Analysis of USB Flash Drives in a Virtual Environment

Derek Bem and Ewa Huebner

***Abstract*—This paper is a continuation of our previous work [1] in which we proposed an approach where two environments, conventional and virtual, are used independently in the forensic analysis of computer systems. We discuss the use of virtual environments in the analysis of USB flash drives in computer forensics investigations. After briefly introducing general concepts of a virtual environment and software tools we show how this approach can be successfully used in the analysis phase of the computer forensics investigation of portable USB flash drives. We also show why virtualisation technique can complement but not completely replace conventional methods of computer evidence analysis.**

***Index Terms*—Computer Forensics, Virtual Machine, computer evidence, USB drive.**

I. Introduction

In this paper we examine the application of the virtual environment in the analysis phase of a computer forensics investigation of USB flash drives. The commercial product VMWare [2] is used to illustrate the strengths and weaknesses of a virtual environment methodology. The environment created by VMWare is considerably different from the original computer system acquired during the process of forensics investigations; analysis of the evidence using VMWare by itself is likely to taint the evidence and make it inadmissible in a court of law. There are considerable differences between original and virtualized machines; the latter emulate a very limited range of hardware. For example, VMWare creates virtual machines with "standardized virtualized hardware" presented to the applications [3] which is very unlikely to be the same hardware as the investigated machine used. This limits the use of virtual environments in computer forensics examinations where 'do not alter the original evidence' is the most important rule [4]. In our previous work [1] we proposed concurrent and independent use of conventional and virtual environments where two copies of forensically acquired images are produced:

- the first, original evidence copy is protected using Standard Operating Procedures and the strict chain of custody rules, and analysed exclusively with forensically sound tools by a more experienced investigator,
- a working copy (or multiple working copies) are made from the evidence copy and analysed in a virtual machine environment by a less experienced investigator who is not constrained by strict forensics procedures.

D. Bem, MElecEng Warsaw, MIEAust, CPEng (d.bem@scm.uws.edu.au) is a Lecturer in the School of Computing and Mathematics at the University of Western Sydney, Australia.

E. Huebner, MElecEng Warsaw, PhD Sydney, MACS (e.huebner@scm.uws.edu.au) is a Senior Lecturer in the School of Computing and Mathematics at the University of Western Sydney, Australia.

Any findings made by the less experienced investigator are documented and passed to the more experienced investigator who confirms them in accordance with appropriate forensics rules.

Further we present a scenario to illustrate our approach. We used a 128Mb USB flash drive with portable application software installed, acquired a forensic image of the USB flash drive, and demonstrated the process of using two environments to analyse the acquired image. The example scenario shows the benefits of the virtual environment approach such as reducing the time required to analyse the evidence, increasing the chances of discovering important data, and allowing less qualified personnel to be involved in a highly productive way. We also show the potential dangers which may cause tainting of the evidence if correct procedures are not followed. We decided to use only free, readily available utilities to allow everyone to repeat our experiments, and to encourage the reader to try experimenting with their own cases.

II. Computer Forensics and USB Flash Drives

For the purpose of this paper we look at the computer forensics investigation as a process which can be divided into four major phases [5]: access, acquire, analyse (the focus of this paper) and report. During the access phase an incident has been identified, or there is a strong suspicion that an incident has happened. An initial responder records the basic details and notifies the individual responsible within the organisation for starting the correct procedure. During the acquiring phase relevant data is collected and passed to the team responsible for analysing it. The end result of this analysis is a report which, if required, may be used in a court of law. It is worth noting here that the 'four phases' classification is somewhat arbitrary, and other sources divide incident response into more steps [6]. Within each specific organization this allocation of 'who does what and when' would obviously vary, however one rule remains common: if the response and findings of the investigators involved in computer related crimes are to be of any use as court evidence they have to comply with the same rules as any other conventional investigations.

