2008

The Impact of U3 Devices on Forensic Analysis

R. Tank
Edith Cowan University

Patricia A.H. Williams
Edith Cowan University

Originally published in the Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

The Impact of U3 Devices on Forensic Analysis

R. Tank and P.A.H Williams

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia

Abstract

Flash and USB portable drives are now in common place use in computing environments. The U3 smart drive is one emerging type of enhanced flash drive. It is believed that U3 smart drive devices do not leave any record or evidence on a host PC after use. Therefore, it is conceivable that it could be used in a digital crime or attack on a computer or networked system. In circumstances where a portable device such as a U3 has been used, it is more complex for a forensic analyst to find evidence of its use. This paper discusses the impact of U3 smart drive devices on a forensic investigation. Further, it describes the forensic investigation undertaken of a computer in which U3 was used.

Keywords: U3, U3 smart technology, computer forensics, forensic investigation, forensic tools.

INTRODUCTION

Computer forensics broadly consists of identification, acquisition, analysis and reporting (Williams, 2008). It focuses on gathering digital evidence from devices such as computers and networks. Evidence may include files, image or the traces of a user's activities. Data on activity is often left in activity logs of operating systems, browsers, databases, web proxies, or network firewalls and so on. The discipline of digital forensics requires a detailed technical knowledge of the relationship between a computer's operating system and the supporting hardware, and between the operating system and system/application programs and the network. Finally, all evidence gathering must precede in a manner that ensures that the evidence is admissible in a court of law, and can be documented and presented in an intelligible manner (Carrier, 2005). It is against this background that the following research was undertaken to find what digital evidence could be retrieved from the new U3 smart drive technology.

The U3 smart drive is an enhanced type of flash drive. The U3 was developed by SanDisk and M-Systems and using an open-platform, allows data and programs to be transferred easily. Essentially, it is a method to auto-launch applications using a portable, removable drive (Everythingusb, 2005). The U3 smart drive is different from the normal flash drive because it comes with preinstalled programs, system files and a U3 launch pad. The U3 launch pad is what makes the U3 device unique, as it is a pre-installed auto-run program manager similar in look to the XP start menu. This automation is achievable because a small partition of the U3 drive mimics a CD-ROM drive whilst the second partition is a normal USB data partition. When attached to a Windows system it is immediately recognised as CD and thus the auto-play feature is enabled on the Windows platform. In addition, U3 devices can be password protected so when plugged in, the users is prompted for a password and then only can access the applications or data from the U3 smart drive (U3, 2008).

When a U3 smart drive is plugged into a host PC it uses the host to record information about the U3 and the programs it runs. However, when the U3 device is ejected from the host computer it runs a program called 'Cleanup.exe' to clean the evidence of the U3 device usage on the host computer. It is promoted by the manufacturer that the U3 smart drive does not leave any residual information or records on to the host PC after it is ejected and the cleaning program has run: "nothing is installed from the U3 smart drive to the PC you are using" and when you remove the U3 smart drive "will put the PC you are using back into the state it was in before you plugged in the U3 smart drive. No personal data or files related the applications you were running are left behind. Everything is cleaned up for you automatically" (Demo clip) (U3, 2008). This misconception has been propagated further by discussion of the technology in the media (Lasky, 2007; Wighting and Christmann, 2006) This facility can be seen as an advantage of the U3 smart drive and because of this advantage, may be favoured for use in digital crimes. For instance a U3 could be used to install software such as malware into a system or network to compromise a host PC. In this situation it is very difficult for a forensic investigator to find evidence of potential crime (Everythingusb, 2005). This research investigates these claims.

U3 TECHNOLOGY

U3 technology is a technology which allows a user to install and remove their own applications on the device as well as keeping data on the device. U3 technology provides the portability for a user to take data and applications with them and place them on any computer system without copyright issues. It provide the facility to utilise a PC and mimic the users' own PC by plugging in the U3 enabled device and using the applications and data installed on it. The U3 technology allows applications to write files or registry information to the host computer whilst also having the facility to removes evidence once it is ejected and removed from the computer. Essentially, leaving the computer as it was prior to the U3 being attached.

A U3 smart drive has two detectable parts to it, as shown in Figure 1.

