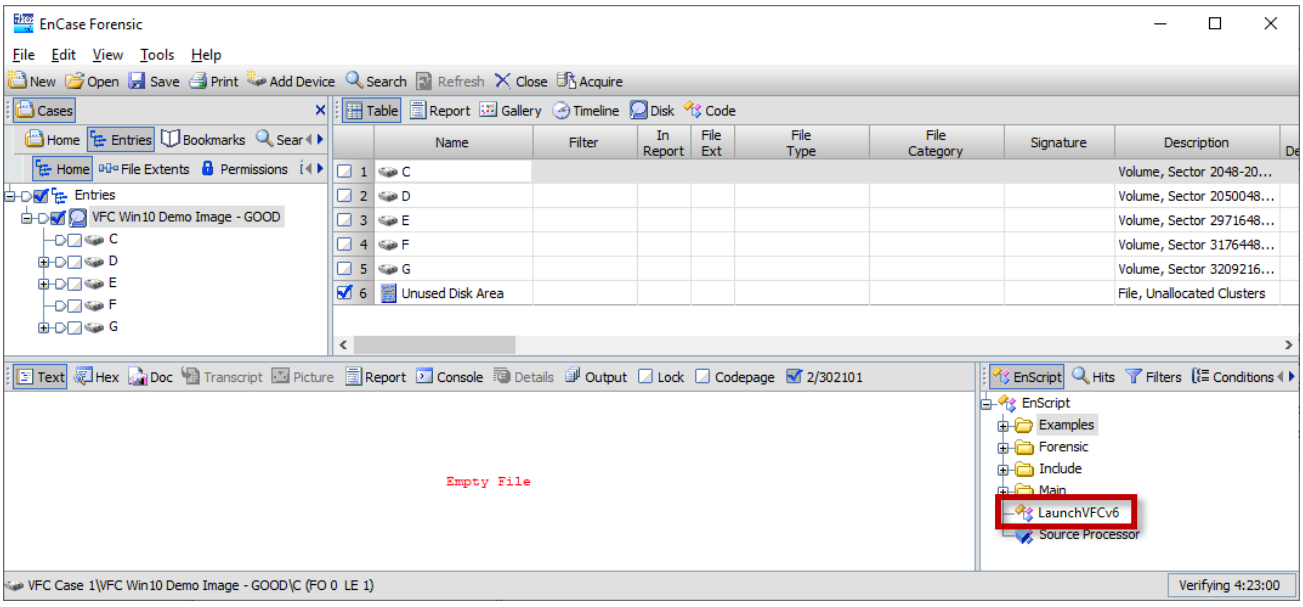
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Using the EnScript

Please see your EnCase documentation for detailed instructions on how to install EnScripts. The following walk-through describes the process for EnCase v6 (the instructions for v8 are different). To make the EnScript available to EnCase, please copy and paste the respective EnScript (for the version you are running) into the appropriate system folder:



EnCase should now pick it up and display it as an option within the EnScript panel within the software:



Ensure you have loaded the relevant disk image(s) you are working with into EnCase. The "LaunchVFCv6.EnScript" script will open each live image within VFC Mount and mount it as a physical drive with the appropriate settings. It will also launch VFC itself so that you can enumerate the connected drives and select the mother image.

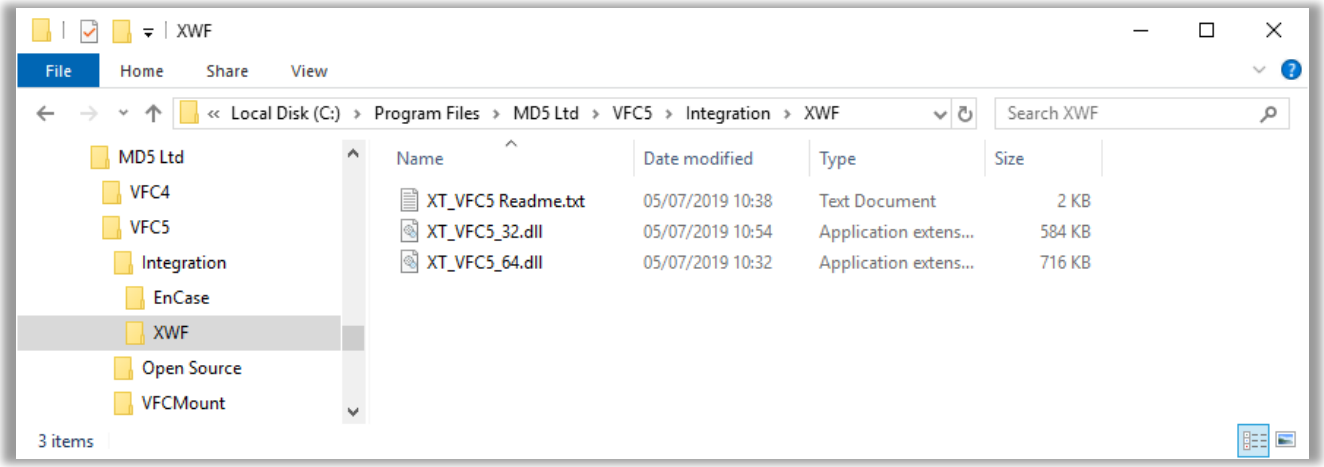
This is currently as far as the CLI integration will take you.
To generate your VFC VM please refer to the instructions above.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Using the X-Tension

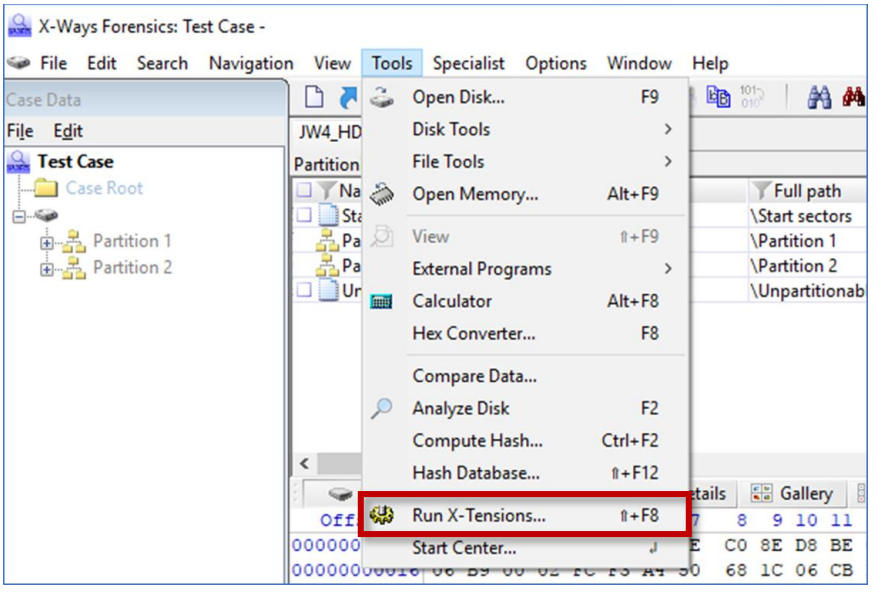
To make the X-Tension .DLL available to X-Ways Forensics (XWF), you will need to install the X-Tension applet which is supplied in the respective Integration folder within the installation folder for VFC.