USB flash drives (also known under many other names) are NAND-type flash memory data storage devices integrated with a USB interface controller. They were invented in the 1980s with the first commercial models reaching the market in 2000. The first USB drives offered very small storage capacities by today standards, but they still compared very favorably with physically larger and less reliable 3.5" diskettes. At the time of writing USB flash drives with capacities ranging between 512MB to 2GB are the most common and affordable, with

larger capacities of 4-8GB also available. The drives with a capacity of 64Mb and below are considered obsolete. A few companies offer drives with a maximum capacity reaching 64GB [7], [8]. While 64GB drives are currently very expensive at around US$3,000-5,000, it is safe to predict that the existing drives will become more affordable, and that drives with even higher capacities will be developed in the near future.

Due to their portability and robust construction (no moving parts) the first major and still most common use of flash drives is to transport personal data like documents, spreadsheets, and pictures. However when the USB flash drives capacity reached around 32MB-64MB and higher, consumers noticed that USB drives open a new possibility: to carry applications that can be run on any standard computer without installation. This became practical only in recent years when USB drives reached a higher capacity at a low hardware cost.

Typical software for Microsoft Windows is not designed to be portable: it relies heavily on the Windows registry, installs or uses already installed dynamic libraries (DLL), stores files and profiles in various system folders, and generally does not provide a portable installation option [9]. To make a portable application a software developer needs to write it in such a way that it does not use the Windows registry, nor store its files anywhere on the host computer. There are many applications written in such a way. Many Web sites also offer advice on how to modify the existing software to make it portable. Recently a new class of commercial software emerged which converts conventional non-portable applications into portable applications [10]. The degree of success varies, and some applications changed for portability do not work.

A new emerging standard for USB flash drives with very strong industry support is U3 [11]. U3 compatible drives and compatible software allow for the creation of a portable full user environment including applications and user files. One can plug a U3 drive into any PC, and use applications installed on the drive to perform practically all tasks one would perform on a desktop computer. What is of particular interest in computer forensics investigations is the statement regarding U3 compliant USB flash keys with installed portable software: “when you unplug it, it leaves no personal data behind” [11].

Yet another complete portable environment is PortableApps [12], a free, actively developed compilation of software tools which offers easy to use installation and menu. PortableApps does not require U3 compatible hardware. Again, a computer forensics investigator should notice that PortableApps can also be used on any Windows computer, and it does not leave any personal data on the computer when unplugged.

III. The Dual Parallel Approach to USB Flash Drive Analysis

A USB flash drive which is part of a forensics investigation may be found plugged into a USB port of a running system, or it may be separated from a computer and inactive. During the acquire phase an investigator has to create a forensic (bit by bit) image of all storage devices [13]. An image of a USB storage device is typically acquired using a dd based tool [14], and is stored in the dd format [15] or a proprietary format typically based on dd [16]. The image is considered to be a forensically valid copy of the original USB flash drive, and it can be analysed using one of many forensics tools in a similar way to analysing dd images acquired from hard disk drives.

The conventional computer forensics technique is then to copy the acquired image to a hard drive and analyse it using appropriate forensics software. This method works best for passive storage devices, although even in this case the large volume of data may itself become a problem. However, as mentioned above, there is a growing trend of using USB flash drives as active devices which carry portable applications and full user environments. This trend is growing because of continuously increasing capacity and dropping prices of the USB flash drives, and easy access to USB equipped computers. We propose a different method which is more suitable to analyse this dynamic environment, that still retains the full integrity of the original image. The method benefits from using a virtual machine environment, as detailed below.

IV. A Brief Overview of Virtual Machines

Virtualization is an abstraction layer that decouples the physical hardware from the operating system [2]. Virtual machine (also known as ‘VM’) is software which runs in a host machine environment and creates separate, independent environments each simulating its own set of hardware and software. Virtualization technology is, by computing standards, a very old concept which was first time proposed in the late 1950s [17]. A series of implementations followed with IBM announcing the first successful commercial product (VM - Virtual Machine operating system) in 1972 [18].

