The Impact of Full Disk Encryption on Digital Forensics

Eoghan Casey, Director of Training,
Gerasimos J. Stellatos, Digital Forensic Examiner
Stroz Friedberg, LLC
1150 Connecticut Ave, NW
Washington, DC 20036
202-464-5800
{ecasey, gstellatos}@strozllc.com

ABSTRACT
The integration of strong encryption into operating systems is creating challenges for forensic examiners, potentially preventing us from recovering any digital evidence from a computer. Because strong encryption cannot be circumvented without a key or passphrase, forensic examiners may not be able to access data after a computer is shut down, and must decide whether to perform a live forensic acquisition. In addition, with encryption becoming integrated into the operating system, in some cases, virtualization is the most effective approach to performing a forensic examination of a system with FDE. This paper presents the evolution of full disk encryption (FDE) and its impact on digital forensics. Furthermore, by demonstrating how full disk encryption has been dealt with in past investigations, this paper provides forensics examiners with practical techniques for recovering evidence that would otherwise be inaccessible.

Keywords
Full Disk Encryption, Computer Forensics, Live Forensic Acquisition, Virtual Forensic Analysis

1. INTRODUCTION
Healthcare and financial organizations, government entities, and higher education institutions have all experienced loss or theft of hard drives containing personally identifiable information (PII). In May 2007, the Transportation Security Administration (TSA) lost a hard drive containing approximately 100,000 employee bank account details, and in October 2007 two laptops containing names and social security numbers of almost 4,000 employees were stolen from the TSA [1]. In November 2007, the government in the United Kingdom reported that two disks containing personal information details of 25 million citizens had been lost [2]. The liability risks associated with exposure of PII, along with increased media and consumer scrutiny has compelled organizations to improve their data security procedures by implementing solutions to encrypt data at rest.

Encryption is one of the strongest protection measures against unauthorized access to data. The need for securing data on hard drives has led to an increase in the use of strong encryption. Until recently, forensic examiners could recover digital evidence from computers despite the use of encryption. However, the integration of encryption into operating systems, specifically full disk encryption (FDE), is making recovery of digital evidence more difficult. Today, a forensics examiner may encounter a full disk encryption interface prior to the machine booting, preventing access to any data unless the necessary credentials are supplied. If these credentials are not available, forensic examiners may have to acquire a forensic image of a live system while the contents are in an unencrypted state.

In a recent case, the US Customs observed possible child pornography on Sebastien Boucher's laptop but did not realize that it was stored in a Pretty Good Privacy (PGP) encrypted container that was open and assigned drive letter "Z" at the time of the inspection. The laptop was shutdown and a forensic duplicate of the hard drive was created, but forensic examiners could not open the PGP encrypted container. A Grand Jury Subpoena to compel Boucher to provide his password for decrypting the data was denied on the grounds that it violated his Fifth Amendment right against self-incrimination [3].

Even when the encryption key and associated passphrase are available, it may be necessary to employ novel approaches to forensic acquisition and analysis. This paper describes the use of encryption on storage media and approaches to performing forensic acquisitions and analysis on systems utilizing disk encryption.

2. EVOLUTION OF ENCRYPTION OF DATA ON HARD DISKS
Programs such as PGP and TrueCrypt enable file-level encryption, as well as encrypted containers that may be mounted as a volume and used to store data. Some encryption systems make an effort to support plausible deniability, making it difficult to determine whether a disk contains encrypted versus random data. TrueCrypt can be configured to manipulate metadata of encrypted containers to make it more difficult to determine encrypted data were last modified or accessed. Rubberhose, another encryption system, allows users to create multiple access paths to their encrypted disk, with different passphrases unlocking discrete data while hiding the existence of other encrypted data on the drive (http://iq.org/~proff/rubberhose.org/).