Installation of the X-Tension

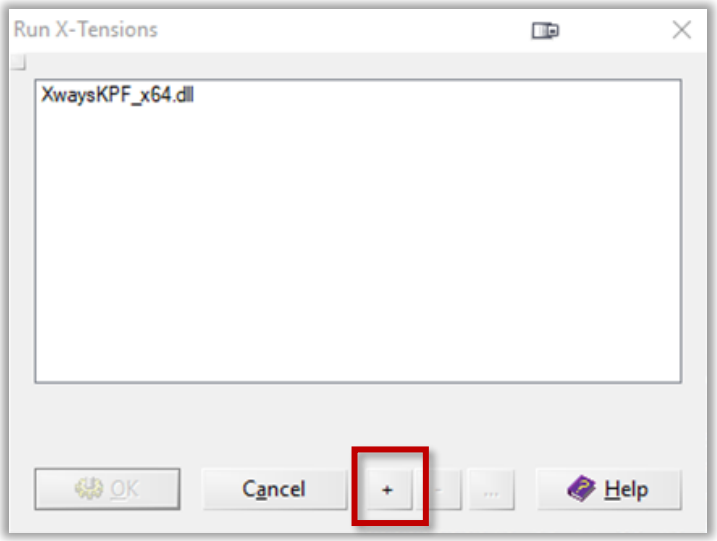


To install the X-Tension in XWF, proceed as follows:

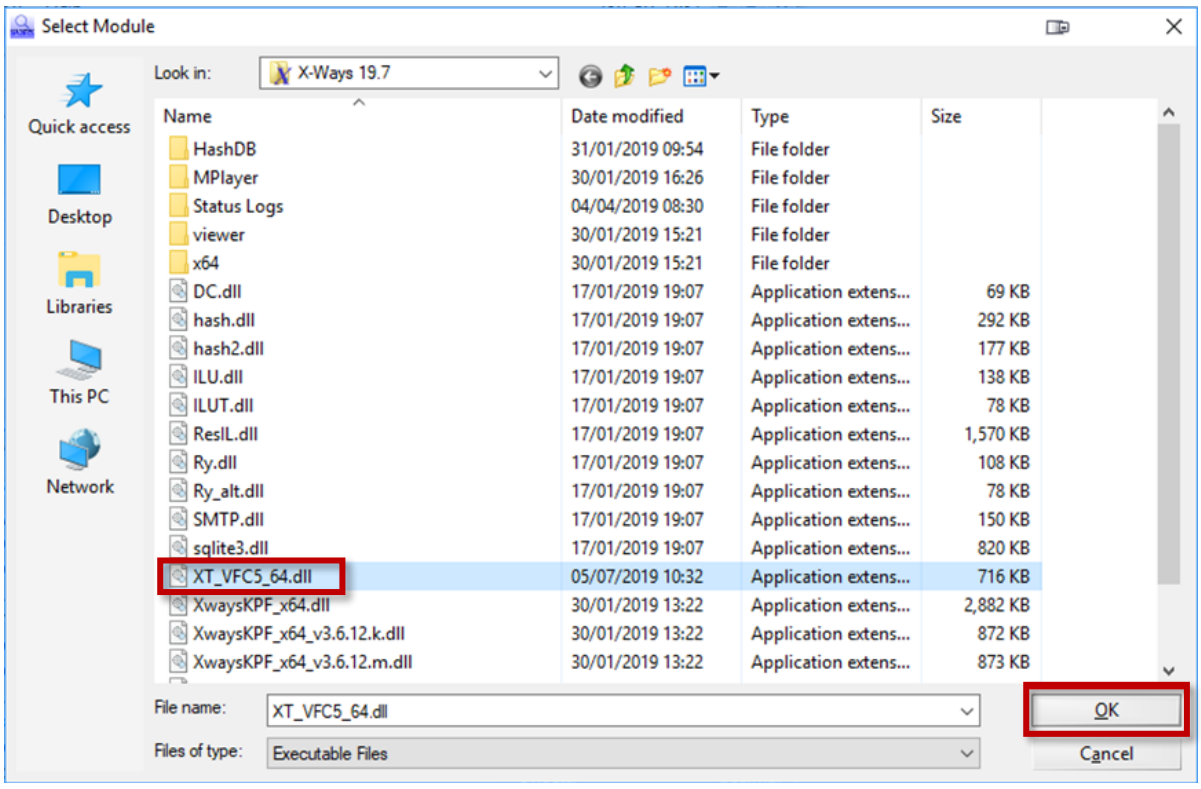
1. Determine if you are using the 32-bit or 64-bit version of XWF.
   - Each requires a distinct version of the XT_VFC5 DLL:
     * For 32-bit XWF use: XT_VFC5_32.DLL
     * For 64-bit XWF use: XT_VFC5_64.DLL
2. Open XWF (requires v18 or later)
3. Navigate to the Tools > Run X-Tensions menu



4. Click + and browse to the folder containing the XT_VFC5 DLL files



5. Select the appropriate DLL:



NB *There is no need to copy the file to the X-Ways folder. Just point XWF at the "Integration" folder to ensure the your X-Tension gets updated each time you upgrade VFC (if appropriate).*

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

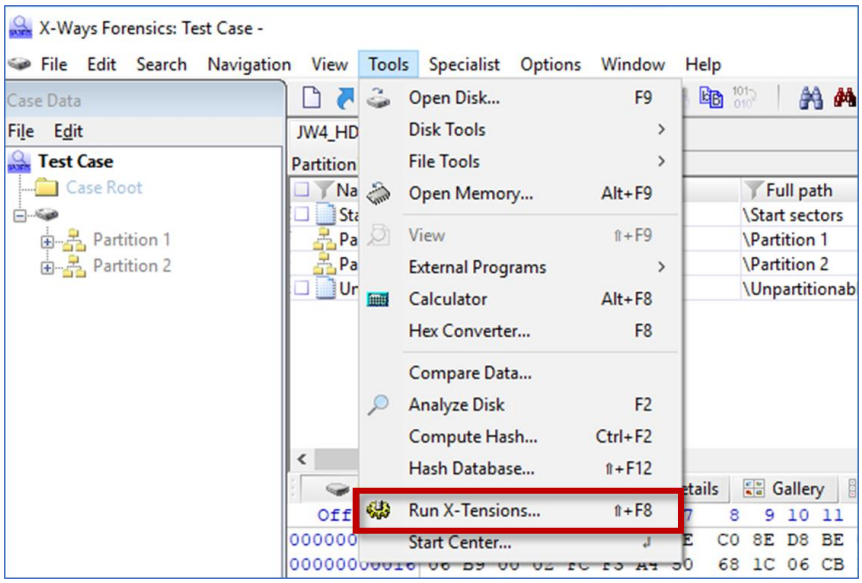
Selecting the X-Tension within XWF

To use the X-Tension in XWF proceed as follows:

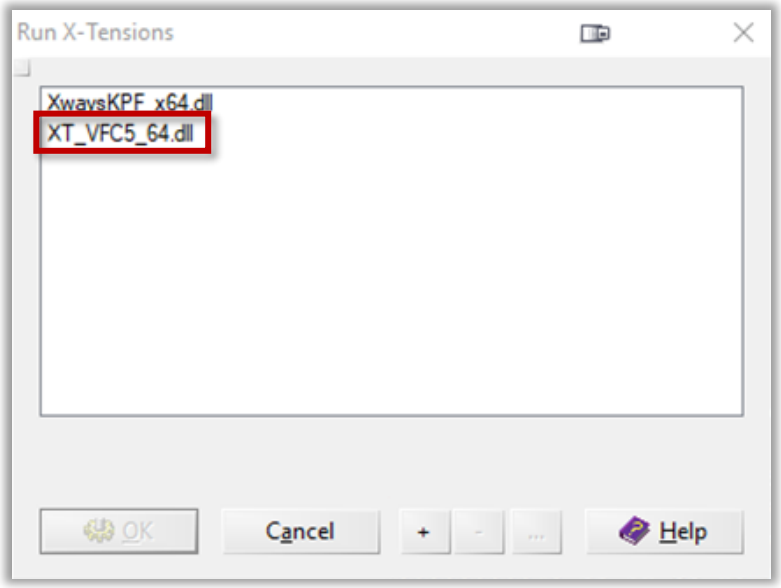
1. Confirm VFC v5.0.5 or later is installed correctly and has been launched at least once

2. Create / open the desired XWF case

3. Navigate to the Tools / Run X-Tensions menu

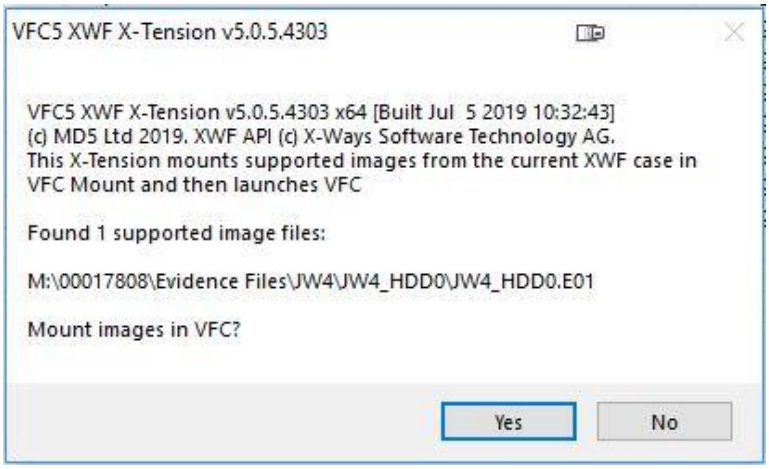


4. Double click the XT_VFC5 DLL in the list:



Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

5. Follow the on-screen prompts to run the X-Tension.



See the XWF message window for progress / troubleshooting information.