Virtualisation is a powerful tool which could be used for many tasks, but it requires additional computing resources. In addition to running a host operating system the computer shares the same set of hardware components between virtual machines, and obviously this need for resources increases if we run more virtual machines on a single host at the same time. Most implementations do not place any specific restrictions on how many virtual machines can be active at the same time. The only practical restriction is the availability of resources, and one can easily run dozens of virtual machines on one host at the same time. Typically a well designed virtual machine has intelligent and complex resources management capabilities. For example memory management in VMWare products are shared dynamically, as required, between virtual machines and real hardware host system space [19]. This extra level of address translation creates complex mapping of real hardware to virtual hardware, but is necessary to provide each virtual machine with an illusion of having full access to the allocated memory range. Practical conclusions for a computer which is to be used to run a virtual environment are as follows: use as much memory as the hardware can accept (typically 3-4GB for a Windows based host computer), consider using two or more CD/DVD burners to allow the virtual machine exclusive access to one CD/DVD burner, and use a very fast CPU.

Conceptual complexity of virtualisation leads to certain compromises and restrictions, some of them (as we explain later) especially relevant in forensic applications. Only very

recently the unique advantages of virtualisation were noticed by professionals in relation to computer forensics.

There are many free and commercial VM products offering different levels of maturity and flexibility, some of the best known are Microsoft Virtual PC [20], the extensive VMWare range of products [2], XenSource range of Xen products [21], and the open source (free) software QEMU [22]. Surprisingly all commercial developers offer selected virtualization software free, thus encouraging further experiments. However it should be remembered that some utilities are the result of the work of a small, dedicated group of hobbyists [23], and while the results achieved are often spectacular, such tools may not be sufficiently stable and tested to be used in forensic investigations. Some restrictions worth noticing here are that options of mixing host and guest systems may be restricted in a specific environment. Hardware configurations emulated by a guest system are limited to only the most common components, for example only one type of video card or one type of Ethernet controller. This may severely restrict use of VM in certain applications, but is of no consequence in USB key image analysis as presented here.

V. Analysing USB Flash Drive Contents in Virtual Machine environment

To describe the proposed approach we introduce two levels of computer forensics personnel; "less experienced" and "more experienced". Depending on the organization involved those descriptive terms will translate to specific titles; here we will be referring to them respectively as 'Computer Technician' and 'Professional Investigator'. This is similar to the roles CNF Technician (Computer and Network Forensic Technician) and CNF Professional (Computer and Network Forensic Professional) in classification proposed by Yasiniac et al [24]. *It should be stressed that this classification, the terms used, and allocation of tasks vary between organisations and countries, and may have different titles such as 'Junior Investigative Officer', 'Digital Forensic Analyst', 'Senior Forensic Analyst', and so on.*

The modus operandi of a team consisting of a Professional Investigator and a Computer Technician is as follows:

- The fully trained and more experienced Professional Investigator adheres strictly to computer forensics investigation methods.
- The less qualified Computer Technician does not have to strictly follow forensic rules, and never has any direct input to the formal reporting process. The Computer Technician checks the copy of the materials for anything of potential interest, and then reports the findings to the Professional Investigator.

A person conducting the final, formal analysis and presenting the report in the court is considered to be an expert [25] who possesses relevant specialised knowledge. We proposed [1] that the the whole process can be faster, more efficient and more reliable if two parallel investigating streams are used as shown in figure 1.

