CHAPTER 6

Antiforensics

Information in This Chapter:

- Introduction of Encryption Technology and the Threat It Poses
- Attacks Used to Break Encryption
- Techniques Used to Hide and Destroy Data

INTRODUCTION

Computer examinations and the resulting evidence make regular appearances in police blotters all across the country. To counter these relatively new forensic advances, antiforensic tools and techniques are cropping up in significant numbers. They are being used by criminals, terrorists, and corporate executives alike. In February 2011, Valerie Caproni, the General Counsel for the FBI, addressed the House Subcommittee on Crime, Terrorism, and Homeland Security. Regarding encryption and the threat it represents, she told the subcommittee, "As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety" (Caproni, 2011).

There are many definitions for the term *antiforensics*. John Barbara defines it this way "an approach to manipulate, erase, or obfuscate digital data or to make its examination difficult, time consuming, or virtually impossible" (Barbara, 2008).

There's even a web site devoted to the subject, and they're not the least bit subtle about their objectives. Anti-Forensics.com is a "community dedicated to the research and sharing of methods, tools, and information that can be used to frustrate computer forensic investigations and forensic examiners." It goes on to describe the web site's purpose, saying, "A major goal of some anti-forensics

The Basics of Digital Forensics. DOI: 10.1016/B978-1-59749-661-2.00006-1
© 2012 Elsevier, Inc. All rights reserved.

software, and the focus of Anti-Forensics.com, is to make the analysis and examination of digital evidence as difficult, confusing, and time consuming as possible" (What Is Anti-Forensics.com?).

The use of antiforensics techniques is not limited to terrorists and pedophiles. Corporate executives have put them to use as well, using these tools and techniques to hide or destroy incriminating e-mails, financial records, and so on. Even everyday applications such as web browsers have features that could be used to obstruct a forensic examination—clearing the Internet history, for example. Most newer browsers come with a "private browsing" mode that doesn't record things such as web sites visited and searches. In the latest version of Firefox, running in private mode will no longer save visited pages, form and search bar entries, passwords, download list entries, cookies, and web cache files (Mozilla Foundation, 2011). See Figure 6.1.

In this chapter we're going to take a look at several techniques used to hide or destroy digital evidence. As you'll see, some of these techniques are highly effective when used properly. Other techniques have little or no impact on a forensic examination. Even using one of the commercially available drive wiping tools is no guarantee that the data will truly disappear.

From an investigative perspective, it's important to know that there are legitimate uses of these antiforensic tools and techniques. Proving the intent, therefore, is critical. Suspects could assert that the wiping application was used only to protect their privacy or they used the defragmentation utility to improve performance. That's possible. However, that defense gets a little tougher to swallow if the tool was only used once and that was three hours after the target became aware of the investigation.

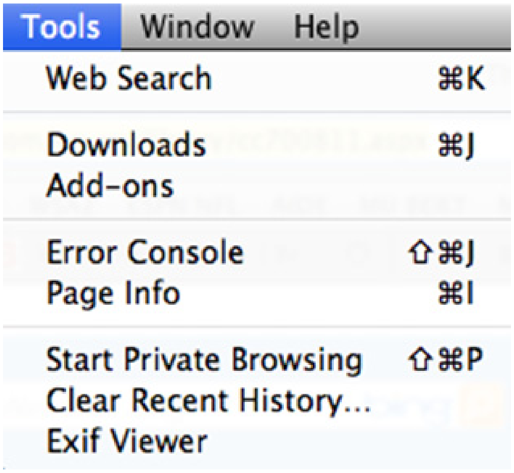


FIGURE 6.1
The "Start Private Browsing" menu option in Firefox 6.0. Also note the option to "Clear Recent History."

HIDING DATA

Hiding techniques range from the simple to the very complex. Changing file names and extensions, burying files deep within seemingly unrelated directories, hiding files within files, and **encryption** are some of the most common hiding techniques. It's the last two techniques that can cause digital forensics practitioners to lose sleep at night.

Encryption

We all have secrets. Companies, governments, and individuals share this universal truth. The Colonel's recipe for fried chicken, our bank account numbers, and the Army's plans for war are just a few examples of information that needs to be kept from under wraps. Before our world became such a wired one, keeping this material safe was, in many respects, a lot less complicated.

The legitimate use of encryption has enabled us to enjoy many of the Internet services that we now take for granted. For example, encryption used in ecommerce permits us to buy our favorite books and book our summer vacation. It keeps our businesses running and our country safe. These modern conveniences, however, are not without a cost. Encryption is a double-edged sword with serious consequences when used by criminals, terrorists, unfriendly nations, and crooked CEOs alike.

Today, we have less direct control over these secrets as they travel over the Internet or fly through the air on a wireless network. It is encryption that provides us with both the mechanism and confidence to store and transmit our most sensitive digital information. In this book, however, the focus is on the darker side of this technology and the threat that it poses. Its value is certainly not lost on many people with bad intentions. Take terrorists, for example; despite their seemingly low-tech lifestyle, they are embracing technology including encryption.

"To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden's al Qaida group, are using computerized files, e-mail, and encryption to support their operations," wrote then–CIA Director George Tenet last March to the Senate Foreign Relations Committee. Ramzi Yousef, the architect of the 1993 World Trade Center bombing, is one of those terrorists putting encryption to use. Yousef saved detailed plans to destroy U.S. airliners encrypted on his laptop (Dick, 2001). If done properly, encryption can keep examiners at bay until hell freezes over, literally.

What Is Encryption?

Encryption is the conversion of data into a form, called **cipher text**, which cannot be easily understood by unauthorized people (Bauchie, Hazen, Lund, Oakley, & Rundatz, 2000). Encryption starts with plain text. **Plain text** is the original, unencrypted message. The plain text message is in the clear and can be read by anyone. A cryptographic algorithm is then applied to the plain text, producing cipher text. Cipher text is basically a scrambled version of plain text that is unintelligible. The algorithm is the method used to encrypt the message. The key is data used to encrypt and decrypt the information. A password or passphrase is commonly used as the key.

Early Encryption

Encryption itself isn't a by-product of computer technology alone. It's been around for thousands of years in one form or another. One of the earliest and best-known encryption schemes is the Caesar Cipher. The Caesar Cipher is a shift cipher and encrypts the data by replacing the original letters with those "x" number of characters ahead in the alphabet. For example, using the Caesar Cipher and a key of five, an "A" would become an "F." Table 6.1 shows the entire alphabet both as plain text and as cipher text after the same cipher has been applied. Note that each letter has been shifted five spaces below its original position.

Now let's encrypt "forensics" using the Caesar Cipher with a key of eight. Table 6.2 shows us the conversion of plain text to cipher text.

This simple process is still employed today. It's frequently used to obfuscate computer code. At first glance, it appears that the terms encryption and obfuscate are interchangeable. They are similar enough to sometimes be confused, but the differences are significant enough to merit clarification. **Obfuscation** and encryption are both intended to make things harder to understand. Obfuscation, however, is used to protect computer code, rather than the data itself (Tyma, 2003). Obfuscation also protects code from reverse engineering. Encryption can't be used in this way because it would render the code totally unreadable to the computer.