Although an encrypted container is an effective mechanism for protecting specific data, it is not integrated with the operating system, and many activities on a computer leave traces outside of the encrypted volume. For instance, Web browsers commonly leave remnants of Internet activities on disk, including details about online transactions, which can be recovered even after they

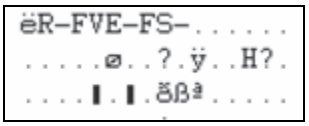

Figure 1: Physical View of a Volume Header Protected by Bitlocker

are deleted. Even when e-mail messages are encrypted or stored in an encrypted container, plaintext versions may exist in the pagefile or unallocated space. In one case, the criminal group under investigation made extensive use of PGP to encrypt e-mail and areas of their hard drives. Searching the entire disk for patterns such as "PGP DECRYPTED" recovered plaintext versions of encrypted data, including e-mail messages between members of the group [4].

Starting with Windows 2000, Microsoft integrated encryption into the Windows operating system with EFS, which is a file system driver that can encrypt files on NTFS [5]. EFS uses a symmetric key to encrypt data, and then protects the symmetric key with the user's public key. The default behavior in Windows 2000 is to also encrypt the user's EFS protected data with the public key of the local administrator account but this poses a security risk and was disabled in later versions of the operating system.

Forensic examiners can still recover useful information despite the use of filesystem-level encryption such as EFS [6]. Plaintext versions of encrypted data may be found in a temporary file created when editing a document, a spool file created when a document is printed, or a deleted file that has not been overwritten. Keyword searching a hard drive for dates, phrases, and other known characteristics is an effective mechanism for finding relevant plaintext. In addition, forensic examiners may be able to recover encryption keys from a hard drive and use them to decrypt files. Forensic examiners might also find valuable information in volatile memory, such as a passphrase used to encrypt data or plaintext of relevance to a particular investigation.

To address weaknesses in file system-level encryption, Microsoft introduced BitLocker in Windows Vista Ultimate to provide full disk encryption [7]. BitLocker is integrated into Windows Vista, however it is not enabled by default and must be enabled and configured to protect data on the hard drive. The encryption keys for BitLocker can be stored in a protected partition on the disk, on removable media, or in Active Directory. Using BitLocker, all data on a hard drive can be encrypted, including unallocated space and all components of the operating system and file system. The first sector of a BitLocker encrypted volume, shown in Figure 1, governs the pre-boot mechanism for loading decryption keys from a protected area on the hard drive or from a removable device. By protecting data at the physical level, BitLocker prevents the approaches to data recovery that work with filesystem-level encryption described above. Without the necessary credentials to unlock the FDE, it is not possible to view any logical level information.

Various third-party FDE solutions have also been developed to provide full disk encryption for Windows platforms including, SafeBoot.com, Pointsec.com, Utimaco.com, PGP.com, and TrueCrypt.org. PGP client version 9.6 also provides support for Mac OS. Some of these third-party FDE solutions use pre-boot authentication to unlock the decryption key, and intercept operation system access to the hard disk, decrypting and encrypting data at the sector level (see Figure 2). In this way, FDE blocks access to the operating system itself and thereby prevents unauthorized access to data even by persons with direct physical access to the hard drive. Some FDE systems can also be integrated with Windows authentication, allowing a convenient single-sign-on mechanism while providing the same sector level protection.

Hardware-based disk encryption technologies such, as FlagStone (www.flagstonerange.com) and DiskCrypt (www.enovatech.net) utilize specialized controller cards and pre-boot authentication to provide full disk encryption. Hard drive manufacturers including, Seagate and Hitachi, are creating devices with built-in disk encryption. The impact of full disk encryption on digital forensics is significant, and may adversely affect the ability to create a forensically sound duplicate of a hard drive or to recover intelligible information useful to an investigation.