In the analysis phase of the computer forensics investigation a master copy of the acquired USB flash drive image is kept

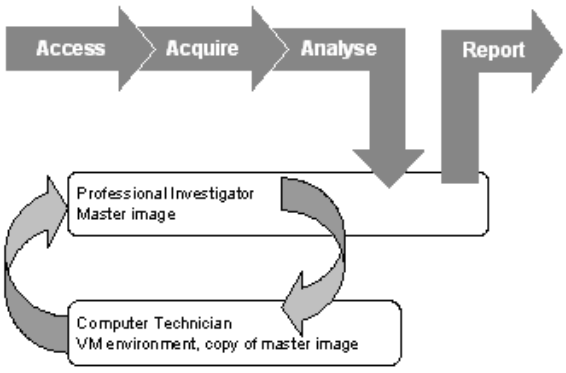

Fig. 1. Using virtual environment in analysing USB flash drive image

by the Professional Investigator, who provides another copy to the Computer Technician. The Computer Technician uses a virtual machine environment to mount the image under an appropriate Virtual Machine (typically Windows XP) and to find all data relevant to the investigation. If at any time the Technician decides that the image has been changed by the procedure he used, he may request another copy of the master image from the Professional Investigator. Typically this should not be required, as the procedure recommended for the Technican to follow would be to duplicate and save the image, or alternatively to save the complete virtual machine which includes a mounted image of the acquired USB flash drive.

The methodology used by the Computer Technician invalidates the integrity of the acquired image, as he can use any suitable tools or methods even if they are not forensically sound. This is of no consequence to the validity of the final report. The Computer Technician makes detailed notes, and communicates all findings to the Professional Investigator, who uses proper computer forensics techniques and tools to confirm all initial findings in a formally approved way. It is crucial to note that no findings of the Computer Technician are included directly in the reporting process. The final report is created by the Professional Investigator, and it is the result of conducting a proper forensic analysis and using the original image.

Next we will use a simple example scenario to demonstrate that the methodology described above can deliver more accurate results faster.

VI. The Example Scenario

A USB flash drive was found as part of a larger investigation. A computer forensics investigator was requested to check the USB flash drive and to find all information pertaining to drug trafficking, including details of financial transactions and any relevant letters or documents.

The investigator documented physical details of the USB flash drive including make and model number, write protected the drive, and acquired the drive image using AccessData FTK Imager [26]. In addition to creating the dd image of the drive, FTK Imager also created a record (see Figure 2) which describes the USB drive geometry, physical drive information, and computed MD5 and SHA1 hashes of the image and the

```
Information for C:\__USB paper\USB27:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Cylinders: 15
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 256,000
[Physical Drive Information]
 Drive Model: KINGMAX USB Flash Disk USB Device
 Drive Interface Type: USB
 Source data size: 125 MB
 Sector count:    256000
[Computed Hashes]
 MD5 checksum:    a40aabec0cdc266e9ad304184a2346b5
 SHA1 checksum:   d31ad8924837eb99e297470968fa94c1012b671a

Image Information:
 Segment list:
  C:\__USB paper\USB27.dd

Mon Feb 26 19:52:00 2007 - Image Verification Results:
 MD5 checksum:    a40aabec0cdc266e9ad304184a2346b5 : verified
 SHA1 checksum:   d31ad8924837eb99e297470968fa94c1012b671a : verified
```

Fig. 2. Acquiring USB flash drive image, FTK Imager report

```
C:\VMBack>vdk install
Virtual Disk Driver for Windows version 3.1
http://chitchat.at.infoseek.co.jp/vmware/

The Virtual Disk Driver is already installed.

C:\VMBack>vdk start
Virtual Disk Driver for Windows version 3.1
http://chitchat.at.infoseek.co.jp/vmware/

Started the Virtual Disk Driver.

C:\VMBack>vdk open 1 c:\_USBimages\USB27.dd /rw
Virtual Disk Driver for Windows version 3.1
http://chitchat.at.infoseek.co.jp/vmware/

Failed to decide type of 'c:\_USBimages\USB27.dd'.
Open as a simple sector image file.
Virtual Disk 1
Access Type     : Writable
Disk Capacity   : 256000 sectors (125 MB)
Geometry        : (C) 125 * (H) 64 * (S) 32
Number Of Files : 1

  Type     Size    Path
 ------   ------  ----
  FLAT    256000  c:\_USBimages\USB27.dd

Partitions      :
     #   Start Sector    Length in sectors    Type
    --   ------------   --------------------  ----
     0              0     256000 (   125 MB)  (disk)
 E:  1             32     255967 (   124 MB)  0Bh:FAT32

C:\VMBack>
```