ROT13 is a modern version of the Caesar Cipher in use today for obfuscation. In ROT13, letters are shifted 13 positions. In this scheme, an "A" becomes an

Table 6.1 The Alphabet with Simple Encryption (Caesar Cipher). The Key in This Example is Five

Plain text	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher text	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Table 6.2 Shows a Letter by Letter Conversion Using the Caesar Cipher and a Key of Eight

Plain text	F	O	R	E	N	S	I	C	S
Cipher text	N	W	Z	M	V	A	Q	K	A

Table 6.3 **The Opening of Lincoln's Gettysburg Address Encrypted Using ROT13**

Fourscore	and	seven	years	ago	our	fathers	brought	forth	on	this
Sbhefpber	naq	frira	lrnef	ntb	bhe	snguref	oebhtug	sbegu	ba	guvf

continent	a	new	nation	conceived	in	liberty	and	dedicated
pbagvarag	n	arj	angvba	pbaprvirq	va	yvoregl	naq	qrqvpngrq

to	the	proposition	that	all	men	are	created	equal
gb	gur	cebcbfvgvba	gung	nyy	zra	ner	perngrq	rdhny

"N," and so on. Table 6.3 shows an excerpt from Lincoln's Gettysburg Address after ROT13 has been applied.

Algorithms

For the mathematically challenged, like myself, just the word *algorithm* can cause some anxiety. The algorithms we use to send our credit card numbers across the Internet are exponentially more complex than the cipher Julius used in Rome. Although algorithms are complicated and well beyond the scope of this book, we can still get a handle on their basic use and functionality. Put simply, an algorithm is just a set of instructions used to accomplish a certain task. As an example, we can create an algorithm for sending an e-mail about an upcoming meeting.

1. Go to office.
2. Turn on computer
3. Open Microsoft Outlook
4. Click "New Email"
5. Fill in the "To" information
6. Type "Meeting" in the subject line
7. Type the body of the message
8. Press send

Fundamentally, there are two types of encryption algorithms: symmetrical and asymmetrical. **Symmetrical encryption** uses the same key to encrypt and decrypt the data. In contrast, **asymmetrical encryption** uses two separate and distinct keys.

There are many encryption algorithms in use today serving a variety of purposes. You may have already heard of some of them. AES, TripleDES, Blowfish, and RSA are just a few.

ALGORITHMS: IT'S NO SECRET

It may come as a surprise, but the algorithms themselves are open and well published. Why in the world would they put this information out there? It sure seems counterintuitive. Believe it or not, the answer is security. Best practice in cryptography states that the security of algorithms should be "independent of their secrecy" (Schneier, 2002).

This fundamental cryptographic principle has been around for quite some time. In 1883 Auguste Kerckhoffs, a Dutch linguist and cryptographer, said that in any truly effective crypto system, the key should be the only secret. Any system that relies on the secrecy of the algorithm is less secure (Schneier, 2002).

"The #1 lesson I've learned from my work at AccessData is 'you cannot trust closed-source crypto.' You have no idea if it is secure or not," said Nephi Allred, a cryptanalyst with AccessData. "I've reverse-engineered a lot of applications in my time: some good, some bad. While there are some good closed-source apps and some bad open-source apps (actually very few), the best apps are invariably open-source and the worst are invariably closed-source. Personally, I would never trust my own data to a closed source application" said Allred.

Key Space

Key space is a metric that is often discussed when talking about the strength of a particular encryption scheme. The key space or key length has a direct impact on our ability to break the encryption, particularly with a brute force attack. A brute force attack tries to break the password by attempting every possible key combination until the right one is found.

This is where this gets particularly troubling when you consider all the possible key permutations and how long it would take to "guess" the password. An encryption scheme with a 128-bit key would have roughly 340,282,366,920, 938,000,000,000,000,000,000,000,000 possible key combinations. How long would that take a computer to guess the password? Crunching some rough numbers will give us an idea. Using one computer, guessing 500,000 passwords per second would break that key in about 21,580,566,141,612,000,000, 000,000,000 years. Let's crank up the number of computers guessing passwords to 1000. That gets us to a much more "manageable" wait time of only 21,580, 566,141612,000,000,000,000 years. Remember these numbers represent rough estimates; the truth is that they can be much higher depending on the algorithm used. Complex encryption schemes such as Pretty Good Privacy (PGP) can radically drop the number of attempts per second to only a few hundred (Schneier, 2007).

Some Common Types of Encryption

With privacy being such a major concern, encryption tools are now included with some versions of the newer operating systems including Windows 7 and Apple OS X. These tools are **BitLocker** and **FileVault**, respectively. These encryption schemes can be applied selectively, only encrypting certain files or folders. They can also be used to encrypt an entire drive. This is known as full or whole disk encryption.

Full disk encryption (FDE) has some noteworthy advantages. We know from previous chapters that operating systems in their course of normal operation will leave artifacts scattered across the drive. Take swap space, for example. Even though we encrypt an entire folder containing our sensitive files, remnants (or the entire file) could be located in the swap space. Full disk encryption takes care of these data "leaks." The term *full disk encryption* is a little misleading. It doesn't really encrypt the entire disk. In order to run BitLocker, there must be two partitions (sections) on the hard drive: one, known as the "operating system volume," and the other, which contains the files to boot the machine, system tools, and so on. The operating system volume contains everything else including the vast majority of the items of most interest to us (Microsoft Corporation, 2009).

As they say, there is no free lunch. FDE has some drawbacks as well. Performance will likely suffer as the data are being encrypted and decrypted. This encryption/decryption is done "on the fly," meaning that it occurs just before the data are saved or loaded into RAM. Passwords and keys are another concern. Recovering your data is dependent on having the proper authentication. If you lose or forget your password, you will very likely never get your data back. Encryption cuts both ways.

ENCRYPTING FILE SYSTEM (EFS)

Encrypting File System (EFS) is used to encrypt files and folders. EFS is simple to use, using nothing more than a check box in a file's properties. It is "not fully supported on Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Home Premium" (Microsoft Corporation). EFS uses the Windows username and password as part of the encryption algorithm. EFS is a feature of the New Technology File System (NTFS), not the Windows operating system (Microsoft Corporation).

BITLOCKER

Unlike EFS, BitLocker can be used to encrypt an entire hard drive, whereas BitLocker To Go is used to encrypt removable media such as a USB drive (Microsoft Corporation). BitLocker isn't available in all versions of Windows. Currently it's only available on the Windows 7 Ultimate systems (Microsoft Corporation). BitLocker doesn't usually function alone. It normally works in conjunction with a piece of hardware called a **Trusted Platform Module (TPM)**. The TPM is a microchip on the motherboard of a laptop or PC that is intended to deliver cryptographic functions (Microsoft Corporation). The TPM generates and encrypts keys that can only be decrypted by the TPM. If configured to work without the TPM, then the required keys are stored on a USB thumb drive.

BitLocker encryption is pretty stout, making decryption doubtful without the key.