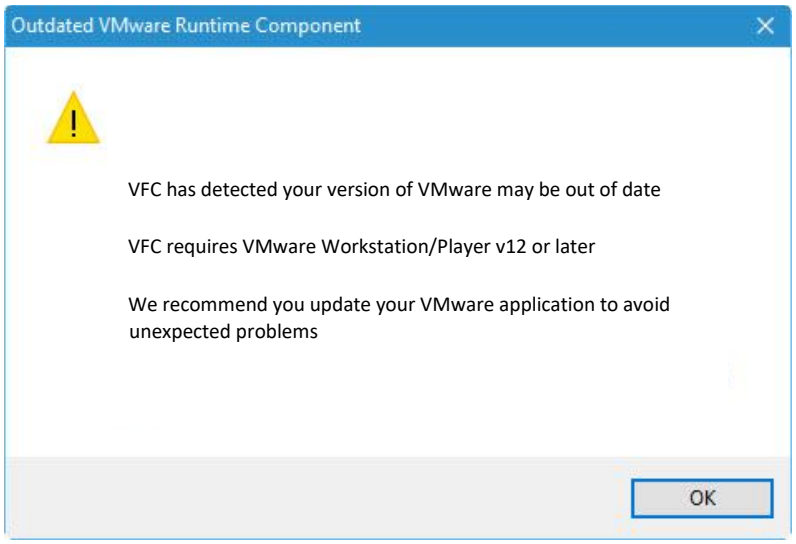
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Known Issues, Error Messages & Troubleshooting

Updated VMware Runtime Component

When you start VFC, any version from 4.16.8.10 onwards will perform a check of your host system for the presence of VDDK and VMware. It will also perform a version check to see if the VMware variant matches what has been tested against.

If your version of VMware predates the earliest supported version (currently v12.5), you will see this message (with varying version numbers):

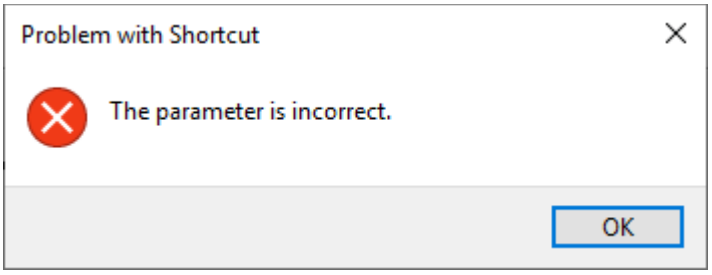


If your version of VMware is recent enough, this message should not appear.

Please note, if your version of VMware is older, you may experience some latency or restriction of functionality within VFC. If you experience issues, please consider updating your version of VMware.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

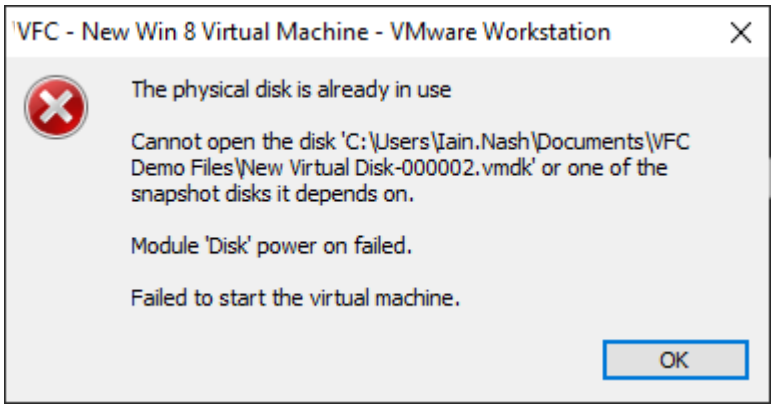
Problem with Shortcut – The parameter is incorrect.



If updating VFC, existing desktop shortcuts may cease to function. Please delete and recreate the shortcuts from the new program file in the Start menu.

The physical disk is already in use

Sometimes, when you launch or power on your VFC VM, you will find a message similar to this pop up and the VM will fail to boot:



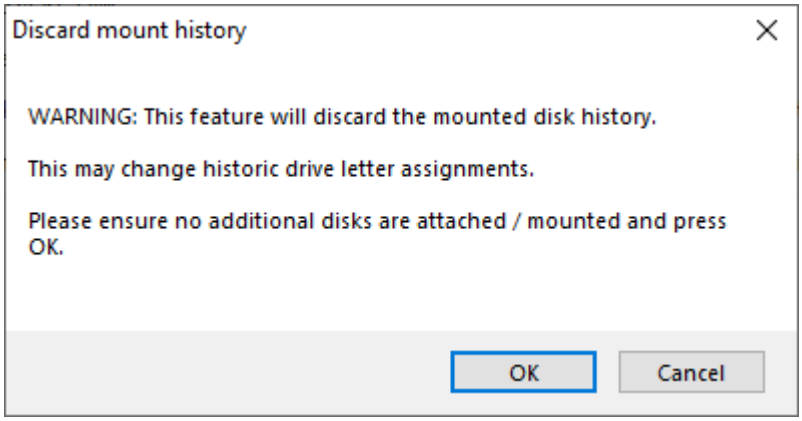
The Physical Disk In Use (PDIU) error is common when working with VMs. Historically, the only solution to this error was to reboot your forensic terminal. It was exceedingly frustrating but once it was there, it wasn't going away.

The features of the "Settings/Tools" tab can be employed to discard offline mount points and disable automatic mounting which allows VFC to have sole access to the connected physical drive/mounted image. Mounted drives will need to be unmounted and then VFC closed. VFC can then be reopened, the images can be remounted and the process started again – it is far from ideal but can prevent the user needing to restart their forensic workstation.

The problem is less likely to occur if you use VFC Mount because it contains special additional logic to mitigate this issue.

See the section above on the Settings / Tools tab for more information.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8



Similarly, with connected physical (tangible) drives, the drives should be disconnected, the tools used as above and the drives reconnected. It is likely that VFC will need to be restarted.

What causes PDIU errors?

Most users of VFC will come across the PDIU error quite early in their use of VFC.

It occurs when Windows automatically mounts new file systems and prevents VMware from gaining exclusive access to the underlying disk. Windows caches the signatures of previously mounted file systems so that it can quickly and consistently re-mount them again in the future. This means that once the PDIU error has occurred it is very likely to occur again. With this regard, if the above method does not work, it is very difficult to solve via any means other than a full system reboot.