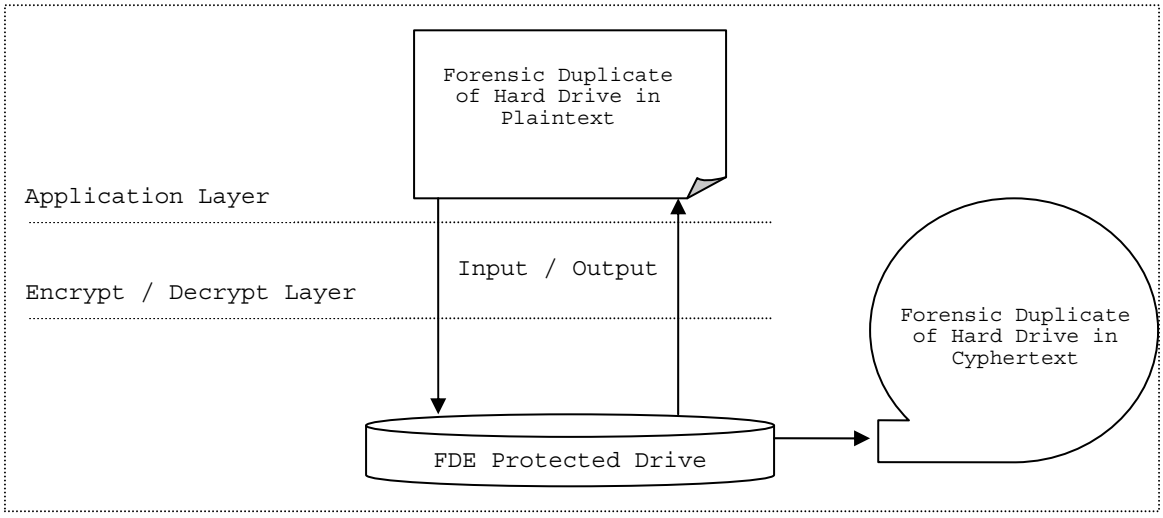

Figure 2: Depiction of FDE driver intercepting I/O system calls to hard drive

3. FORENSIC ACQUISITION OF FULLY ENCRYPTED DISKS

Forensic examiners who do not check for the presence of full disk encryption run the risk of preserving data at a site and returning to their forensic laboratory only to find that they cannot view any data in a logical form. Performing a forensic preview of an evidentiary hard disk can provide forensic examiners with the necessary information to determine the most effective method of acquiring a forensic duplicate. During a forensic preview, experienced examiners look for a FDE boot loader, the lack of folder structure, and patterns that are associated with common FDE systems.

The most common approach to creating a forensic duplicate of storage media is to remove the hard drive and connect it to an acquisition system. However, FDE programs such as SafeBoot make all data on a hard drive, starting with the first sector, unreadable without the decryption key and passphrase. Figure 3 demonstrates that a forensic duplication device reports an error when FDE is encountered. Although a forensic duplicate of the physical device can be acquired, no logical structure will be visible to forensic examiners.

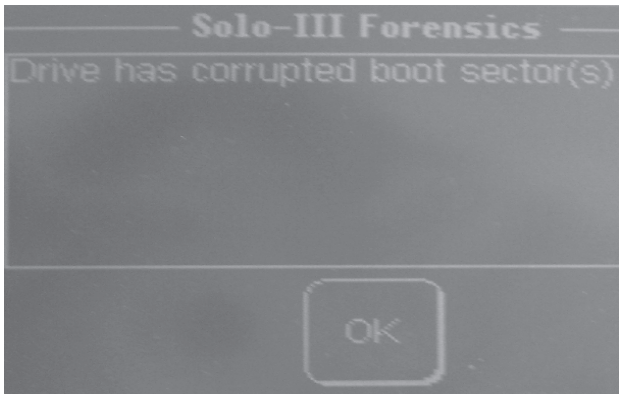

Figure 3: Message Displayed by ImageMASSter Solo-III when Acquiring a Forensic Duplicate of a Hard Drive Encrypted Using FDE.

A manual inspection of the beginning of a hard drive, such as sector 0 or 63, can also reveal patterns associated with certain types of FDE. For instance, SafeBoot uses the word “safeboot” in sector 0, and some versions of PointSec put the word “Protect” in sector 63.

It is possible to decrypt a BitLocker protected disk by connecting the drive read-only to a forensic examination system running Windows Vista and providing a recovery password to BitLocker. Although data will still be encrypted at the physical level, a forensic acquisition tool can be use to acquire the logical volume in unencrypted form (see Figure 4).