Encountering a running BitLockered machine affords an examiner an excellent opportunity to recover data without having to defeat the BitLocker encryption. Files stored in a BitLocker protected area of the hard drive are decrypted when they are requested by the system (Microsoft Corporation, 2009). Any time you can avoid going toe to toe with encryption is a good thing.

When dealing with a running computer, recognizing the presence of BitLocker could make all the difference in a case. That running BitLockered machine may very well represent the only chance you would have to recover any evidence from that computer.

APPLE FILEVAULT

Apple's latest version of OS X, Lion, comes with FileVault 2. FileVault2 uses 128 bit, AES encryption. With FileVault 2 you can encrypt the content of your entire drive. Apple gives customers the chance to store their recovery key with them. Passwords stored with Apple could be retrievable with the proper legal search authority (Apple, Inc., 2011).

TRUECRYPT

TrueCrypt is a free, open source software that provides on-the-fly-encryption functionality. In on-the-fly encryption, the data are automatically encrypted and decrypted as they are saved and opened. All of this is done behind the scenes without any user involvement. TrueCrypt also is capable of providing full disk encryption. This includes file names, folder names, as well as the contents of every file. It also includes those files that can contain sensitive data that the system creates on its own. These files include things like log files, swap files, and registry entries. Decryption requires the correct password and or key file(s). TrueCrypt supports Windows, Mac, and Linux operating systems (TrueCrypt Developers Association, 2011). TrueCrypt can use multiple encryption algorithms including AES, Serpent, Twofish, or some combination of these three. The key space is 256 bits.

Breaking Passwords

Breaking passwords, or cryptanalysis, can be daunting or practically impossible. In order to give us the best chance for success, we'll need to use any advantage we can get. There are multiple ways to break passwords; some are technical, some are not. Sometimes it's as simple as asking. Options include **brute force attacks**, **dictionary attacks**, and **resetting passwords**. They can all yield positive results. We'll dig into these attacks more in an upcoming section.

The good news is that it's not all gloom and doom. In most cases, we are still dealing with people, and they represent the weakest point in this entire process. Humans can be both lazy and careless, giving us the chance we need to crack the encryption. Far too many people use simple passwords that are easy to break. Some of the best include "password," "letmein," or the ever-popular "123." Birthdays, pet names, or the name of our favorite sports team are also used routinely. Memorizing long random passwords is not easy or convenient for the majority of us. Even if a strong password is used, oftentimes it is written down on a Post-It note and stuck to the monitor. Furthermore, encryption keys can be left unsecured and subject to compromise.

People, being creatures of habit, quite often reuse at least a portion of their passwords. We can exploit this behavior to our advantage. If we can get one password, many times we can get them all. "Sometimes if we can go in and find one of those passwords, or two or three, I can start to figure out that in every password, you use the No. 3," said Stuart Van Buren, a U.S. Secret Service agent (Homeland Security Newswire, 2011).

What exactly qualifies as a strong password? According to Microsoft, a strong password uses a variety of letters, numbers, punctuation, and symbols, and has a minimum length of fourteen characters (Microsoft Corporation).

Examiners may get lucky and find the password in the swap space on the hard drive. Capturing the RAM of a running machine can also help in breaking passwords. You've probably entered a password on a web site at one time or another. As you entered your password, dots appeared, concealing the text as you type. What you may not realize is that the actual password is recorded in RAM. Failing to grab the RAM from a running machine could truly be a missed opportunity.

When the need arises, we have special tools available to us that can break passwords through a variety of attacks. These tools can break some simple passwords in less than a second. One of the leading tools of this type is the Password Recovery Toolkit (PRTK) from AccessData, the Utah-based computer forensic software company. Other tools include John the Ripper and Cain and Abel.

PASSWORD ATTACKS

Passwords can be attacked and broken in multiple ways, but avoiding encryption is always preferable to having to attack passwords. There are tools and techniques we can use to increase our chances of success. One thing working in our favor is the vulnerability that humans bring to the table. Long random strings of letters, numbers, and characters make for excellent passwords. Unfortunately, they are also tough for people to remember. As such, most passwords are based on actual words, recognizable patterns, or both.

Brute Force Attacks

A brute force attack is just what it sounds like. We are using as much computing power as we can muster to guess the correct password. The more computers (or, more precisely, central processing units) we can throw at it, the faster we can break it. As you'll see, "faster" is a relative term when it comes to breaking passwords. Products are available now that harness otherwise idle computers and use them against the encrypted file, folder, or drive. This is known as a distributed attack since the computational burden is spread among multiple computers. Some agencies are getting quite creative in breaking encryption.

The digital forensic folks with the U.S. Immigration and Customs Enforcement Cybercrime Center are using networked Sony PS3 gaming consoles to attack passwords. This approach leverages the power of these devices as well as their cost-effectiveness. “Bad guys are encrypting their stuff now, so we need a methodology of hacking on that to try to break passwords,” said Claude E. Davenport, an agent in the U.S. Immigration and Customs Enforcement Cyber Crimes Center. “The Playstation 3—its processing component—is perfect for large-scale library attacks” (Wawro, 2009).

Password Reset

Sometimes we will go after the software rather than the password. Some applications have vulnerabilities that can be exploited to simply reset the password, giving us the access we need. Unfortunately, the password reset isn’t widely effective, working only on a relatively small number of applications. In instances where it becomes necessary to bypass Windows system passwords, bootable CDs can get the job done. They do this by overwriting data in the Security Account Manager, or SAM for short. Elcomsoft’s System Recovery tool is one of many products that fill this need (Elcomsoft Co. Ltd.).

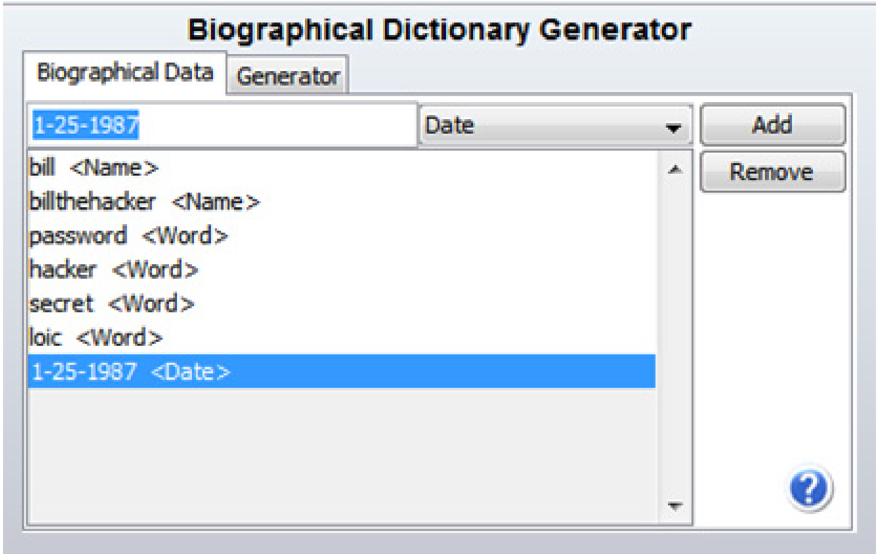
Dictionary Attack

A dictionary attack is more precise, using words and phrases that can be collected from multiple sources. For example, a forensic application can create an index of all the words found on a suspect’s hard drive. These words would come from both the allocated and unallocated space. Other dictionary sources could be terms commonly used in certain criminal circles such as child pornography or narcotics trafficking. Dictionaries can also contain words from specific sources such as web sites.