- The first part is as a CDRom. The U3 file system which contain the necessary files to run U3 applications and system files that are read only are shown as part of the CDRom. Actually, the CDRom part of a U3 device is an ISO image, with the extension .ISO which is a standard CDROM file types, and it contains the auto run file for U3. When U3 is plugged in, the auto-run file runs and launch the U3 launch pad which is similar to Windows start menu.
- The second part of U3 device is a storage device where user can keep all the data as well as the all installed program in U3. This is shown as a removable disk.

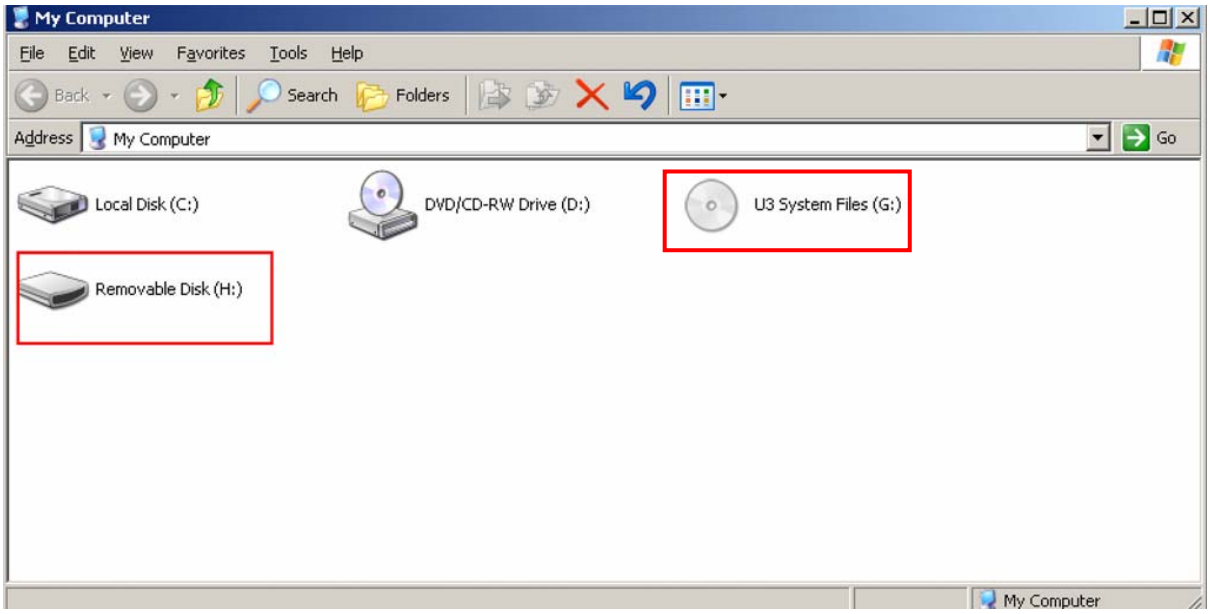

Figure 1: U3 devices detected by an operating system.

When the U3 device is plugged into a PC, the resulting entries can be found in the Windows registry consistent with the apparent detection of two devices by the operating system.

- The hardware id of the CDRom (G:) which can be located in registry is:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\CdRom&Ven_Memorex&Prod_Mini_TravelDrive&Rev_6.50\0CF0C86102B0990B&1
- The hardware id of the storage device (H:) which can be located in the registry is:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Memorex&Prod_Mini_TravelDrive&Rev_6.50\0CF0C86102B0990B&0

PROCEDURE

This research used the hardware, software and procedures described below to investigate a U3 device. This investigation is similar in nature to that proposed by Spruil and Pavan (2007).

Preparation

The hardware and software used in this investigation were:

- PC with Intel P4 2.4 GHZ

- Gigabyte GA 8IG1000MK mother board
- Sandisk cruzer BI0805KCIB U3 smart drive 4GB
- WD 140 GB portable hard drive
- Windows XP SP2
- Access Data FTK Imager Version 2.1a
- Autopsy Forensic Browser
- Helix Linux 1.9

Prior to analysing the residual information the following steps were undertaken to prepare the U3 device and create known application usage from the U3 device.