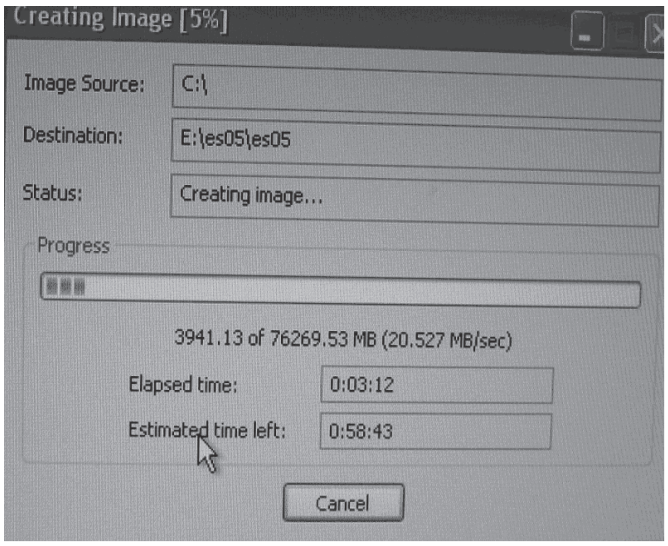

Figure 4: FTK Imager Acquiring a Logical Volume on a Live System with a FDE.

Another approach to acquiring a forensic duplicate of storage media is to boot the evidentiary system from a forensic boot disk and to copy the data to other media. In some products, a specific command key sequence is required immediately after the Power-On-Self-Test is complete to interrupt the pre-boot process. Even when this key sequence is known and entered, the adverse impact that integrating encryption with the operating system has on digital forensics is clear when the only thing that a forensic examiner sees when attempting to boot from a forensic boot disk is the FDE pre-boot authentication prompt. In PointSec, entering the necessary credentials at the pre-boot authentication prompt can be accompanied by another command key sequence to ensure that the boot device menu is displayed, allowing the forensic examiner to boot from a forensic acquisition boot disk.

Case Example: Security conscious individuals store their encryption keys on removable media, making forensic acquisition more complicated. In one investigation the authors conducted, a RAID server was fully encrypted and the associated keys were on a removable USB thumb drive. Forensic examiners first created a forensic duplicate of the device that contained the encryption keys and restored the data onto a clean USB thumb drive. They then booted the server using Helix, mounted the cloned USB device to access the encryption keys, and decrypted the RAID using a password provided by the system administrator and the command “cryptsetup --keyfile gpg_key luksOpen /dev/sda”. Only then was it possible to acquire a forensic duplicate of logical volumes on the server.

Although somewhat complicated, one important advantage to using a forensic acquisition boot disk to create a forensic duplicate of encrypted disks is that file system metadata are not altered by the processing.

An alternate method of acquiring data on an encrypted disk is to create a forensic duplicate of a live system provided forensic examiners can gain access before the computer is shut down. A live forensic duplicate can be acquired either from the console using tools such as X-Ways Capture and FTK Imager Lite running from removable media as shown in Figure 4, or remotely using tools such as EnCase Enterprise and ProDiscover IR [8].

The X-Ways Capture program can be run from the command line of a live Windows or Linux system, and has a feature that checks for common encryption programs and can create a forensic duplicate of the decrypted drive.

Provided the necessary servlet is running on the target system, remote forensics tools can be used to connect to a remote system and acquire data from encrypted disks that are currently mounted. When dealing with a live system locally or remotely, it is necessary to acquire the logical volume since accessing the physical device will only preserve encrypted data as depicted in Figure 2 above.

4. FORENSIC SOUNDNESS CONSIDERATIONS

The act of collecting data from a live system causes changes that an examiner will need to explain with regards to their impact on the digital evidence. For instance, running forensic tools like FTK Imager Lite and X-Ways Capture from a removable mass storage device will alter volatile data when it is loaded into main memory, and will generally create or modify files and Registry entries on the evidentiary system. Similarly, using remote forensic tools necessarily establishes a network connection, executes instructions in memory, and makes other alterations on the evidentiary system.