Intelligence, the background information on our suspect or target, can really increase our chances of success. This information can be used to build a dictionary of potential passwords. Gathering this information starts at the scene. We are not solely interested in the digital devices alone, but photos, books, etc. We want to know the name of our subject’s children and pets. We want to know their hobbies and interests. The terms and words associated with these interests could provide clues to the suspect’s password. For example, if the suspect is a huge Lord of the Rings (LOTR) fan, we can employ a tool that will index (record the content) of a web site devoted to LOTR. The tool will grab names and places such as Aragorn and Rivendell. These terms can then be used to create custom dictionaries that can help unlock the password.

Let’s look at creating a custom dictionary based on biographical information on our suspect, Bill Thehacker. We’ll be using AccessData’s Password Recovery Toolkit. We enter a total of seven bits of information including names, birth date, and some keywords related to Bill. (See Figure 6.2.)

From the seven words in Figure 6.2, the tool then generates over twenty-six hundred permutations, a sampling of which is shown in Table 6.4. Note the combinations of terms with a multitude of prefixes and suffixes.



Biographical Dictionary Generator

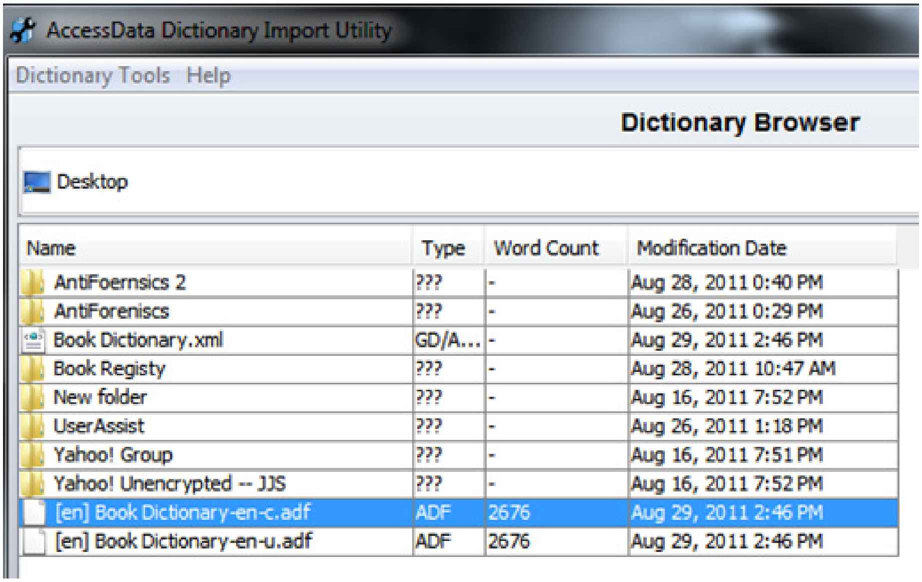
1-25-1987 Date

bill <Name>
billthehacker <Name>
password <Word>
hacker <Word>
secret <Word>
loic <Word>
1-25-1987 <Date>

FIGURE 6.2
Biographical Dictionary Generator in PRTK.

Table 6.4 A Sampling of the Over Twenty-six Hundred Keywords Generated from Our Original List of Seven

1	b25billthehacker	251987secret
25	billthehacker251b	251987 secret
1987	billthehacker125b	secret1987h
1251987	b251billthehacker	h1987secret
billbill	b125billthehacker	secret198725h
bill bill	25billthehacker1b	secret251987h
bill-bill	25b1billthehacker	h198725secret
bill_bill	1billthehacker25b	h251987secret
billb	1b25billthehacker	1987secret25h
bill b	billthehacker1b25	1987h25secret
bill-b	b1billthehacker25	25secret1987h
bill_b	billthehacker25b1	25h1987secret
billbillthehacker	b25billthehacker1	secret25h1987
bill billthehacker	billthehacker25bill	h25secret1987
bill-billthehacker	bill25billthehacker	secret1987h25
bill_billthehacker	billthehacker251bill	h1987secret25
billb	billthehacker125bill	secret1987
bill b	bill251billthehacker	secret 1987
bill-b	bill125billthehacker	1987secret
bill_b	25billthehacker1bill	1987 secret
	25bill1billthehacker	



Name	Type	Word Count	Modification Date
AntiFoernsics 2	???	-	Aug 28, 2011 0:40 PM
AntiForenisics	???	-	Aug 26, 2011 0:29 PM
Book Dictionary.xml	GD/A...	-	Aug 29, 2011 2:46 PM
Book Registy	???	-	Aug 28, 2011 10:47 AM
New folder	???	-	Aug 16, 2011 7:52 PM
UserAssist	???	-	Aug 26, 2011 1:18 PM
Yahoo! Group	???	-	Aug 16, 2011 7:51 PM
Yahoo! Unencrypted -- JJS	???	-	Aug 16, 2011 7:52 PM
[en] Book Dictionary-en-c.adf	ADF	2676	Aug 29, 2011 2:46 PM
[en] Book Dictionary-en-u.adf	ADF	2676	Aug 29, 2011 2:46 PM

FIGURE 6.3
The final word count generated by our seven original entries.

ADDITIONAL RESOURCES

Encryption

Bruce Schneier is a well-respected author and cryptographer who regularly publishes on encryption and security-related issues. He is the author of several books as well as the Blowfish Encryption Algorithm. His book *Secrets & Lies: Digital Security in a Networked World* is both fascinating and highly readable. He also publishes a blog and the Crypto-Gram Newsletter. A visit to his web site, http://www.schneier.com/, is highly recommended.

STEGANOGRAPHY

Steganography, or stego for short, is another and very effective way to conceal data. The word steganography comes from the Greek words "Stegos" meaning covered and "Graphie" meaning writing. Its exact roots equate to covered writing. SearchSecurity.com defines steganography as "the hiding of a secret message within an ordinary message and the extraction of it at its destination" (TechTarget, 2000).

There are two files composing the finished stego file. The file that contains the secret message is called the **carrier file**. Carrier files can be image files, video files, audio files, and word processing documents, just to name a few. The embedded secret document is called the **payload**. The underlying concept behind steganography is fairly straightforward. Let's start with the carrier files.

These file types are used because they have a significant amount of redundant data, also known as "noise." The redundant data are replaced with the data composing the hidden message. Payload files don't necessarily have to be text based. An image file can be inserted into another image file. There are multiple variants or combinations that are possible.

Steganography applications are widely available on the Internet, and many are free. Backbone Security, a company that makes one of the more popular steg detection tools, has cataloged more than 960 separate steganography applications available for download on the internet (Backbone Security.com, 2011).

What makes stego such a concern? First, it's very difficult to detect. Second, once discovered it's very tough, if not impossible, to extract the payload without knowing the steg application and password used to create it.