Fig. 3. The Virtual Disk Driver in VMWare guest machine

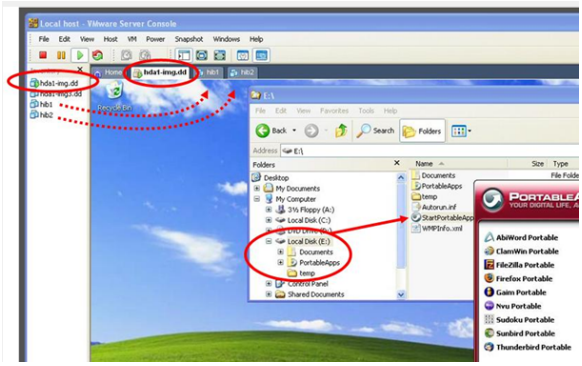

Fig. 4. VMWare running master Windows XP guest and USB image mounted as a drive

original drive, verifying their match. The chain of custody was created according to local forensic procedures [27].

Two copies of the image USB27.dd were given to two people in the forensic lab: the Professional Investigator, and the Computer Technician. Both updated the respective chain of custody records and physically secured the image by locking it in a safe place. The Computer Technician was asked to investigate the image in a virtual environment (see Figure 1), and to use any suitable tools to search the image for any materials which may be relevant to the investigations.

VMWare Server [3], a free virtualisation product from VMWare, was installed on a separate computer, and a Windows XP SP2 guest virtual machine was installed under VM [1]. After booting the Windows XP VM guest the USB flash drive image was copied to the virtual machine. However the USB flash drive image was in dd format, and thus it would only be of use if proper forensics tools and methods were used. There are a few different ways to use a dd image in a Windows environment in such a way that Windows treats the image as a disk drive. Still inside the guest virtual machine, the Computer Technician used VDK virtual driver [28] which mounted the USB27.dd image as a separate drive E: - see Figure 3.

At this stage it is interesting to compare Figure 2 and Figure 3, and to notice that the virtual disk driver mounted the USB27.dd image as a FAT32 drive with 125 cylinders, 64 heads and 32 sectors per track, totalling 256 000 sectors. FTK Image logged the geometry differently (see Figure 3) as follows: 15 cylinders, 255 tracks per cylinder, 63 sectors per track, 512 bytes per sector, giving a total sector count of 256,000.

This difference is not unusual; the virtual machine automatically emulates real drive geometry and it may use a different virtual drive configuration. An important confirmation of the validity of the process is that the sector size and the total sector count are identical, in this case 512 bytes per sector and 256,000 sectors.

When browsing the contents of the E: drive with Windows Explorer the Computer Technician noticed a file named StartPortableApps.exe in the root directory. When the file was executed, it started the PortableApps application, see Figure 4.

Looking at the environment built by the Computer Technician we notice the following (numbers refer to Figure 5):

1) Windows XP system running on the host PC used for testing of the image.
2) VMWare virtual environment running.
3) Four virtual machines are configured, and three are running, namely: hd1, hd2 and hda1-img.dd.
4) Desktop of the virtual guest named hda1-img.dd running Windows XP.
5) Acquired USB flash drive dd image mounted as a separate hard drive E: inside the virtual machine with a menu showing installed applications.
6) PortableApps panel also shows drive letter 'E:', as well as the amount of total and free space on the virtual USB drive E:.