1. A fresh copy of Windows XP SP2 with the default drivers was loaded onto a PC.
2. Using a separate PC, a new U3 smart drive was plugged in and software for the U3 was downloaded directly to the device from the U3 official website. The software downloaded included Fire Fox, Open Office etc. This software is free to download and use on the U3 device.
3. The U3 smart drive was plugged into the newly loaded computer installed with XP SP2 (from step 1).
4. Open Office was opened directly from U3 smart drive and a file created and saved onto U3 drive only.
5. Next, Fire Fox was opened and an image downloaded from internet directly to the U3 flash drive.
6. Next, an email account was opened using Fire Fox on the U3 and an email sent to another email account.
7. Lastly, the U3 flash drive was ejected.

Post Procedure and Analysis
Following the preparation, the following procedure was followed for data acquisition and analysis:

- Using a Helix CD, the PC hard disk was imaged and a hash value calculated for this image.
- A copy of the image was made (and an additional copy of the copy) and the hash values re-calculated and compared to ensure they were identical.
- Using a copy of the image, the residual information from the U3 usage was investigated, to see what data was left behind on the image.
    - Initially Autopsy was used to analyse the image, however a cursory search for the known .jpg file could not find any trace and it was decided not to pursue the investigation using the Autopsy software.
    - Next, FTK Imager Version 2 was used to analyse the image, with appropriate hash values calculated at each step.
    - The investigation looked for time line information, user account and other information.
    - A list of the findings was made and hash values re-calculated and compared.

RESULTS
Using the FTK Imager, the PC investigated and the following results obtained.

Post cleanup analysis
When the U3 drive was plugged into the PC it created a folder called U3 in the currently logged on users' directory. In this case the pathname was

Root/Document and settings/RAV (*User Name)/*Application data/U3

This folder holds an entry for each and every application run from the U3 device and thus logs user activity. Subsequently, when the U3 is ejected, the process automatically invokes a program called cleanup.exe to clean the entries from the host PC. However, after ejection of the U3 device, the files "cleanup.exe" and "Launch pad Removal.exe" remain on the host PC in a subfolder called 'temp' in the U3 folder, as shown in Figure 2. The path of the file and temp folder is

Root/document and setting/RAV (User Name)/Application data/U3/Temp/Cleanup.exe
Root/document and setting/RAV (User Name)/Application data/U3/Temp/Launch pad Removal.exe

It is therefore possible to ascertain that the U3 device has indeed been used on the host PC and the date and time the cleanup programs were executed.

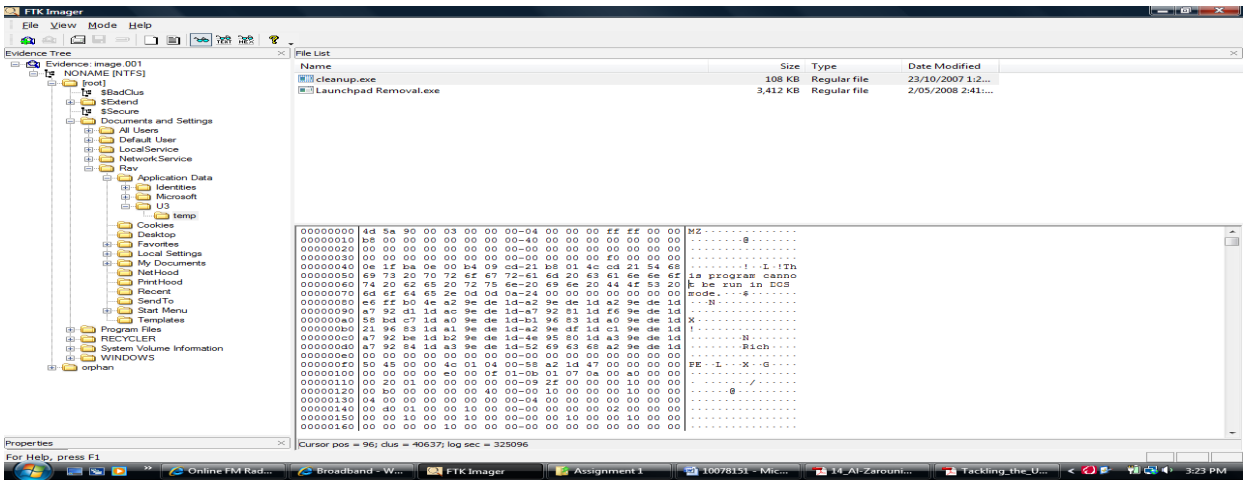

Figure 2: cleanup.exe and launch pad removal.exe

'Recent' folder data

Other information discovered which can be considered for evidence was found in the folder called 'Recent' under the current users' folder. The path of that folder was:

Root/document and settings/RAV (user name)/Recent

As the U3 file system is linked with the Windows file system and therefore relies on the Windows built-in explorer option, it creates a link for each file accessed using the U3 in the 'Recent' folder, as shown in Figure 3. The 'Recent' folder has an entry of all files using the file extension .LNK. With the help of this information it is possible to build up a picture of what activities were carried out involving the U3 device. As previously, the date and time of execution or file modification is recorded.