To minimise the chances of experiencing this error it is recommended that when performing virtualisation with VFC, you follow the following steps, in order, by way of precaution:

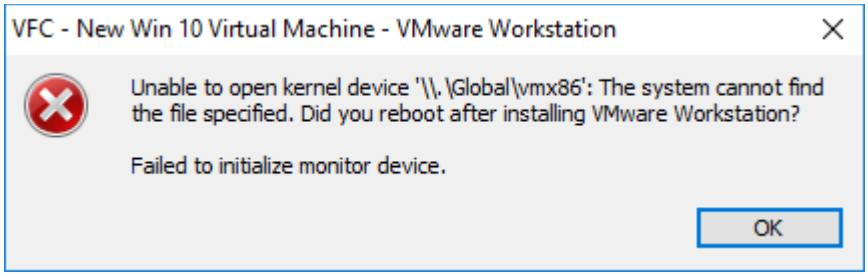
Recommended procedure:

1. Disconnect all external disks, write blockers
2. Unmount any mounted disk images
3. Tick checkbox
4. Press button
5. Prefer VFC Mount in future and always tick checkbox

Please note, this is not a guaranteed tactic but it should reduce the instances where you will need to reboot your system.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

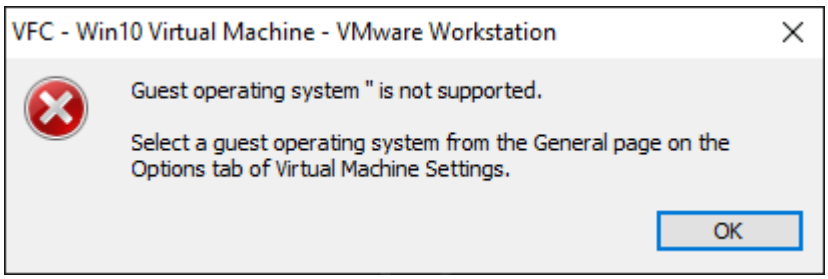
Unable to open kernel device



"Failed to initialise monitor device"

This error can occur if VFC or VMware are not being run with Administrator privileges.

Guest operating system " is not supported



This can happen if VFC has not correctly identified the OS and could require you to manually select the requisite OS from the drop-down list.

If this happens, please send a copy of your log file and an explanation of the issue to our Support team for further investigation by our Development team. Please send your log file to support@md5.uk.com.

VMware wants you to Take Ownership of the VM

Sometimes when trying to boot an image using VFC, once you generate and launch the VM you will get an error asking to take ownership and selecting either response can cause the VM to close.

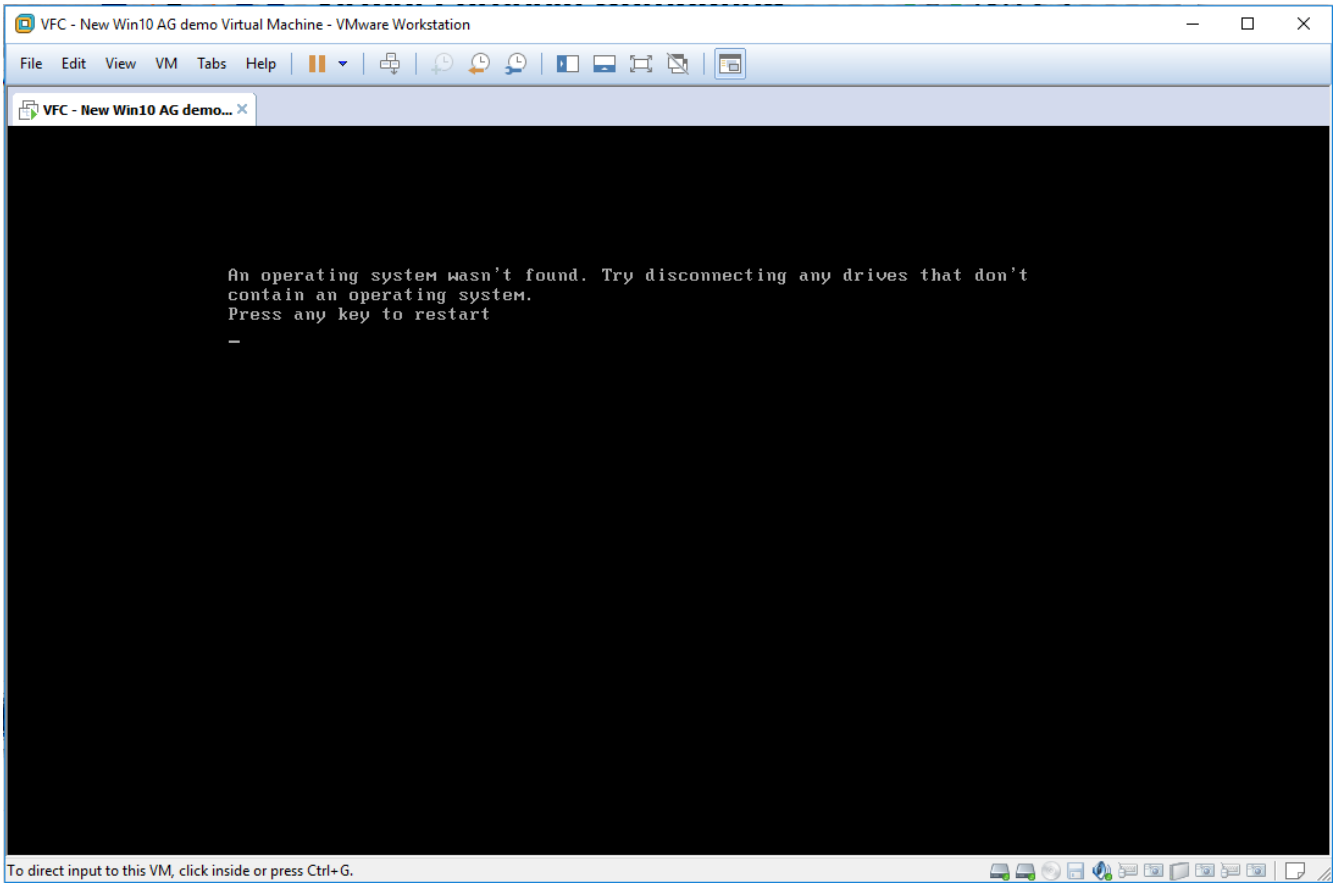
The most common reason this occurs is that the VM was created by VFC but you are trying to open it directly in VMWare. This will fail unless VMWare was launched with Admin rights (right-click, select 'Run as administrator').

If this doesn't resolve the problem, please check the VMWare log files. They should contain an explanation of why it has failed.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

VMware reports that the Operating System has not been found on Launch

An operating system wasn't found. Try disconnecting any drives that don't contain an operating system.



This can happen if you have created a VM with multiple drives and have chosen the wrong drive interface. Unless you know the exact configuration of the original hardware, the safest bet to avoid this issue is to add additional hardware using a SCSI interface.

Alternatively, you can change the boot order in VMware BIOS (or mount the disks in a different order in VFC Mount before creating the VM).

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

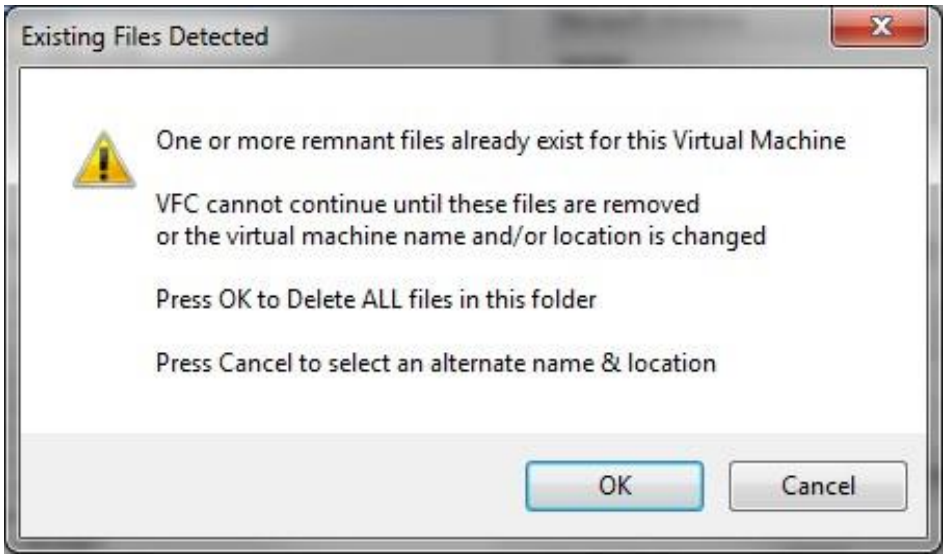
Cannot open the disk

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.

