

Virtual Forensic Computing

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

The science of forensic computing encompasses the identification, analysis, preservation, and presentation of digital evidence in a legally acceptable manner, covering not only computers, but all manner of digital storage devices. Data retrieval is accomplished using the accepted and proven concepts of digital image acquisition. Subsequent to acquisition, a number of specialist 'forensic' tools can be used on the secured data in order to perform detailed examinations. The forensic methodology enables an investigator to report upon their findings and allows them to reach conclusions based upon the scrutinised material, without fear of altering any of the original material.

There are a vast number of specialist tools available to an investigator to assist in the analysis of acquired digital media. Whilst such tools can and do provide a great depth of analysis, it is possible that the 'scene of crime' part of the examination process is often overlooked as an additional and perhaps valuable source of information.

Although forensic computing provides great insight into both current and previous activity on a system, the actual environment that a user would experience often remains unvisited during a forensic examination.

How better to gain a feel for what a user would have seen, how they had their desktop settings, the actual software they were using, other than by using a clone of their original system.

Hard disk cloning provides a method by which the original system can be used, just as a user would have seen it, by copying the original disk and placing it back into the original machine.

But what if the original machine is not available...

Or indeed it may have been damaged and the hard drive containing the data is all that has been obtained...

Any cloned disk will need to be hosted in a different computer environment – one which will doubtless modify some of the settings of the original.

Each time the machine is started, changes will be made to the cloned disk – to replicate the processes will involve time-intensive re-cloning of the original.

Virtual Forensic Computing, or more accurately, 'methodologies for using virtual environments to access cloned / mounted subject hard disk images', details an investigation into the restoration of forensically acquired digital data to virtual hardware. The objective of the investigation was to devise a methodology by which a subject operating system could be operated within a wholly virtual environment. This would enable the investigator to experience the subject system in a controlled environment where file system changes

could be discarded and the 'original' clone preserved for future, repeatable usage, with minimal time-overheads in relation to creating a 'clean' copy of the original.

In certain circumstances, it is possible to create a forensically sound virtual clone of a subject computer within minutes of completing the forensic acquisition process. In other circumstances, it is necessary to 'clone' out the original disk (from the secure forensic copy), to a 'virtual disk' that can be operated inside the virtual machine, in essence exactly as if 'real' physical hardware were to be used.

When referring to forensically sound, it is necessary to consider the four Principles of Computer Based Electronic Evidence, as detailed in the Association of Chief Police Officers Good Practice Guide for Computer based Electronic Evidence.

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

By utilising the Virtual Forensic Computing methodology, all aspects of these principles are adhered to, in as much as any subject machine is not accessed other than through a secure forensic image or a 'virtual' clone thereof.

The systems researched and activated using the methods described encompasses Windows 95/98/ME & Windows NT/2000/XP.