Purists argue that forensic acquisitions should not alter the original evidence source in any way. However, traditional forensic disciplines such as DNA analysis show that the measure of forensic soundness does not require the original to be left unaltered. When samples of biological material are collected, the process generally scrapes or smears the original evidence. Forensic analysis of the evidentiary sample alters the sample even more because DNA tests are destructive. Despite the changes that occur during preservation and processing, these methods are considered forensically sound and DNA evidence is regularly admitted as evidence.

Setting an absolute standard that dictates "preserve everything but change nothing" is not only inconsistent with other forensic disciplines but also is dangerous in a legal context. Conforming to such a standard may be impossible in some circumstances and, therefore, postulating this standard as the "best practice" only opens digital evidence to criticisms that have no bearing on the issues under investigation. In fact, courts are starting to compel preservation of volatile computer data in some cases, which requires forensic examiners to preserve data on live systems [9]. In Columbia Pictures v. Bunnell, the court held that RAM on a Web server could contain relevant log data and was therefore within the scope of discoverable information in this case.

One of the keys to forensic soundness is documentation. A solid case is built on supporting documentation that reports on where the evidence originated and how it was handled. From a forensic standpoint, the acquisition process should change the original evidence as little as possible and any changes should be documented and assessed in the context of the final analytical results. Provided the acquisition process preserves a complete and accurate representation of the original data, and its authenticity and integrity can be validated, it is generally considered forensically sound [10].

5. FORENSIC EXAMINATION OF FULLY ENCRYPTED DISKS

In cases when credentials for decrypting a disk are not available at the time of acquisition, a forensic duplicate of the encrypted disk can be acquired using a normal method, such as the ImageMASSter, and data can be decrypted later in a number of ways. In the simplest case, such as BitLocker, an encrypted drive can be connected to a forensic examination system and mounted using the encryption program and a recovery password. The decrypted disk can then be examined using forensic tools to recover deleted data, file system metadata, and other information useful to the investigation.

One effective approach to analyzing an FDE protected system is to load the forensic duplicate into a virtual environment using a tool like LiveView [11]. Figure 5 shows the PointSec pre-boot screen after a forensic duplicate of a fully encrypted hard drive was launched in VMWare with the aide of LiveView.

Figure 5: PointSec Pre-boot Menu Presented After Loading a Forensic Duplicate in VMWare using LiveView.

Another example of a forensic duplicate loaded in a virtualized environment is provided in Figure 6. In this instance, the original user passphrase was not available so the SafeBoot Recovery process was initiated, prompting the examiner for a recovery code that was obtained from the system administrator.