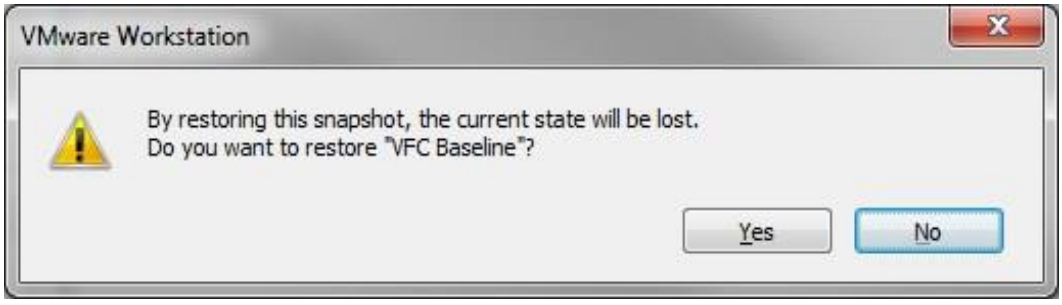
There are several methods to resolve this issue if it is encountered.

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



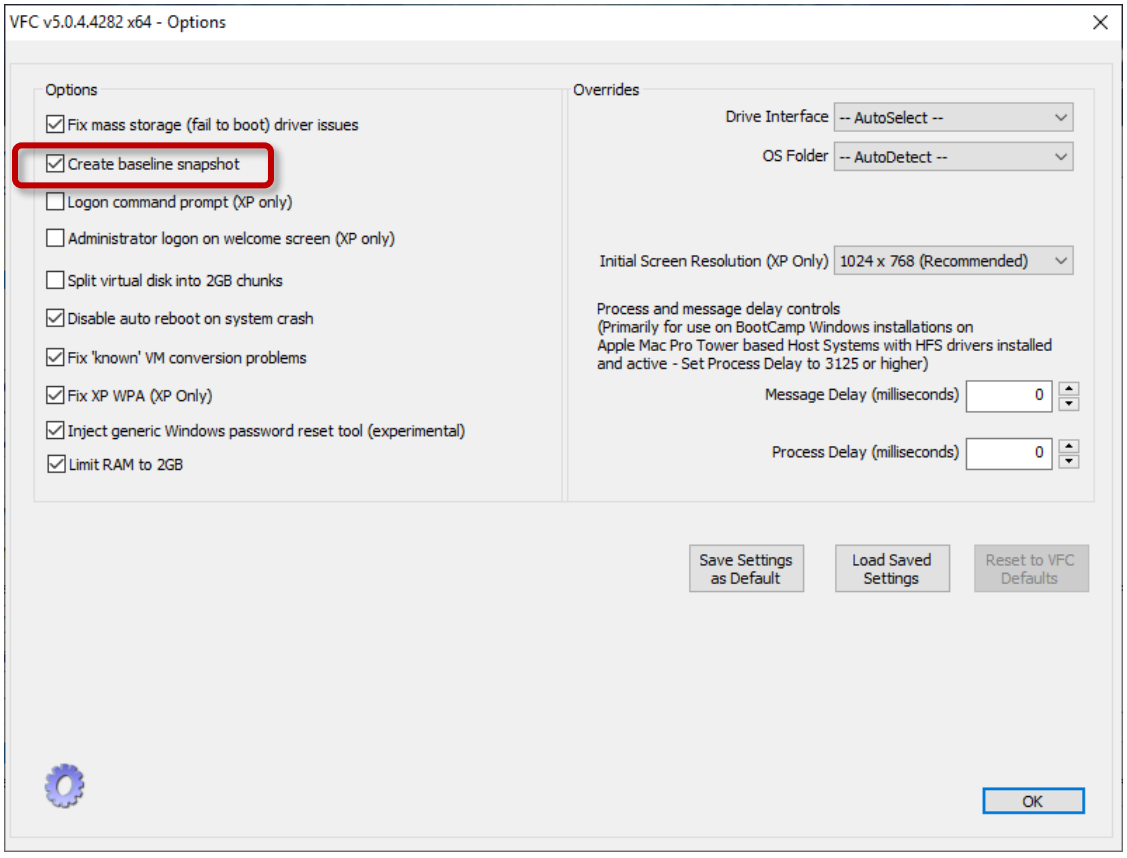
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

(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.



Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Host System is Windows 7 on a Boot Camp Mac Pro

It has been identified that when running Windows 7 on a Boot Camp Apple Mac Pro (and potentially other Mac hardware), VFC does not function as expected during the analysis and generate VM procedures.

It is believed that the installation of the Apple Boot Camp drivers causes an issue with VFC whereby the mounted disk caches (generated as part of the analysis and generation stages of the VFC virtualisation process) fail to be read correctly.

This failure to read the mounted cache partition leads to errors detecting the operating system and injecting the requisite patch code into the subject registry.

The current resolution is to either remove the Boot Camp drivers; adjust the 'Process Delay' setting to 3125 or higher, or both of these options, whereby it has been found that the VFC will function as expected.

Investigation and development continue in order to attempt to make VFC fully compatible with Mac based Windows installation which incorporates the Apple Mac Boot Camp drivers.

NB: The above is guidance that has come to us which we wanted to share because we can see how it could be useful. Whilst we understand that VFC may be used successfully with BootCamp we are unable to formally support this at this time.

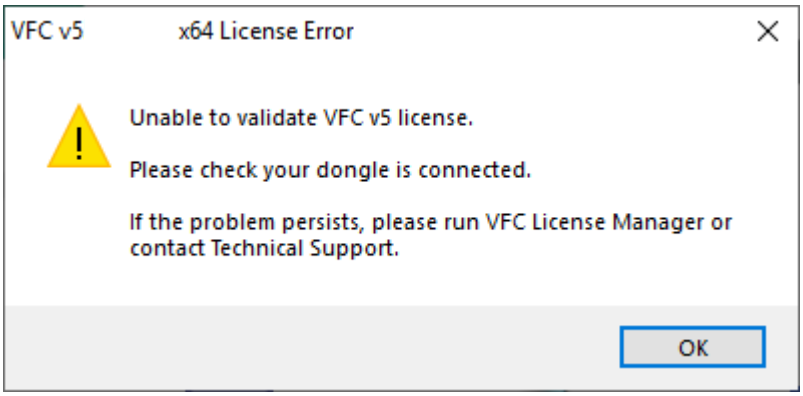
Could Not Unload Registry

If the VM generation process fails unexpectedly, this may result in the previous guest OS registry remaining mounted. This can prevent further VMs from being created. To fix this problem, please restart VFC to unload any remnant hives. If this fails, please reboot your forensic workstation.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

The VFC was unable to communicate with the dongle

If you attempt to run VFC without a dongle*, or with a green dongle and the dongle drivers have not been installed, you will see the following error message:



Install the respective drivers or plug in your dongle to overcome this.

