



## VFC (Virtual Forensic Computing)

VFC is one of the most significant breakthroughs in forensic computing in the last ten years. VFC enables investigators to rapidly recreate a subject machine in a virtual environment directly from a mounted forensic hard drive image. The investigator can then experience the 'desktop' as seen by the original user in an entirely forensic manner.

There are numerous specialist software applications available to assist the investigation and analysis of digital media which has been forensically acquired. Whilst these tools can and do provide a great depth of analysis and will reveal data fragments of material no longer readily available, it is often the case that the 'scene of crime' part of the examination process is overlooked as an additional source of potentially invaluable information.

In the 'real' world, it is almost unthinkable not to examine in detail the actual crime scene and then perform 'forensic' examinations on evidence gathered from the scene. In the 'virtual' world of Forensic Computing, the same is not true and all too often it is only the underlying data and information that resides on the storage devices that is examined in detail.

The VFC (virtual forensic computing) application utilises VMware's freely available Player or server software to assist in re-creating a subject machine within seconds.

VFC can successfully create bootable virtual machines from:

- > Encase (\*.e01) or Smart (\*.s01) forensic image files (requires Mount Image Pro - [www.mountimage.com](http://www.mountimage.com)).
- > Write blocked original storage devices.
- > Unix style 'dd' bit-for-bit disk images.
- > Vobson format 'img' image files.

VFC has been developed by Michael P enhallurick, a senior forensic computing analyst with MD5 Forensic Solutions. In 2005 an abridged version of his research was published in Digital Investigations, a magazine aimed directly at the forensic computing arena. His successful methods of transposing digital data into a virtual machine have been read and utilised by investigators across the globe. Building from this research, Michael has now developed this standalone application that enables an investigator to experience almost any Windows based system within seconds of acquisition.

- > There is no need to have access to a full forensic application or any additional disk emulation modules.
- > There is no need to create full, uncompressed, bit for bit sector copies of the original media.

Once the forensic image has been acquired, simply mount it, select the relevant drive, generate the virtual machine and launch it in VMware in seconds!

VFC has been successfully applied to every Windows version from Windows 95 through to the newly released Windows Vista.

Michael P enhallurick holds a Master of Science Degree in Forensic Computing and has over 25 years computing experience. He has been involved specifically in forensic computing since 1997 and for the past four years has undertaken detailed research into 'cloning' digital data so that it can be experienced inside a virtual environment.

Windows is a trademark and copyright of Microsoft Corp.  
VMware is a trademark and copyright of EMC.  
Mount Image Pro is copyright of GetData.

MD5 Ltd  
PO Box 96  
Normanton  
West Yorkshire WF6 1WY  
Tel: 01924 220999  
Fax: 01924 899856  
e-mail: [info@md5.uk.com](mailto:info@md5.uk.com)  
web site: [www.md5.uk.com](http://www.md5.uk.com)



INVESTOR IN PEOPLE

GetData Pty Ltd is an authorized reseller of MD5  
1A / 124 Forest Road,  
Hurstville NSW, Australia, 2220  
Ph: +61 2 82086053  
Fax: +61 2 95808447  
sales@getdata.com  
web site: [www.getdata.com](http://www.getdata.com)  
web site: [www.mountimage.com](http://www.mountimage.com)