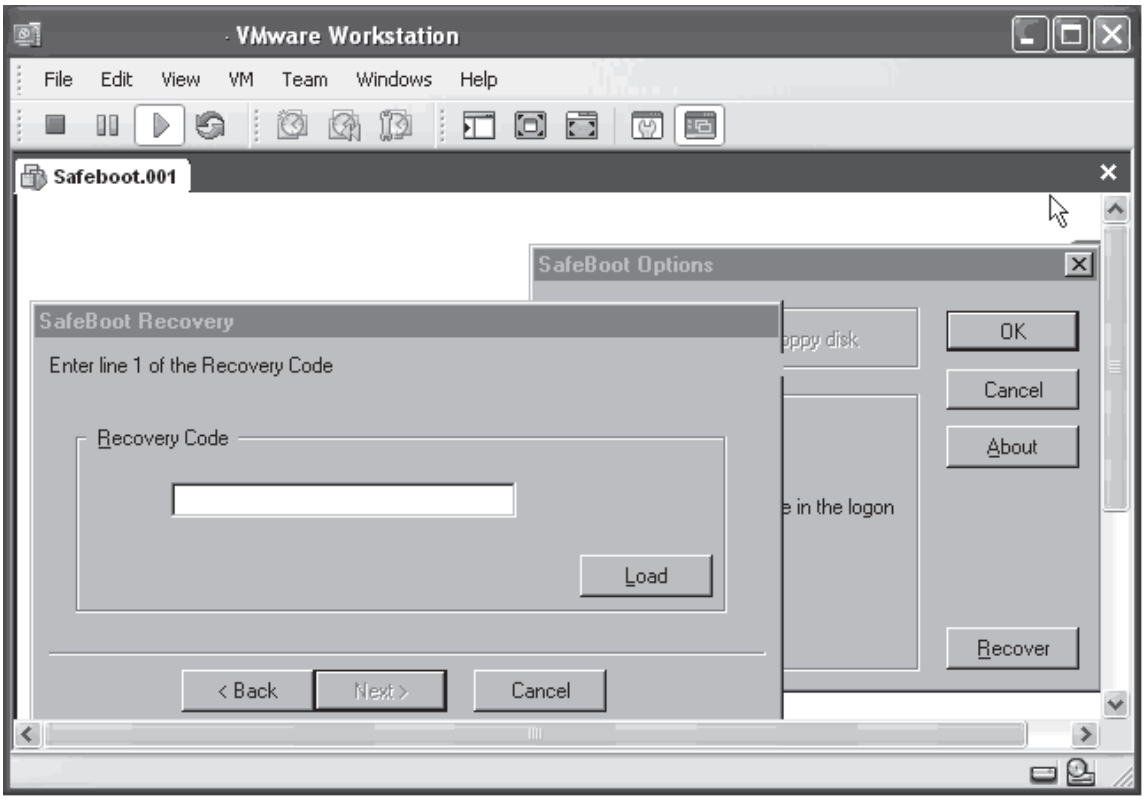

Figure 6: Using LiveView and VMWare to Boot the Forensic Duplicate of a SafeBoot Encrypted Hard Drive.

Booting a forensic duplicate of an FDE protected system in a virtualized environment allows the forensic examiner to decrypt the drive using a passphrase or recovery key, acquire a forensic duplicate of the decrypted drive using a tool like FTK Imager Lite, and view the virtualized computer system as the user would have seen it.

Because not all forensic duplicates will load successfully in a virtualized environment, in some cases it will be necessary to use another approach. For example, the forensic duplicate can be restored to a working hard disk that is connected to a different computer, and the disk can be decrypted and acquired using a forensic acquisition boot disk as described above. Forensic examiners may also be able to boot a restored clone of the original disk, log in with the necessary credentials, and view the system as it would have appeared to the user.

Case Example: The sensitivity of time sometimes requires forensic examiners to image a fully encrypted disk by removing the hard drive and connecting it to a speedy hardware-based forensics duplication device such as the ImageMASSter. In one investigation the authors conducted, an organization that used FDE on all of their laptops required forensic examiners to preserve data on-site and return the computers to their owners as quickly as possible. There was insufficient time to bypass the FDE system and use a forensic acquisition boot disk; use of remote forensic tools was not an option in their environment. In this situation, the forensic examiners acquired forensic duplicates of the encrypted disks on-site and, back at their laboratory, restored the data to a clean hard disk and booted the restored clone in a different computer. This approach was dependent on the drive restoring properly, and still required the proper credentials to bypass the FDE and access data on the restored clone. For those FDE systems that use security features of a Trusted Platform Module (TPM), this approach may not be possible since the hard disk must be connected to the original hardware in order to be decrypted.

Some FDE vendors, including Utimaco and PC Guardian, have worked with the developer of the forensic software EnCase to allow examination of forensic duplicates of encrypted hard drives. For instance, by pointing EnCase at a component of Utimaco named “SGEPROVIDER.dll” that provides decryption functions, the examiner will be prompted for a username and password to view data on the disk. In this way, EnCase can decrypt all sectors in the forensic duplicate and parse the file system, giving forensic examiners access to the same information they are accustomed to seeing on an unencrypted hard drive.

6. CONCLUSIONS

With encryption becoming more integrated into operating systems, individuals have easier access to encryption capabilities that provide strong data protection. In turn, forensic examiners are being compelled to alter our approach to preserving digital evidence. In the past, some best practice guidelines recommended shutting down an evidentiary computer immediately to prevent any alteration of data. With the proliferation of full disk encryption, pulling the plug can prevent future access to all relevant digital evidence and, therefore, forensic examiners must

decide whether to perform a live forensic acquisition before shutting a system down.