*Please note, if your computer crashed while using VFC or for some reason VFC itself crashed, you may need to unplug and re-insert the VFC dongle to re-initialise the licence and release the licence from the previous session. If the issue persists, you may need to restart your workstation.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

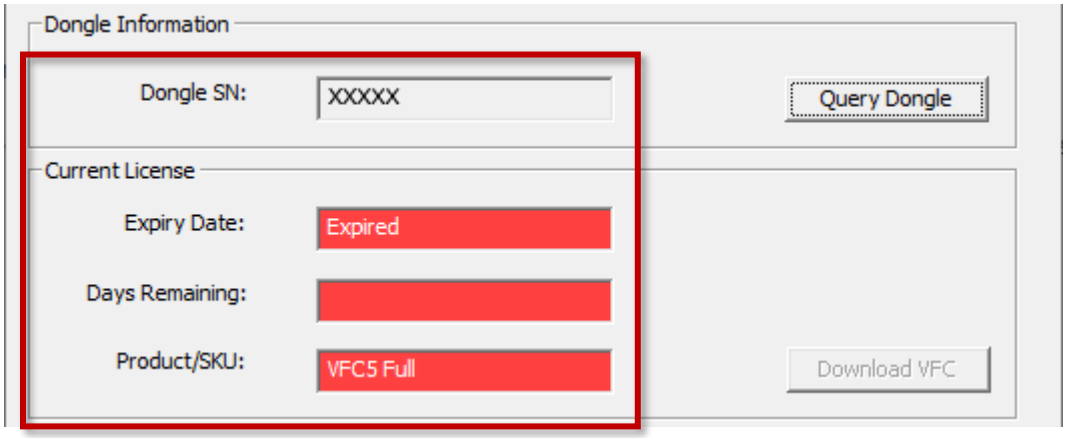
Updating your VFC Dongle

The VFC 'License Manager' is installed alongside VFC and can be accessed either from the VFC program installation folder or within the program itself. Please refer to the earlier section on **Updating or Upgrading your VFC Dongle**.

- **YOU MUST CLICK 'UPDATE DONGLE' TO APPLY THE NEW SETTINGS.**
- If you have multiple dongles that require updating, please insert only one at a time and program them independently. Once each has been updated, just swap the dongles and click 'Query Dongle' and start over again.
- To update multiple dongles, please program them one at a time and proceed as follows:

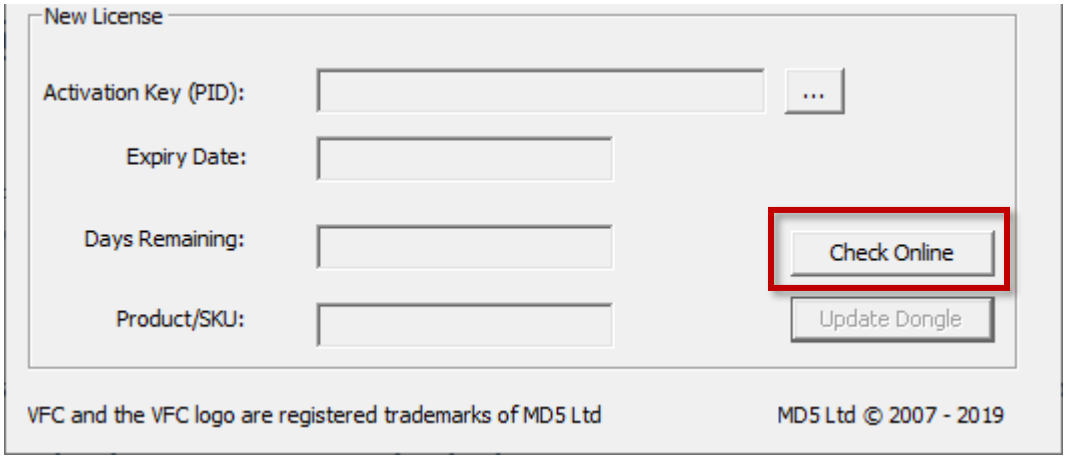
1. Insert the dongle and wait a few seconds for it to be detected by Windows
2. Click 'Query Dongle'**:**

3. The dongle serial number and existing license information (if present) should populate:

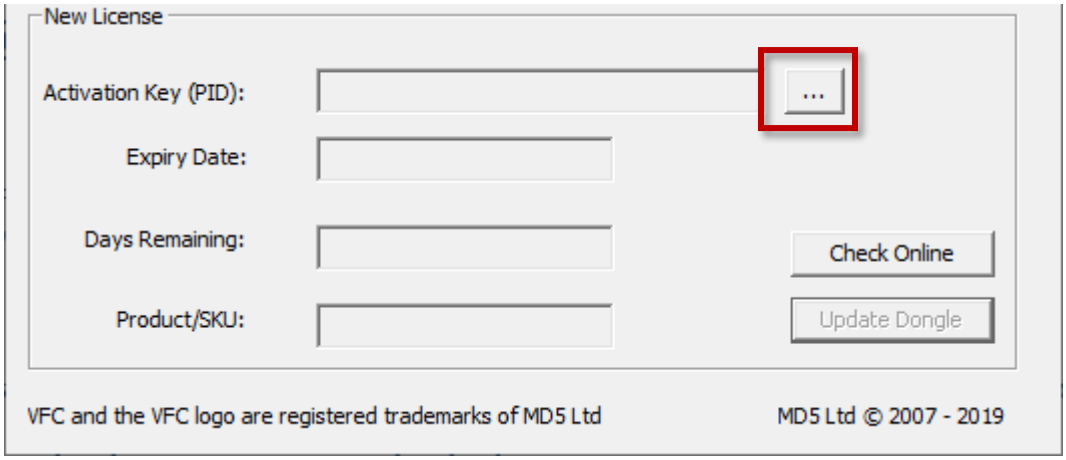


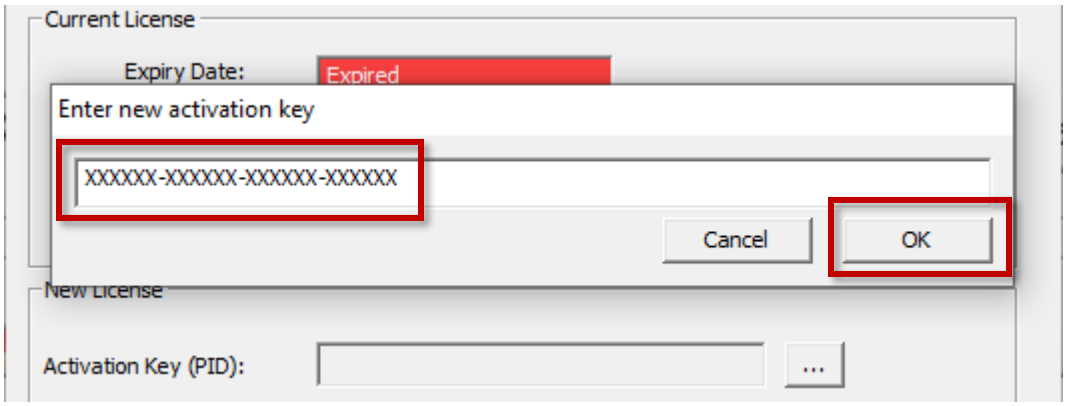
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

4. Depending on how you intend to update:
   a) If online: Click 'Check Online' to permit License Manager to query the online license system:

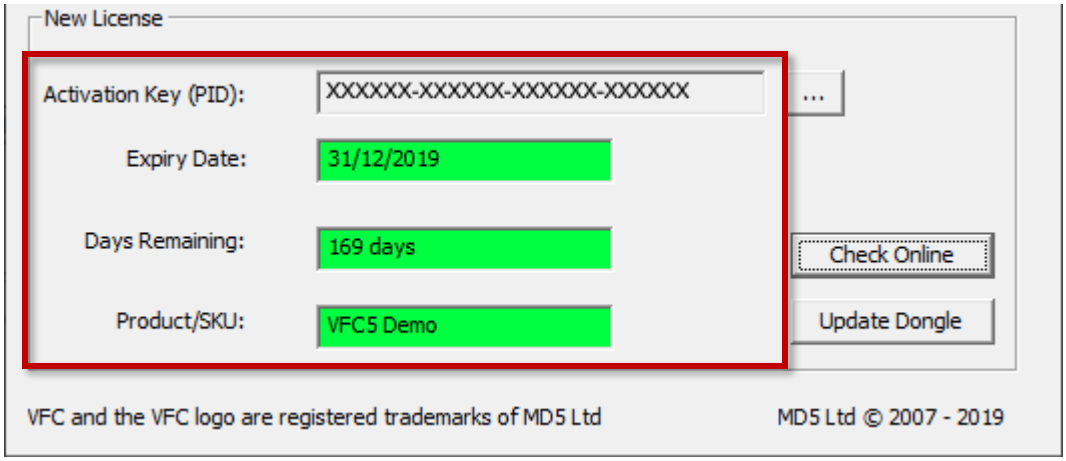


   b) If offline: Click '…' and enter the new PID authorisation code (this should have been supplied to you by our Sale team) and click 'OK':