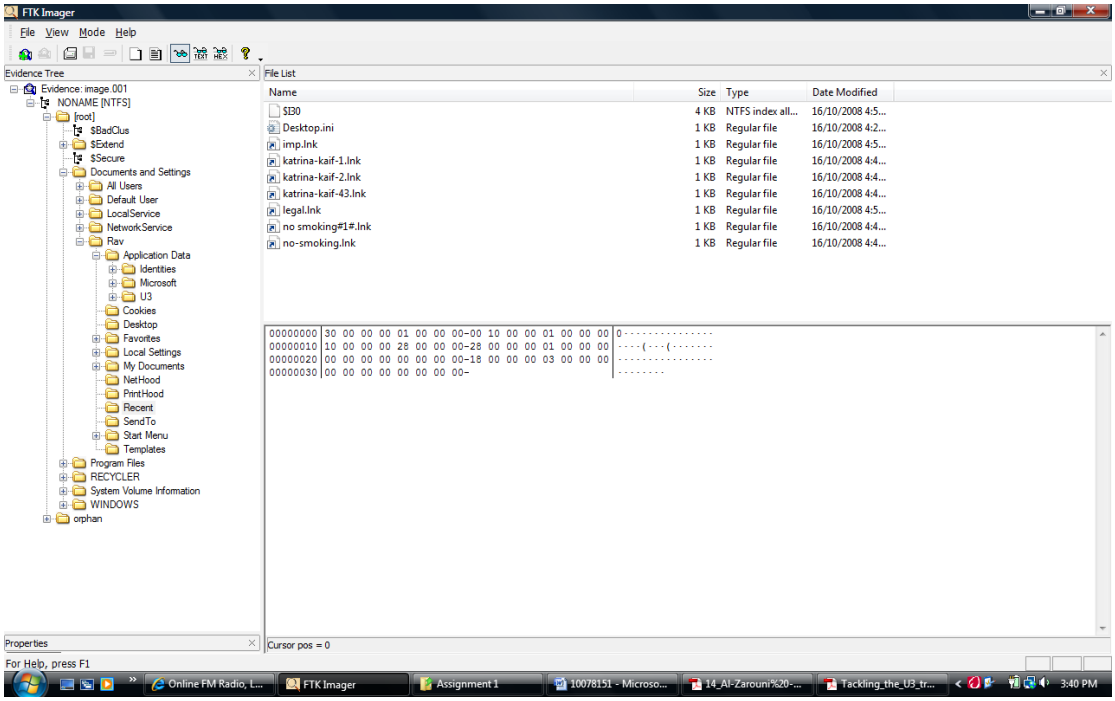

Figure 3: Recent folder

When analysing each link file dump, it can be seen that the information about the file modified. E.g. the file name Katrina-kaif-1.lnk contains information that the actual file accessed is Katrina-kaif-1.jpg and it also has been saved to the drive called G:, and which folder it was saved to, in this case under the folder 'Legal', together with the date and time. For each .LNK file it shows the particular information about the file. This information may be very useful to a forensic investigation.

PREFETCH persistent data

In addition, the Windows PREFETCH folder could be analysed. This folder stores the PREFETCH files, which are created by Windows to enhance the speed of the system. PREFETCH file are with .PF format. Windows records every activity of the computer in the PREFETCH folder which is located at the path

Root/Windows/PREFETCH

Figure 4 indicates that the PREFETCH folder shows the activities/programs run on the computer, with the date and time modified. If any application runs from the computer it creates the file of the format '*application name*.pf', with file size, disk type and date and time the file was opened or the application executed. This information can be used to create a timeline and indicates what activities were undertaken or files accessed from the computer.