The Computer Technician checked applications installed on PortableApps, browsed the contents of the E: drive, and

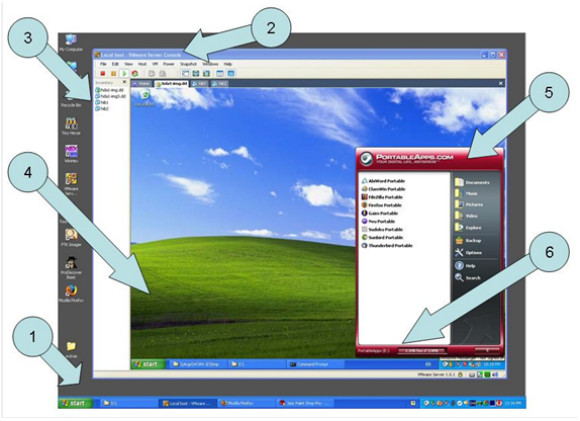

Fig. 5. Virtual environment: Windows XP VMWare host and Windows XP guest

continued the examination using standard Windows tools. The Computer Technician discovered a series of folders containing documents relevant to the investigation: letters, emails, spreadsheets and records of transactions. When Portable Firefox was started one of the links pointed to the online storage system Mozy [29]. As the user of the USB key decided to use the Mozy log on panel option 'remember my details on this computer'. The Computer Technician extracted the Mozy account user name and password using a password revealing tool [1].

Two important points are worth noting here:

1) The E: disk in the virtual machine is no longer identical with the image USB27.dd acquired from the USB storage device using forensically sound methods. The Computer Technician started the PortableApps application installed on the E: disk - various files and folders were 'touched' by checking them in Windows Explorer, and by opening them in their native applications. It would be unrealistic to argue that the image is still valid as evidence, as it is now clearly contaminated.
2) The originally acquired image USB27.dd is still kept in custody by the Professional Investigator; it is unchanged and forensically valid.

The Computer Technician reported the result obtained in the virtual environment to the Professional Investigator who can now confirm all the findings using forensically sound methodology, proper forensics software tools, and the original image USB27.dd.

VII. Conclusion

We described the process of using conventional and virtual environments in computer forensics investigations of USB flash drives. This approach is particularly suitable and brings faster results in cases when a USB flash drive is used not just to store data, but to contain a full set of portable applications, and used as an independent, fully self contained environment. We demonstrated a possible approach where virtual machine is used to quickly and efficiently recreate the original dynamic environment.

To illustrate the concept we presented a relatively simple scenario where a single USB flash drive containing an independent PortableApps environment was analysed. The method of conventional and virtual environments used in parallel made it fast and simple to see the original environment as it was seen by the last user of the USB key, to still retain the integrity of the original image and giving the ability to confirm all findings using conventional forensics methods. The scenario demonstrated that the cooperation between two teams with different levels of expertise can produce more thorough results faster, and will lessen the workload of a Professional Investigator, who is a highly qualified specialist, and ideally should be involved only in resolving complex issues. The Professional Investigator would most likely achieve the same results using a conventional approach; however the described method saves time and increases the chances of finding important evidence. An additional advantage of using a dual conventional/virtual setup is involving less experienced technical personnel in a real investigation with no risk of compromising the integrity of the evidence.

We believe that more research is needed to formalise the process of using a parallel conventional/virtual environment. Future research is also required to more thoroughly test other available virtual environment software. We believe that some of those tools may be more suitable to analyse USB devices, and thus may speed up the process. Also, some virtual machines may provide more accurate emulation of a wider range of hardware. Currently the hardware emulated by VM software is limited to very few devices. At this stage no such overview of utilities exists. It is also important to survey and test peculiarities of available portable applications and systems to better understand their behaviour in a virtual environment. Finally it is necessary to conduct more experiments with a growing range of large capacity USB storage hardware and document the peculiarities of various scenarios and devices.