Before his demise at the hands of Seal Team Six, Osama Bin Laden and his colleagues made extensive use of steganography to communicate. Stego files were posted in sports chat rooms and pornographic bulletin boards (Kelley, 2005).

Detecting the use of steganography is pretty tough. One of the most popular tools is Stego Suite™ from the Steganography Analysis and Research Center (SARC). The current version identifies over five hundred known steganography applications and has the ability to crack and extract payloads from carrier files (Wetstone Technologies, Inc.).

In June 2010, The FBI arrested ten Russian spies who had been in the United States for roughly a decade. These spies made extensive use of steganography as they passed secret messages to the SVR, the Russian intelligence service (CBS News, 2010). A criminal complaint in the case, filed in the Southern District of New York, provided some insight into the use of steganography by the Russians. In the complaint, Special Agent Maria Ricci said in part:

> "In addition, and among other things, a number of the Boston Conspirators' Electronic Messages appear directly to concern communication by means of steganography. For example, one message, dated December 15, 2004, discussed the process of 'decrypt[ing]' messages embedded in images; another message, dated February 22, 2005, discussed 'decypher [ing] [sic]' data embedded in images. Similarly, on or about October 3, 2004, law- enforcement agents, acting pursuant to a judicial order, intercepted aural communications taking place inside the Boston townhouse. Tracey Lee Ann Foley, the defendant, was heard saying to Donald Howard Heathfield, the defendant: 'Can we attach two files containing messages or not? Let's say four pictures ....' Based on my training, experience, and participation in this investigation, I believe that this was a reference to conveying messages by means of steganography—placing 'files containing messages' in 'pictures.' On or about March 7, 2010, law-enforcement agents, acting pursuant to a judicial order, intercepted aural communications taking place inside the Boston townhouse. As a

> final example, in or about March 2010, Foley and Heathfield were heard discussing Foley's use of steganography and the schedule of her communications with Moscow Center"
>
> (*United States of America v. Christopher R. Metsos,* 2010)

DATA DESTRUCTION

Sometimes hiding data isn't enough, and perpetrators try to destroy the data instead. Actually destroying the data is a little more complicated than many people think. The uninitiated may simply hit the delete key, assuming that the data no longer exist. As we've seen, this approach is not effective because the "deleted" data remain on the media and are easily recovered. In contrast, many drive wiping tools can be very effective. Using utilities such as these can leave telltale signs of their use, providing substantial evidence even without the original data in question.

Data destruction can be accomplished or attempted in several ways. Some of them are better than others. **Drive wiping** software is commercially available and can be effective in destroying potential evidence. Much of its effectiveness rests with the quality of the software, how it is used, and the number of "wipes" that are made. Defragmenting or reformatting a drive is frequently attempted, but often delivers limited results.

Drive Wiping

Drive wiping utilities are used to overwrite data on a hard drive in such a way as to make them unrecoverable. Most of these applications are promoted and/or intended to keep personal or corporate information private. Both are noble causes indeed. Unfortunately, these same utilities can be used for other, less honorable purposes. Examples of these tools include "Darik's Boot and Nuke," "DiskWipe," "CBL Data Shredder," "Webroot Window Washer," and "Evidence Eliminator."

Using these tools is not an "all or none" proposition. They can be somewhat surgical in their application, wiping only specified files while leaving others untouched. Operating system files, for example, could be left intact. They can target specific files and folders as well as potentially incriminating system values like those found in the Windows Registry.

These tools do have a legitimate use and are available at many technology stores such as Best Buy. Privacy is a major concern for everyone, and wiping utilities can help. If we want to donate our old computers we certainly don't want our e-mails and other personal information going with it to Goodwill.

Using these tools is no guarantee that the data can't be recovered. Success depends largely on the quality of the tool and the skills of the user.

From an evidentiary or investigative perspective, the presence or use of these applications can serve as the next best thing to the original evidence. Suspects may find it hard to explain why "Evidence Eliminator" software was installed

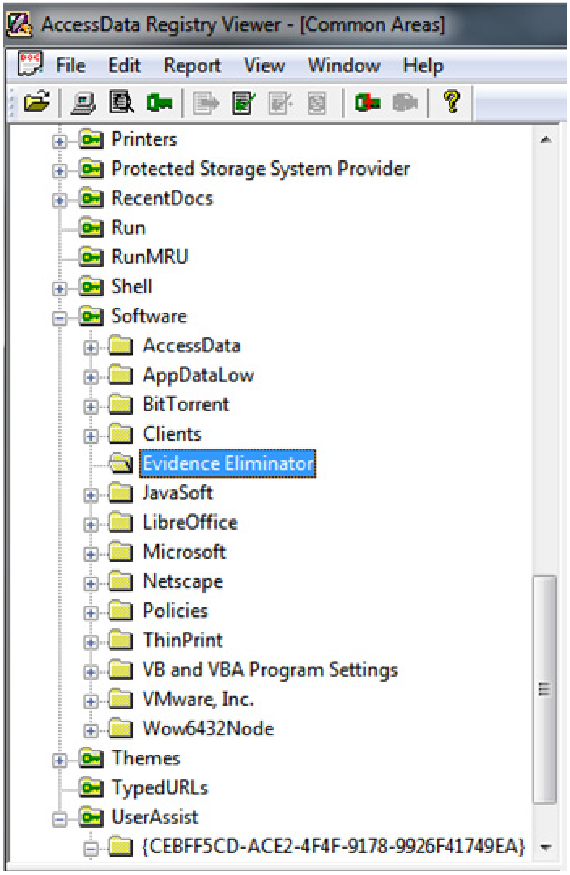


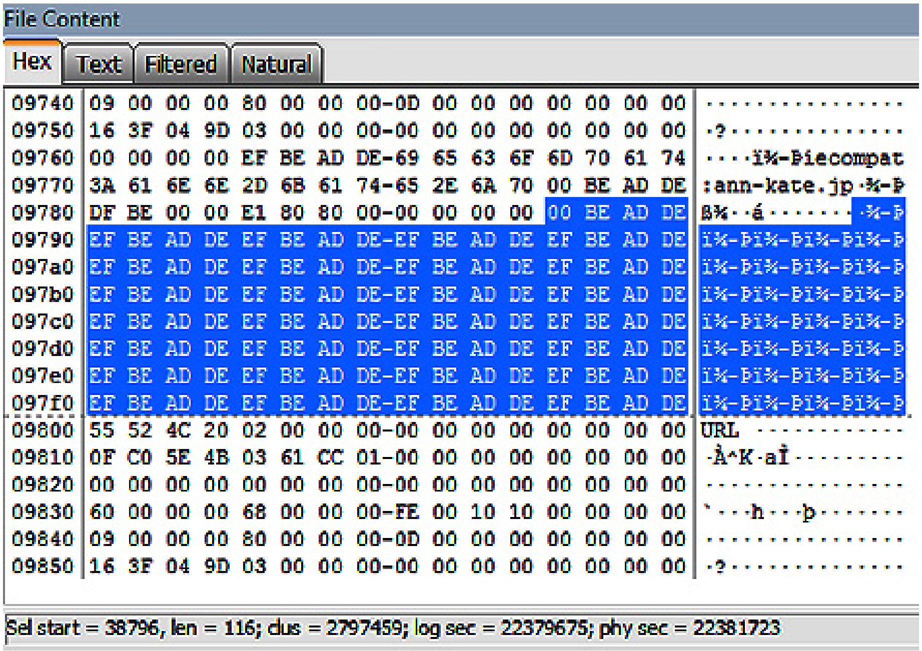
FIGURE 6.4
Note the presence of “Evidence Eliminator” in the Windows Registry software key.

and run on their computer the day before their computer was searched. Figure 6.4 shows the entry for “Evidence Eliminator” in the software key in the Windows Registry. This is an indicator that this software was installed on the machine.