Despite the increasing prevalence of FDE, all hope is not lost for forensic examiners. Since the comprehensive protection provided by FDE can translate into complete loss of data in the event of a problem, most FDE systems have an optional disaster recovery mechanism that forensic examiners may be able to use to recover data. Moreover, FDE makes passwords more critical to users, since loss of the password to unlock an FDE protected system prevents them from using their computer at all. As a result, password accessibility and convenience is going to become more important, giving forensic examiners another possible approach to unlocking FDE. Individuals may store the critical password with other important documents or save disaster recovery keys on removable media, increasing the importance of collecting notes, thumb drives, hardware tokens, and other removable devices that can store encryption keys. In corporate environments, forensic examiners may be able to leverage assistance from system administrator and information security personnel to obtain decryption keys to unlock a fully encrypted disk.

The increasing availability and use of strong encryption in the corporate environment is also mirrored among criminal elements. Law enforcement organizations and digital investigators have responded with new strategies and approaches to combat this trend. The FBI installed keystroke monitoring software to capture PGP passphrases during the Scarfo investigation [12]; in October 2007 the UK activated Part III of Regulation of Investigatory Powers Act which enables law enforcement to demand that suspects turn over their encryption keys or face up to five years in prison; the German government recently announced its intention to develop remote access search capabilities of terrorist computers [13]; and governments have long debated the need for key escrow to facilitate law enforcement investigations, as consumers and privacy interest groups have weighed against. Our guidance that examiners make sure to collect written notes and removable media becomes all the more important in the criminal context after the recent ruling that production of encryption keys cannot be compelled and is protected under the Fifth Amendment [3].

7. REFERENCES

[1] Privacy Rights Clearinghouse 2007. A Chronology of Data Breaches. Updated December 31, 2007. DOI= http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[2] BBC 2007. UK's families put on fraud alert, November 20, 2007. DOI= http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm.

[3] In Re Boucher 2007. Case No. 2:06-mj-91, document 35, WL 4246473, 11/29/2007, United States District Court for the District of Vermont. DOI= https://ecf.vtd.uscourts.gov/doc1/1851273316.

[4] United States v. Stop Huntingdon Animal Cruelty USA, Inc. 2006. No. 04 Cr. 00373, District Court for the District of New Jersey.

[5] Microsoft 2003. Encrypting File System in Windows XP and Windows Server 2003. DOI= http://technet.microsoft.com/en-us/library/bb457065.aspx.

[6] Casey, E. 2002. Practical Approaches to Recovering Encrypted Digital Evidence. International Journal of Digital Evidence. Volume 1, Issue 3, Fall 2002. DOI= http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=issue&id=3.

[7] Microsoft 2006. Windows Vista: Security and Protection. DOI= http://technet2.microsoft.com/WindowsVista/en/library/ba1a3800-ce29-4f09-89ef-65bce923cdb51033.mspx?mfr=true.

[8] Casey, E. 2004. Tool review – remote forensic preservation and examination tools. Digital Investigation. Volume 1, Issue 4, December 2004, Pages 284-297.

[9] Columbia Pictures Industries v. Bunnel 2007. No. 2: 06-cv-01093 FMC-JCx. Central District of California..

[10] Casey, E. 2007. What does "forensically sound" really mean?, Digital Investigation. Volume 4, Issue 2, June 2007, Pages 49-50.

[11] Bem, D., Huebner, E. 2007. Computer Forensic Analysis in a Virtual Environment. International Journal of Digital Evidence. Volume 6, Issue 2, Fall 2007. DOI=http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?current=1.

[12] Rasch, M. (2001). Break the Scarfo Silence. BusinessWeek, September 4, 2001. DOI= http://www.businessweek.com/technology/content/sep2001/tc2001094_186.htm.

[13] Leyden, J. 2007. Germany seeks malware 'specialists' to bug terrorists. November 21, 2007. DOI= http://www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/.

ACKNOWLEDGEMENTS

We would like to thank our other colleagues at Stroz Friedberg, LLC, particularly Terrance Maguire and Ryan Sommers.