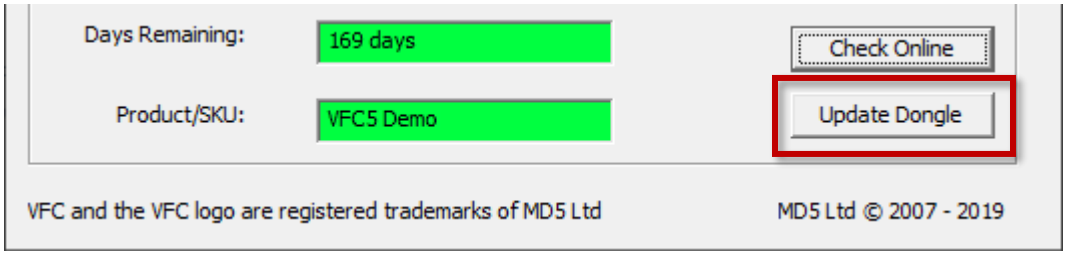




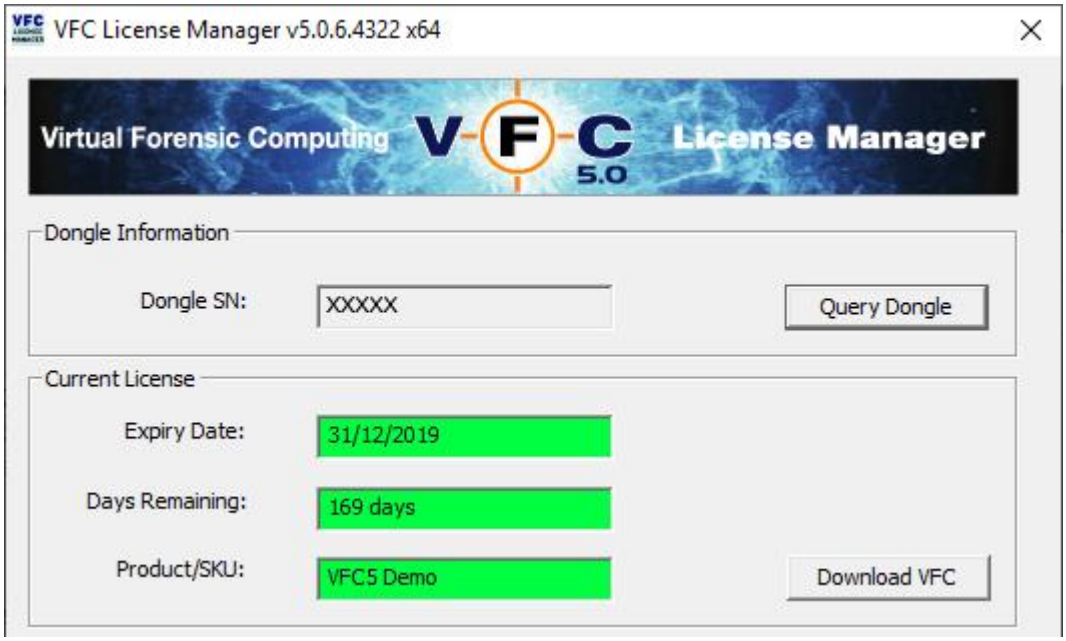
5. Confirm that the 'New License' information is as expected:



6. Click 'Update Dongle' to program the dongle:



7. The new license information will appear:

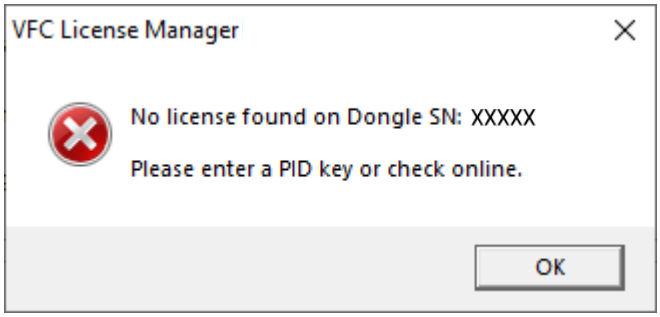


8. Remove dongle and repeat as necessary

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

No license found on Dongle SN: XXXXX

Please enter a PID key or check online



If you have problems updating your dongle or renewing your licence, this may be caused by the wrong dongle drivers being installed. Please ensure the relevant dongle drivers are installed if required.

Alternatively, this may be caused by the utilisation of an older and potentially obsolete version of the VFC License Manager tool.

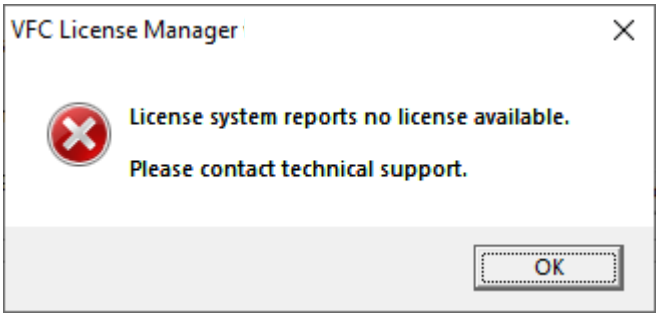
A third option is that your dongle was programmed with a legacy system and needs bringing up to date. Please install the latest License Manager software and contact our Sales team at sales@md5.uk.com if the update/upgrade instructions linked above don't work.

OLDER VERSIONS OF THE SOFTWARE CANNOT UPDATE DONGLES FOR VFC5.

Please ensure you are using the latest version of the VFC License Manager software. You may have existing shortcuts on your desktop to obsolete versions of the License Manager. It is recommended these are removed.

License system reports no license available

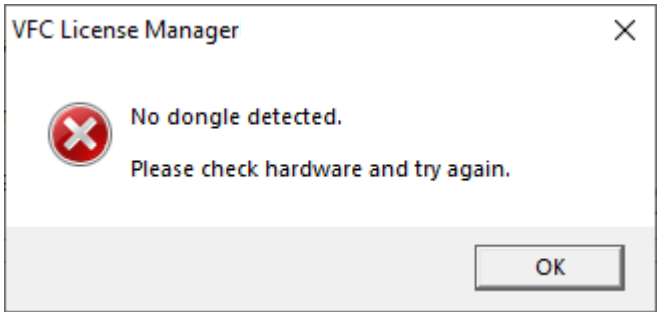
If you see this message, it could be that you are trying to access our database via a proxy server, or that the database doesn't currently hold an update for your dongle. If you see this message, please contact sales@md5.uk.com to check that the license has been upgraded, or to upgrade your subscription. They can issue you with a PID key if you are still experiencing problems:



Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

No dongle detected. Please check hardware and try again

If your dongle is not detected, please ensure your dongle is plugged in correctly:



If your dongle is not correctly detected and VFC fails to start or License manager reports no dongle detected, please try the following troubleshooting tips:

1. Remove / re-insert the dongle
2. Try the dongle on another workstation
3. Start VFC License Manager and click 'Query Dongle' (then follow appropriate instructions)
4. Contact Technical support

NT4 SP0-SP5/ NTFS OS will fail to boot after virtualisation with VFC

A virtual machine containing NT4 SP0 – SP5 will typically fail to boot after it has been virtualised with VFC.