Wiping utilities can leave telltale signs of their use. When looking at the drive at the bit level, a distinct repeating pattern of data may be seen. This is completely different from what would normally be found on a hard drive in everyday use. (See Figure 6.5.)

Evidence of their use can be found elsewhere on the drive. Figure 6.6 shows signs of Evidence Eliminator being opened on that machine.

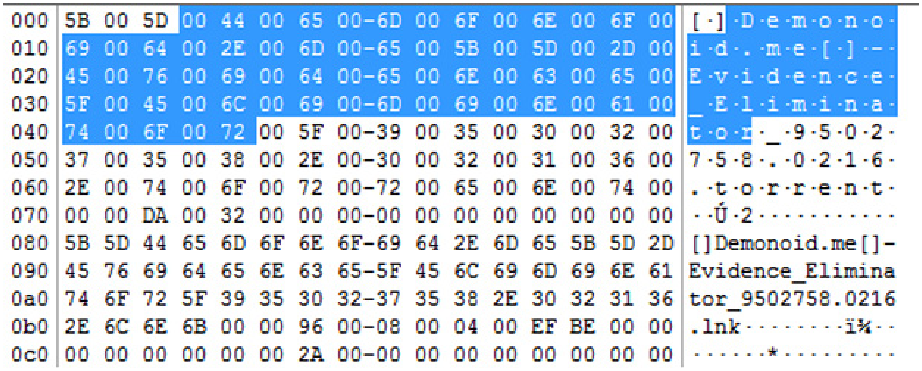
Some operating systems, Apple OSX Lion for example, ship with a drive wiping utility installed. Called Secure Erase, this utility offers multiple options for data destruction. (See Figure 6.7.)



```
09740 09 00 00 00 80 00 00 00-0D 00 00 00 00 00 00 00 ················
09750 16 3F 04 9D 03 00 00 00-00 00 00 00 00 00 00 00 ·?··············
09760 00 00 00 00 EF BE AD DE-69 65 63 6F 6D 70 61 74 ····ï¾-Þiecompat
09770 3A 61 6E 6E 2D 6B 61 74-65 2E 6A 70 00 BE AD DE :ann-kate.jp·¾-Þ
09780 DF BE 00 00 E1 80 80 00-00 00 00 00 00 BE AD DE ß¾··á········¾-Þ
09790 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097a0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097b0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097c0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097d0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097e0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097f0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
09800 55 52 4C 20 02 00 00 00-00 00 00 00 00 00 00 00 URL ············
09810 0F C0 5E 4B 03 61 CC 01-00 00 00 00 00 00 00 00 ·À^K·aÌ·········
09820 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
09830 60 00 00 00 68 00 00 00-FE 00 10 10 00 00 00 00 `···h···þ·······
09840 09 00 00 00 80 00 00 00-0D 00 00 00 00 00 00 00 ················
09850 16 3F 04 9D 03 00 00 00-00 00 00 00 00 00 00 00 ·?··············
```

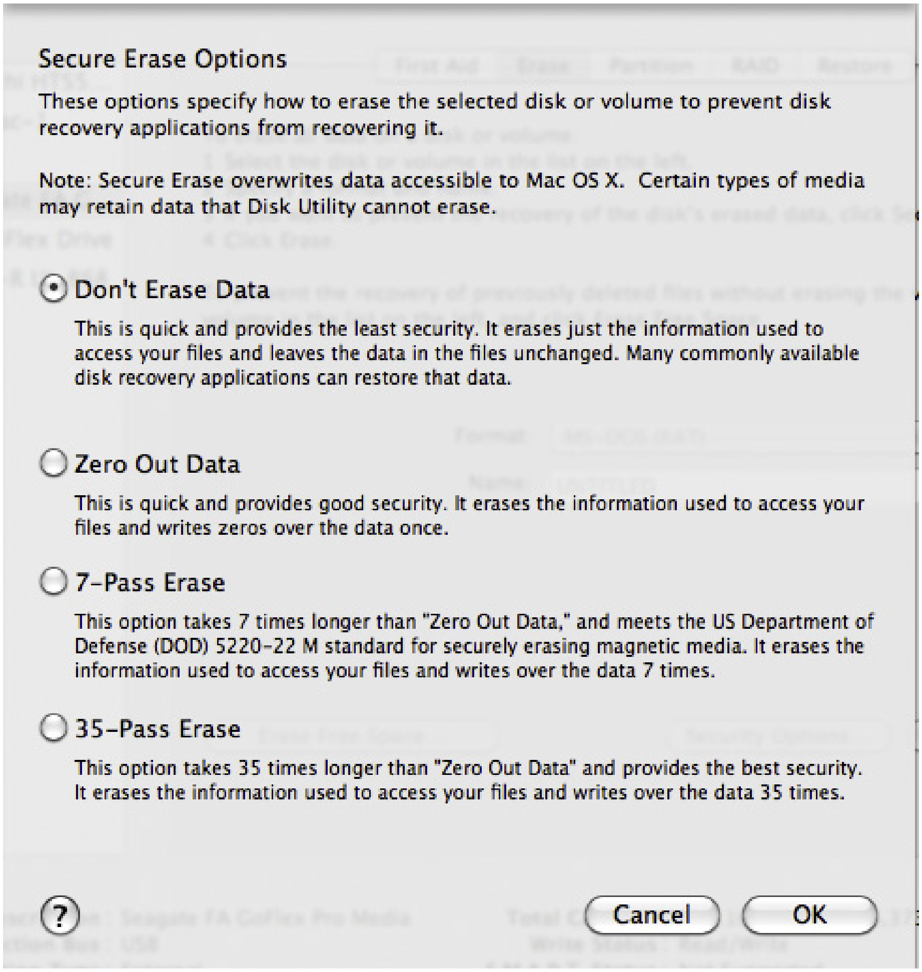
Sel start = 38796, len = 116; clus = 2797459; log sec = 22379675; phy sec = 22381723