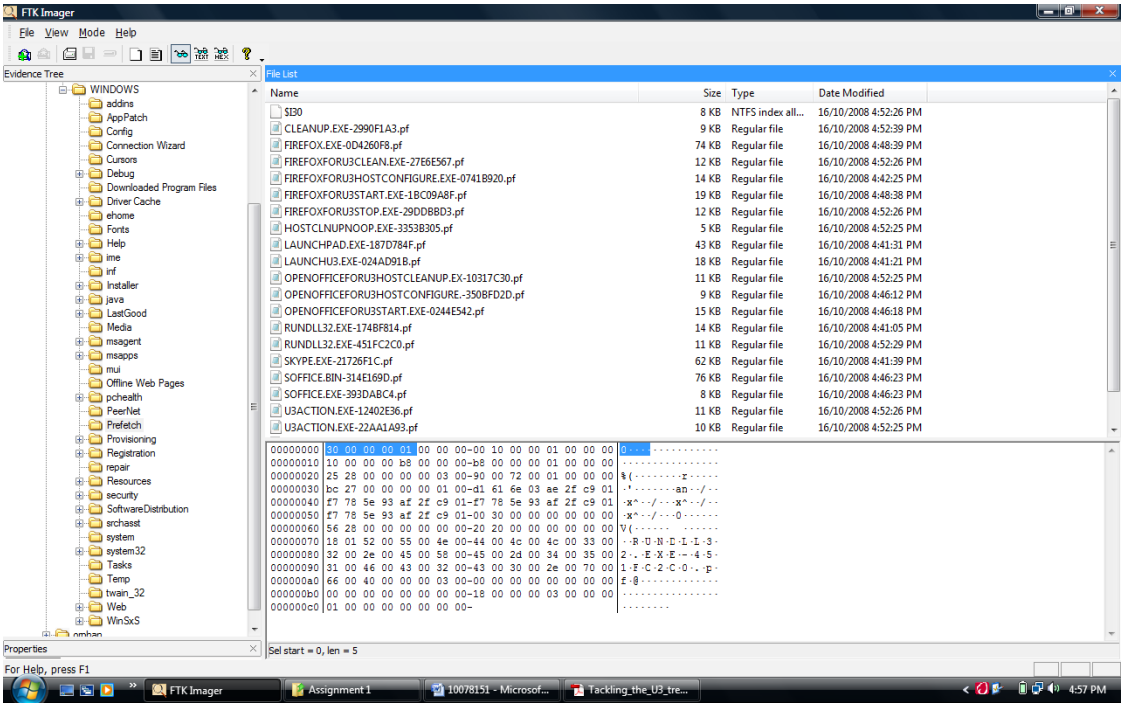

Figure 4: Windows PREFETCH

Figure 4 shows that the program entries include (in most recent first order):

- Cleanup.exe-2990F1a3.pf
- Firefox.exe-0D4260F8.pf
- FirefoxforU3hostconfigure.exe-0741B920.pf
- FirefoxforU3stop.exe-29DDBBD3.pf
- Launchpad.exe-187D784F.pf
- OpenofficeforU3hostcleanup.ex-103117C30.pf
- Skype.exe-21726F1C.pf
- U3action.exe-12402E36

From these entries it is possible to ascertain that a U3 device has been plugged into the computer and which applications like Skype, Open Office, Firefox was accessed from the U3 drive.

In addition, other information was located in the 'textconv' file, located at:
Root/Program files/common files/Microsoft shared/TEXTCONV

DISCUSSION

The collection of evidence to prove organisational misconduct or criminal activity is crucial to successful prosecution. As the U3 smart drive becomes a more commonly used device the opportunity for digital crime increases with such devices since software can easily be installed on the device and it is highly portable. Tracking the use of portable devices is a security issue that organisations face day-to-day and therefore the use of such devices for malicious or criminal activity pose even larger problems in detection. Since it is believed that these devices are undetectable after usage is incorrect. Therefore, this finding has positive implications for organisational security where detection of portable devices is problematic.

From a forensic investigation perspective, another important aspect is that at present U3 is very new technology and therefore few tools and procedures for forensic investigation exist specifically for this device. This initial research indicates that there is some forensic trace of U3 usage left on the host computer. This provides a starting point for further forensic investigation of a computer if it is believed that a crime has been enacted involving a U3 smart drive.