This problem is caused by the Windows 2000 and later NTFS driver on the host PC. This automatically upgrades the on-disk NTFS format to v3.x the first time the file system is mounted. This upgrade process cannot be disabled. Unfortunately, the new NTFS format incompatible with Windows NT prior to SP6. There are two ways to work around this:

1. Install NT4 SP6 prior to virtualisation

2. Confirm the image to FAT (This will lose file permissions but should still produce a bootable system.)

NB *This is a Windows OS limitation and not a bug in VFC.*

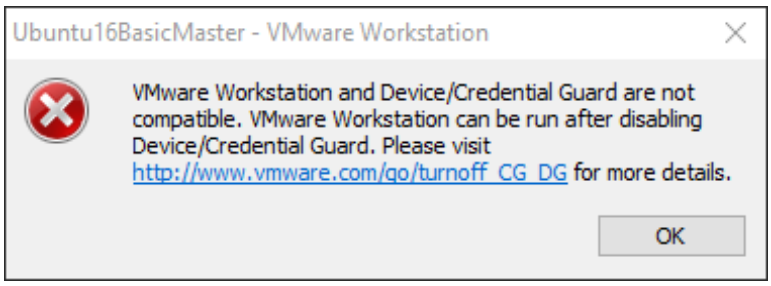
Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Windows 10 Creators Update

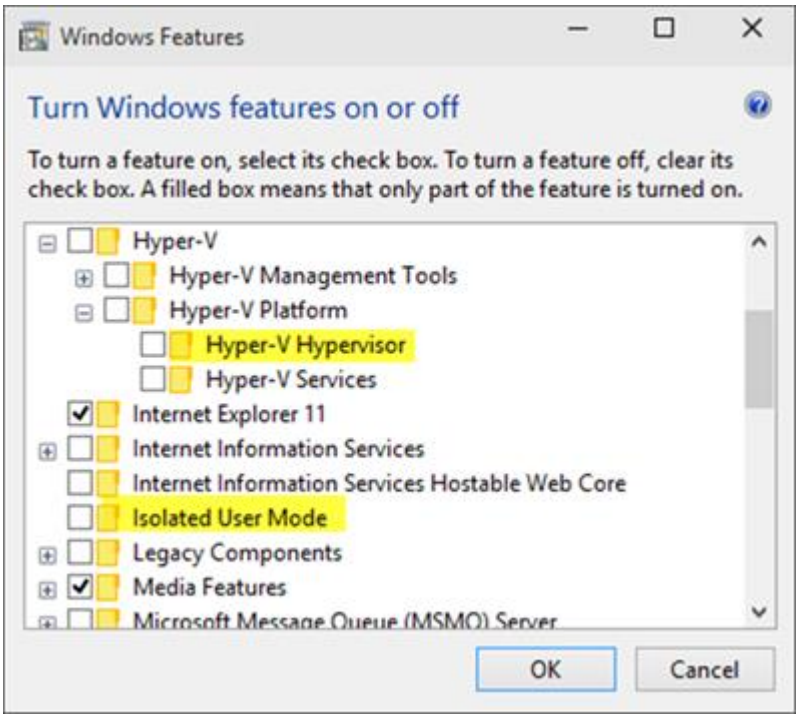
With the Win10 Creators update, Microsoft enabled Hyper-V by default. Hyper-V and VMware don't play nicely together and VMware won't run VFC VMs (and probably ANY VM).

The issue is that the various virtualisation platforms will not run concurrently and you should therefore only have one running at any time. To use VFC (and therefore VMware), you must disable Hyper-V.

If Hyper-V is enabled and you try to run VMware, you will see the following error message:



The fix is actually quite straightforward, in that all that is required is that the newly auto-enabled Hyper-V feature just needs to be unchecked and 'turned-off' within the Windows features menu:



Please note, this is a VMware/Microsoft and User-environment issue, and not directly related to VFC.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Frequently Asked Questions

Which Disk Formats are supported by VFC?

VFC continues to develop and currently supports:

- Forensic image files mounted using VFC Mount Tool (preferred)
  - It currently supports .E01, .EX01, AFF4, .VMDK, .BIN, .IMG, .RAW, and .DD images.
- Forensic image files mounted using AccessData FTK Imager 3
- Forensic image files mounted using Mount Image Pro
- 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 virtualise the following:

- Windows 3.1
- Windows 95
- Windows 98
- Windows ME
- Windows NT
- Windows 2000 (Pre, Server and Advanced Server)
- Windows XP (Home, Professional, Media Center, Professional x64)
- Windows Vista (x86 & x64)
- Windows 7 (x86 & x64)
- Windows 8 (x86 & x64)
- Windows 8.1 (x86 & x64)
- Windows 10 (x86 & x64)
- Windows Server 2003 (Web, Standard, Enterprise, DataCenter, Small Business – x86 & x64)
- Windows Server 2008 (x86 & x64)
- Windows Server 2012 x64
- Windows Server 2012 R2 x64
- Windows Server 2016 x64
- Windows Server 2019 x64
- Linux (experimental)
- MAC OS X (10.5 and above) (experimental)
- Sun Solaris

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

What do I need to run VFC?

VFC utilises the freely available VMware Workstation Player/Workstation Pro, Virtual Disk Development Kit (VDDK) and a Mount Utility to mount forensic images files – it comes with its own Mounting tool and a table version of VDDK is supplied so you will only need to acquire a copy of VMware.

Do I need to have a mounting utility?

Not strictly. VFC is capable of using physical disks or 'dd' images and comes with its own mounting utility (VC Mount) so there is no need to utilise a third-party mounting tool for VFC to work.

VFC Mount creates read-only physical disks. FTK Imager/Mount Image Pro may be required if you need an option to allow for it to be blocked but writeable. This may be the case if you need to be able to change the files (in the cache) for making changes to the OS and/or for hacking defences (deploying sniffers etc.).

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 host system will almost certainly try to write to the physical disk and this will change the evidence.*

Do I need to have EnCase?

EnCase is only required if you wish to utilise the Encase Physical Disk Emulator (PDE) in order to emulate a physical disk. VFC Mount, FTK and MIP will provide the same solution in a more flexible format.

Please note, if using EnCase PDE, you will only be able to mount one image at a time so the options for adding drives via Modify Hardware will not be available.

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, or workaround full disk encryption without the encryption key.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

Will booting an image using VFC alter the original evidence?

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.

Does VFC support 'partition only' images?

No. This feature didn't work properly in earlier versions and was dropped for v4.50.

Does VFC support multi-boot systems?

Yes, multi-boot systems will generally work. In some cases, for instance if one OS requires legacy BIOS start-up and another uses EFI based start-up it may be necessary to create two distinct VM's using VFC. This is necessary because VMware can emulate either BIOS or EFI but not both at the same time.

I've used VFC but still get a BSOD halfway through the boot sequence! (What should I do?)

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

- Full disk encryption or wrong disk interface (SCSI, SATA or IDE)
- NVidia or ATI graphic drivers
- custom audio drivers
- OEM specific utilities

If you are stuck in a repair-cycle boot-loop it may be necessary to change some settings using the "Options" button on the home-screen.

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 and then reboot. This should result in the VM being more stable and functional.

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

VMware Workstation Pro and VMware Workstation Player 12 and above include a suite of tools known as the VMware Tools Package. Installing this will improve the performance of the VM.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

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 network. It is possible to add network support and hence connect to other networks (including the Internet), but this is not recommended. Adding Network support is currently a manual process undertaken at the discretion of the user.

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 Workstation 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 should be able to 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 dependent 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.

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8

How do I get Additional Support?

You will find the most up-to-date version of the VFC User Guide and other useful documentation available to download online at:

vfc.uk.com/downloads

Please check the User Guide in the first instance. For other enquiries not answered by the User Guide, please:

- e-mail support@md5.uk.com or
- call us on +44 (0)1924 220 999 between 08.30 and 16.30 GMT

We aim to respond to all requests within 48 hours.

Download Links

VFC SOFTWARE & PWB.BIN

https://www.vfc.uk.com/downloads

VMware Workstation Pro or Workstation Player

Buy:

https://store.vmware.com/store?Action=home&Locale=en_GB&SiteID=vmwde

Try:

https://www.vmware.com/uk/products/workstation-player/workstation-player-evaluation.html

VMware VDDK 5.1.4

(please find a copy in the downloaded VFC-Setup folder)

Copyright 2007-2019 MD5 Ltd, Revision 19.8.30.5.0.8