FIGURE 6.5
Note the distinct repeating pattern of hexadecimal numbers. This pattern is unusual and may be an indication that a wiping utility was used.



```
000 5B 00 5D 00 44 00 65 00-6D 00 6F 00 6E 00 6F 00 [·]·D·e·m·o·n·o·
010 69 00 64 00 2E 00 6D 00-65 00 5B 00 5D 00 2D 00 i·d·.·m·e·[·]·-·
020 45 00 76 00 69 00 64 00-65 00 6E 00 63 00 65 00 E·v·i·d·e·n·c·e·
030 5F 00 45 00 6C 00 69 00-6D 00 69 00 6E 00 61 00 _·E·l·i·m·i·n·a·
040 74 00 6F 00 72 00 5F 00-39 00 35 00 30 00 32 00 t·o·r·_·9·5·0·2·
050 37 00 35 00 38 00 2E 00-30 00 32 00 31 00 36 00 7·5·8·.·0·2·1·6·
060 2E 00 74 00 6F 00 72 00-72 00 65 00 6E 00 74 00 .·t·o·r·r·e·n·t·
070 00 00 DA 00 32 00 00 00-00 00 00 00 00 00 00 00 ··Ú·2···········
080 5B 5D 44 65 6D 6F 6E 6F-69 64 2E 6D 65 5B 5D 2D []Demonoid.me[]-
090 45 76 69 64 65 6E 63 65-5F 45 6C 69 6D 69 6E 61 Evidence_Elimina
0a0 74 6F 72 5F 39 35 30 32-37 35 38 2E 30 32 31 36 tor_9502758.0216
0b0 2E 6C 6E 6B 00 00 96 00-08 00 04 00 EF BE 00 00 .lnk········ï¾··
0c0 00 00 00 00 00 00 2A 00-00 00 00 00 00 00 00 00 ······*·········
```

FIGURE 6.6
Shows signs in the MRU that the program Evidence Eliminator has been opened on this machine.



Secure Erase Options

These options specify how to erase the selected disk or volume to prevent disk recovery applications from recovering it.

Note: Secure Erase overwrites data accessible to Mac OS X. Certain types of media may retain data that Disk Utility cannot erase.

● Don't Erase Data

This is quick and provides the least security. It erases just the information used to access your files and leaves the data in the files unchanged. Many commonly available disk recovery applications can restore that data.

○ Zero Out Data

This is quick and provides good security. It erases the information used to access your files and writes zeros over the data once.

○ 7-Pass Erase

This option takes 7 times longer than "Zero Out Data," and meets the US Department of Defense (DOD) 5220-22 M standard for securely erasing magnetic media. It erases the information used to access your files and writes over the data 7 times.

○ 35-Pass Erase

This option takes 35 times longer than "Zero Out Data" and provides the best security. It erases the information used to access your files and writes over the data 35 times.

FIGURE 6.7
Secure Erase options from Apple OS X. Note the array of options, particularly the number of passes over the data.

MORE ADVANCED

Defragmentation as Antiforensic Technique

Defragmentation or "Defragging" as it's commonly called is often done to improve computer performance. Defragging is the process of moving clusters as close together as possible in order to speed the system up. This procedure involves moving data from one location on the drive to another. As such, data can be overwritten in the process. These overwritten (destroyed) data may have had some evidentiary value.

(Continued)

(*Continued*)

The defragmentation process can occur in three ways; it can be user scheduled, manually initiated by the user, or done automatically by the operating system (Casey, 2009).

There are a few different ways you can attempt to determine whether a drive has been recently defragmented. One way is to boot the drive image in Windows and look at the amount of file fragmentation. Drives in regular use normally show a significant amount of file fragmentation. Drives that show otherwise, without a plausible explanation, would be suspect.

Q & A With Nephi Allred, Cryptanalyst with AccessData, the Maker of Password Recovery Toolkit (PRTK).

By now it should be clear that encryption is a major concern to the digital forensics community. As such, we must be prepared to deal with encrypted data. Decryption tools are one weapon we can bring to the fight. One of the premier decryption tools on the market is Password Recovery Toolkit (PRTK) from AccessData. In the Q&A below, we get a closer look inside PRTK and the encryption it aims to break. PRTK is widely used worldwide by law enforcement, intelligence agencies, and private corporations such as large financial institutions. U.S. users include the FBI, CIA, and Secret Service, just to name a few.

[Q] About how many passwords per second does PRTK guess on a "standard" machine?

[A] Allred: We get this question a lot. It's impossible to answer as it stands because the question itself has an implicit assumption, which is wrong. Namely: all password schemes are not the same. It's a bit like asking how fast animals can go. Which animal? Every program or application or other system that uses passwords does it differently. The way they do it makes all the difference in the world in how much computation is required to test a password.

For example, a "typical" machine might guess two million passwords per second trying to crack an Office 97 file, while the same machine might only guess five hundred passwords per second cracking an Office 2010 file.

And of course the answer also depends on what you mean by a "typical" machine (and that changes as time goes on, too).

[Q] PRTK guesses passwords in a certain order to improve the speed and efficiency. Can you talk a little about how that works and why it's important?

[A] Allred: Not all passwords are created equal. In the space of all possible passwords, some are more likely to be used by humans than others. (For example, "Br1tn3y" is much more likely to be used than "H*i3}-aV.K=TyG7"). So if you are trying to guess passwords, you will be faster and more successful on average if you guess the more probable passwords first.

Of course which passwords are more probable is not always easy to determine, and certainly varies from person to person. PRTK defines a default ordering of passwords that we have tried to make as effective as possible, given what is known about how people tend to choose passwords. But an investigator often has specific knowledge about a suspect and can use that to make a password ordering more tailored to that individual. This is why PRTK gives its users a great deal of password space customization. For example, rather than going with the default, you can specify that a job first try all the passwords in a (possibly customized) dictionary, then all of those words in reverse order, then all of those words with "123," "4eva," or "asdf" appended. And lots more.

[Q] I know that PRTK also relies on identified patterns of passwords (roots and appendages). What are those based on and how does that work?

[A] Allred: Based on various password lists that we've obtained over the years (some from clients of ours, others freely available), we've tried to make password "rules" that generate passwords that people actually use in real life. At this point, this is still more an art than a science. That is, there is no deep statistical analysis going on (yet)—mostly we eyeball the lists and look for patterns. For example, a lot of passwords seem to end with "1". So one of our password rules is "Dictionary followed by common suffixes" (and "1" is one of those common suffixes).

[Q] Do you know just how effective PRTK is in breaking passwords?

[A] Allred: Again, this varies widely over the kinds of files and suspects. I don't have any numbers for you, unfortunately. You should probably talk to people who use PRTK (or DNA) on real cases.

It's worth noting that not all attacks PRTK does are password guessing attacks. Some crypto systems have flaws that allow their passwords to be recovered instantly, with no "guessing" involved. For example, PRTK can instantly recover the master password on the "Whisper32" password manager. This was not uncommon in applications a decade ago, but these days it's becoming much more rare as software developers become more crypto savvy.

[Q] Is there anything that slows down the decryption process? Can you talk about that and why that is?

[A] Allred: Yes, there is. These days, most developers of password using applications are aware of tools like PRTK, and they will use measures to slow down password guessing attacks. As I explained in #1, the speed at which we can guess passwords all depends on how the application uses the password.

An application could deliberately choose a very slow password-to-key methodology. It might hash the password ten thousand times, for example, instead of just one, while transforming the password into a key. (This is a simplification, but you get the idea). This forces the password-guessing tool to also hash the password ten thousand times per password guessed, which leads to many fewer passwords per second.

[Q] How is encryption changing? What do you see is the next "big thing" in cryptography? What challenges do you see ahead?

