VFC5 Data Sheet

VFC5 makes it easy to create a virtual machine (VM) replica of a target system.

- Works with mounted forensic images and write-blocked physical drives
- Quickly creates VMs of Windows, Linux, Solaris and other OS platforms
- Simplifies the VM-generation process into a few mouse clicks
- Command Line options aid integration with existing forensic analysis tools
- VMs can give access to evidence that would otherwise be unavailable
- VMs help explain technical concepts visually

First launched in 2007, VFC is the original virtualisation solution for the forensic investigator. It saves crucial time by enabling an investigator to recreate and interact with the "digital crime scene" within a matter of seconds! With efficiency savings made throughout the entire VFC process, VFC5 is lighter, faster, more powerful and more integrated than ever before.

With VFC5, the preparation of powerful visual evidence is easier than ever!

New Features

VFC Mount™, MD5's proprietary, complementary mount tool – VFC Mount™ helps speed up the mounting process and removes issues associated with mounting forensic images with incorrect settings. VFC Mount also takes steps to reduce instances of common VMware errors such as "The physical disk is already in use" (see **VMware KB 2046678**).

Command Line Interface (CLI) allows you to launch VFC from existing forensic analysis suites – CLI enables integration with major forensic analysis tools. VFC5 is supplied with EnCase 'EnScript' and XWF 'X-Tension' plugins to launch VFC from within EnCase & X-Ways Forensics*. Further forensic software integration will follow.

Enhanced Password Bypass (PWB) – PWB now supports over 2,300 discrete Windows builds and VFC5 has added a fuzzy logic search feature to increase the chances of a successful routine being found. PWB can be used on any suspended Windows VM.

Generic Password Reset (GPR) with integral "Live ID" exploit – GPR is completely separate to the Password Bypass (PWB) feature. It injects a proprietary VFC component into the generated VFC VM, which can then be used to identify Windows user accounts and change passwords to known values. It can also be used to open a powerful system-level Command Prompt.

64-bit host system support – delivers enhanced compatibility with modern systems.

Technical Requirements

VFC works alongside VMware's Workstation Pro (or Workstation Player) and Virtual Disk Development Kit (VDDK). MD5 have found VMware to be the most reliable virtualisation solution which makes for a smoother user experience. To use VFC5, you will need:

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

vfc.uk.com

* Visit **https://www.vmware.com/uk/products/workstation-player/workstation-player-evaluation.html** to download the free/evaluation version of VMware.

✞ 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.

MD5
evidence you can trust

How It Works:

VFC interrogates the target drive to gather relevant system information, so that it can very quickly build the VMware framework to create a forensically sound replica of the target system (the exhibit) as a Virtual Machine (VM). It follows accepted forensic practices while fixing known problems to avoid BSOD and driver errors, often saving the user hours of manual diagnosis and repair.

VFC offers the option to add hardware to an existing VFC VM (e.g. to rebuild a tower system with multiple drives), and the capability to export a standalone clone of a VM, for further investigation without tying up the forensic workstation further.

VFC5 ships with XWF X-Tension and EnCase EnScript integration components. Both behave in a similar way; they mount supported images from the current case (in XWF or EnCase respectively) using VFC Mount™, 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.

Current supported formats are: .e01, .ex01, .vmdk, .bin, .img, .raw, .dd, AFF4

VFC Key Features & Benefits

Launch VFC from existing Forensic software using pre-written scripts* or build your own command line processes.

Avoid common errors when working with mounted images by using VFC Mount™ to mount images. VFC also gives quick access to popular mounting tools such as FTK Imager and Mount Image Pro via the newly added quick-launch buttons in the program footer.

Boot a (mounted) forensic image of a suspect's computer and experience the "desktop" as seen by the original user. Supports Windows 3.1-Windows 10 (including GPT formatted disks), Apple Mac OSX, Linux and SunSolaris OS. Works with mounted forensic images, physical drives and now also VMDK files.

Take screenshots of key evidence such as folder structure, evidence location, recently accessed files, browsing history, saved passwords, P2P shares and virus definitions among others.

Interact with fully licenced software to view files and data in its native environment (e.g. Sage or QuickBooks) without the need to invest in a copy of the often-expensive or obsolete/proprietary software.

Interact with connected devices (e.g. iPhones connected to iTunes accounts on the VM or encrypted USB drives).

Bypass local Windows User Account passwords in seconds. VFC5 includes PWB routines for over 2,300 discrete Windows builds. PWB can also be used on non-VFC VMs. No need to reinstall the software for updates; just update the PWB5.BIN database.

The Generic Password Reset (GPR) feature is very powerful. It works by injecting a proprietary VFC component directly into the VM. This component allows you to easily reset a user account password or open a powerful system-level Command Prompt

Local User Account Password hashes are extracted to the splash screen and embedded in the VMX annotation (and stored in the VFC log file). The provision of password hashes enables the use of external hash-cracking tools to identify the original system-password. This helps with programs that require EFS access.

Add Hardware to an existing VFC VM using a straightforward wizard to load multiple drives into an existing VM (to rebuild the suspect machine as last viewed by them).

Point-and-click generation of a standalone Virtual Machine for sharing with non-technical departments (which won't need VFC).

Repair a VM or 'rewind' it back in time using Patch VM/Restore Point Forensics.

* VFC5 contains Command Line functionality. With the correct interface – such as an EnCase EnScript, or an XWF X-Tension – VFC can be launched directly from the analytical platform. VFC5 comes with pre-prepared scripts for integration with EnCase v6, and v8 and also X-Ways Forensics (XWF) v18 and later.

Schippers IT

Schippers IT B.V.
www.schippers-it.nl
+31 (0) 161 454 449
sales@schippers-it.nl

MD5
evidence you can trust