References

[1] D. Bem and E. Huebner, Computer Forensic Analysis in a Virtual Environment: University of Western Sydney. University of Western Sydney, 2007.
[2] VMWare, "VMWare," 2007; http://www.vmware.com/
[3] VMWare Server, "VMWare Server," 2007; http://www.vmware.com/products/server/
[4] B. Shavers, "VMWare as a Forensic Tool," 2006; http://www.forensicfocus.com/vmware-forensic-tool
[5] W.G. Kruse II and J.G. Heiser, Computer Forensics: Incident Response Essentials, 1st ed. Addison-Wesley Professional, 2002.
[6] K. Mandia, C. Prosie and M. Pepe, Incident Response & Computer Forensics, 2nd ed. Emeryville, CA: McGraw-Hill/Osborne, 2003.
[7] Buslink Media, 2007; http://www.buslink.com/B1/index.asp
[8] Kanguru Solutions, 2007; http://www.kanguru.com/
[9] M.E. Russinovich and D.A. Solomon, Microsoft Windows Internals. Redmond: Microsoft Press, 2005.
[10] Montage, 2007; http://www.ideaxchg.com/montage/portability.htm
[11] U3, 2007; http://www.u3.com/default.aspx
[12] PortableApps, 2006; http://portableapps.com/
[13] C.L.T. Brown, Computer Evidence: Collection & Preservation. Hingham, MA: Charles River Media, 2005.
[14] B. Nelson, A. Phillips, F. Enfinger and C. Steuart, Guide to Computer Forensics and Investigations, 2nd ed. Boston, MA: Thomson Course Technology, 2006.
[15] B. Carrier, File System Forensic Analysis, 1st ed. Upper Saddle River, NJ: Addison-Wesley, 2005.

[16] S. Bunting and W. Wei, EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide, 1st ed. Indianapolis, IN: Wiley Publishing, 2006.
[17] L. Chao, Intel Virtualization Technology, Vol. 10 Issue 3. Intel technology Journal, 2006.
[18] VM History and Heritage, 2007; http://www.vm.ibm.com/history/
[19] C. Waldspurger, Memory Resource Management in VMware ESX Server:Paper presented at the Fifth Symposium on Operating Systems Design and Implementation (OSDI '02). Boston, Massachusetts: 2002.
[20] Microsoft, "Microsoft Virtual PC 2007," 2007; http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx
[21] XenSource, 2007; http://www.xensource.com/
[22] F. Bellard, "QEMU," 2007; http://fabrice.bellard.free.fr/qemu/index.html
[23] SourceForge.net, "Bochs IA-32 Emulator," 2007; http://bochs.sourceforge.net/
[24] A. Yasinsac, R.F. Erbacher, D.G. Marks, M.M. Pollitt and P.M. Sommer, "Computer Forensics Education," IEEE Security and Privacy, Volume 1 Issue 4, 2003, pp. 15-23.
[25] M. Meyers and M. Rogers, Computer Forensics: The Need for Standardization and Certification, Vol. 3 Issue 2. International Journal of Digital Evidence, 2004.
[26] AccessData, "FTK Imager," 2006; http://www.accessdata.com/common/pagedetail.aspx?PageCode=downloads
[27] S.V. Hart, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," April 2004; http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm
[28] VM Back, "Virtual Disk Driver," 2005; http://chitchat.at.infoseek.co.jp/vmware/vdk.html
[29] Mozy, 2007; http://mozy.com/

Derek Bem Derek is a Lecturer in the School of Computing and Mathematics at the University of Western Sydney, Australia. Derek has extensive experience in the computer industry, where he worked in IBM and other companies as a hardware and software engineer. Derek is currently coordinating UWS teaching in the Computer Forensics area.

Ewa Huebner Ewa is a Senior Lecturer in the School of Computing and Mathematics at the University of Western Sydney, Australia. Ewa has extensive experience teaching computer science subjects, and she is currently leading the UWS Computer Forensics group. The UWS computer forensics web site can be found at http://www.scm.uws.edu.au/compsci/computerforensics/