The results obtained are in three basic categories:

- Cleanup files:
  - The two files Cleanup.exe and Launch pad removal.exe this both can be find , which proves that the U3 smart drive has been used in the computer.
- Recent Folder:
  - In the recent folder all the .lnk files can be find so this helps in to find that what files has been accessed in this computer.
- PREFETCH Folder:
  - From PREFETCH folder the list of all activity can be find.

From these investigations it may be possible for a forensic investigator to create a timeline and produce activity evidence which may be useful in a court of law. The three sections covering cleanup, the Recent folder and the Prefetch folder, indicate that a U3 device has been used and when. Further, it shows what software or application has been run from the U3 smart drive, and at what time and what files has been created or modified or saved to U3 drive. This information may assist in forensic investigations or U3 and other similar devices using the same or technology.

CONCLUSION

The U3 smart drive is a powerful transportable device for a user to keep applications and data. However, this test found that it is an erroneous assumption that it does not leave any trace on the host PC after it is used. There is potentially useful evidence which can be located on the host PC after use of a U3 smart drive, as this paper demonstrates. Record of U3 usage, if left uncleansed, can provide evidence of all applications run. Further, it provides links to the names of files accessed although not to the actually contents of these file.

Further research needs to be undertaken in regard to the cleanup.exe program itself, to identify if other useful evidence can be located. This would include the exacted files created or modified with the use of the U3 smart drive applications, or user installed applications. If security and system administrators are to protect their systems with the advent of new technologies such as smart drives, then finding methods to detect the use of such technology and collect forensic evidence to prove its use, is essential.

REFERENCES

Al-Zarouni, M., & Al-Hajri, H. (2007). A Proof of concept project for utilizing U3 technology in incicent response. In C. Valli and A. Woodward (Eds.), *Proceedings of the 5th Australian Digital Forensic Conference*, School of Computer and Information Science, Edith Cowan University, Perth, WA.

Carrier, B. (2005). *File system forensic analysis*. Upper Saddle River, NJ: Addison-Wesley

Everythingusb. (2005) *U3 - 'Official' Portable USB Apps Platform.* Retrieved October 3, 2008, from http://www.everythingusb.com/u3.html.

Forensicfocus. (n.d.). *U3 capable USB.* Retrieved October 7, 2008, from http://www.forensicfocus.com/index.php?name=Forums&file=viewtopic&t=1225.

ForensicsComputer. (n.d.). Retrieved September 26, 2008 from http://computer-forensics.safemode.org/index.php.

Lasky, M.S. (2007). Painless backup to USB drives. *PC World* 25(10), 140.

Mckinnon, M. (2007). *Computer Forensics/E-Discovery Tips/Tricks and Information.* Retrieved September 26, 2008, from http://cfed-ttf.blogspot.com/.

Microsoft. (2006). *U3 USB drives.* Retrieved October 8, 2008, from http://forums.microsoft.com/MSDN/ShowPost.aspx?PostID=942660&SiteID=1.

Nirsoft. (2003). *IEHistoryView v1.37 - View Visited Web Sites of Internet Explorer.* Retrieved October 14, 2008, from http://www.nirsoft.net/utils/iehv.html.

Searchenterprisedektop. (2005). *Empty the prefetch folder.* Retrieved September 26, 2008, from http://searchenterprisedesktop.techtarget.com/tip/0,289483,sid192_gci1088757,00.html.

Spruil, A. & Pavan, C. (2007). Tackling the U3 trend with computer forensics. Digital Investigation 4(1), 7-12.
U3. (2008). *Homepage*.. Retrieved September 19, 2008, from http://www.u3.com/default.aspx.
U3devforum. (2006). *U3 Deployment Kit.* Retrieved September 23, 2008, from www.u3devforum.com/claudio/U3_Deployment_Kit_081406.pdf.
Williams, P. A. H. (2008). Is there an ideal forensic process? In H.R. Arabnia, S. Aissi & M. Bedworth (Eds.) *Proceedings of the 2008 World Congress in Computer Science, (2nd ed)* Computer Engineering, and Applied Computing - SAM'08 - The 2008 International Conference on Security & Management, (pp. TBA). USA: CSREA Press.
Wighting , M. J. & Christmann, E.P. (2006). The Size of Things to Come.(LaCie Brick, portable hard drive). *Science Scope* (Dec), 72-73.

COPYRIGHT