[A] Allred: Cryptography is a big subject, and I'm hardly an expert in any of the cutting edges of new research. But in the arena of password based encryption, things are changing.

It's not exactly a new insight, but people are becoming more and more aware that passwords as a security device are often inadequate. What we'll use instead of them (or, more likely, in addition to them) is not yet entirely clear, but encryption providers are trying new things.

For example, several applications, like TrueCrypt, allow users to enhance their password with "key files." A key file can be any file, and it is used to scramble a password before use. This means that to run a successful password-guessing attack, PRTK needs to have any and all key files used. It may not be easy for the investigator to figure out what key files were used, if any.

SUMMARY

Antiforensic tools and techniques can have a significant impact on a forensic examination of a computer. To frustrate examiners, subjects generally attempt to either hide the incriminating data in some fashion, or try to destroy it altogether. Encryption is one of the most common and potentially potent forms of data hiding. Powerful encryption is available free on the Internet and included with some versions of both Microsoft and Apple operating systems. These tools can make it practically impossible to recover the encrypted data.

Should encryption be encountered, it can be attacked in different ways. In a brute force attack, every possible password is tried until the right one is found. This is the slowest and least desirable of all the attacks. Increasing the processing power used in an attack can reduce the time needed to break the password. Some password-protected applications have vulnerabilities that can be exploited. These vulnerabilities can allow us to reset the password to one of our choosing.

Dictionaries can be created and used to break passwords. These can range from standard dictionaries to custom ones based on information specific to the target. Pet names, hobbies, interests, and birth dates are just some of the details that can compose a custom dictionary.

Messages or data can be hidden within other files. In a process known as steganography, files (called payloads) are inserted into other files such as pictures or movies (called carrier files). Steganography can be very difficult to detect. If it is detected, it can also prove tough to extract the message from the carrier file.

A subject may choose to destroy the data with a commercially available drive wiping tool. The effectiveness of these tools is far from foolproof. Incriminating data can still be recovered even after the tool has been used. Even if data have been successfully deleted, the software can leave behind telltale signs of their use. Proof of their use can be potent evidence as well.

References

AntiForensics Community. (n.d.). *About AntiForensics: AntiForenics*. Retrieved May 13, 2011, from: http://www.antiforensics.com/

Apple, Inc. (2011, July 26). *OS X Lion: About FileVault 2*. Retrieved August 14, 2011, from: http://support.apple.com/kb/HT4790

Backbone Security.com. (2011, April 26). *Backbone's Digital Steganography Database Exceeds 925 Applications*. Retrieved August 14, 2011, from: http://www.sarc-wv.com/news/press_releases/2011/safdb_v39.aspx

Barbara, J. (2008, December 01). *Anti-Digital Forensics, The Next Challenge: Part 1*. Retrieved August 15, 2011, from: http://www.forensicmag.com/article/anti-digital-forensics-next-challenge-part-1

Bauchie, R., Hazen, F., Lund, J., Oakley, G., & Rundatz, F. (2000, July). *Encryption*. Retrieved August 17, 2011, from: http://searchsecurity.techtarget.com/definition/encryption

Berghel, H. (2011, February 17). Hiding Data, Forensics, and Anti-forensics. *Communications of the ACM*, 15–20.

Caproni, V. (2011, February 17). *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*. Retrieved August 15, 2011, from: http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime, 3rd ed.: Forensic Science, Computers, and the Internet*. Waltham, MA: Academic Press.

CBS News. (2010, June 29). *FBI: 10 Russian Spies Arrested in U.S*. Retrieved September 11, 2011, from: http://www.cbsnews.com/stories/2010/06/28/world/main6627393.shtml

Dick, Ronald, L., (2001, April 5). *Issue of Intrusions into Government Computer Networks*, Retrieved August 14, 2011, from: http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks

Elcomsoft Co. Ltd. (n.d.). *System & Security Software*. Retrieved August 27, 2011, from: http://www.elcomsoft.com/esr.html#forgot%20administrator%20password

Geiger, M. (2005). Evaluating Commercial Counter-Forensic Software. *DFRWS*. New Orleans.

Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden Disk Areas: HPA, and DCO. *International Journal of Digital Evidence*, 1–8.

Homeland Security Newswire. (2011, March 18). *Feds Forced to Get Creative to Bypass Encryption*. Retrieved August 14, 2011, from: http://www.homelandsecuritynewswire.com/feds-forced-get-creative-bypass-encryption

HowStuffWorks, Inc. (n.d.). *What Is a Computer Algorithm*? Retrieved August 17, 2011, from: http://computer.howstuffworks.com/question717.htm

Kelley, J. (2005, February 5). *Terrorist Instructions Hidden Online*. Retrieved August 14, 2011, from: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm

Microsoft Corporation. (n.d.). *BitLocker Drive Encryption Overview*. Retrieved June 20, 2011, from: http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview

Microsoft Corporation. (n.d.). *Compare Windows*. Retrieved June 20, 2011, from: http://windows.microsoft.com/en-US/windows7/products/compare

Microsoft Corporation. (n.d.). *Create Strong Passwords*. Retrieved August 13, 2011, from: http://www.microsoft.com/security/online-privacy/passwords-create.aspx

Microsoft Corporation. (n.d.). *The Encrypting File System*. Retrieved September 11, 2011, from: http://technet.microsoft.com/en-us/library/cc700811.aspx

Microsoft Corporation. (n.d.). *Unique Technology for Enterprise Customers*. Retrieved August 27, 2011, from: http://www.microsoft.com/windows/enterprise/products/windows-7/features.aspx#bitlocker

Microsoft Corporation. (n.d.). *What Is Encrypting File System (EFS)?* Retrieved June 20, 2011, from: http://windows.microsoft.com/en-US/windows7/What-is-Encrypting-File-System-EFS

Microsoft Corporation. (n.d.). *Windows BitLocker Drive Encryption Step-by-Step Guide: Microsoft Corporation*. Retrieved May 13, 2011, from: http://technet.microsoft.com/en-us/library/cc766295%28WS.10%29.aspx

Microsoft Corporation. (2009, July 10). *Windows BitLocker Drive Encryption Frequently Asked Questions*. Retrieved August 18, 2011, from: http://technet.microsoft.com/enus/library/cc766200%28WS.10%29.aspx#BKMK_EntireDisk Microsoft.

Mozilla Foundation. (n.d.). *Private Browsing*. Retrieved August 27, 2011, from: http://support.mozilla.com/enUS/kb/Private%20Browsing#w_what-does-private-browsing-not-save

Phillip, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions*. New York: McGraw-Hill.

Rogers, M. (2005). *Anti-Forensics. Lockheed Martin*. San Diego.

Schneier, B. (2002, May 15). *Crypto-Gram Newsletter*. Retrieved June 20, 2011, from: http://www.schneier.com/crypto-gram-0205.html#1

Schneier, B. (2007, January 15). *Secure Passwords Keep You Safer*. Retrieved August 25, 2011, from: http://www.schneier.com/essay-148.html

Strickland, J. (n.d.). *How Stuff Works: How Computer Forensics Works*. Retrieved May 13, 2011, from: http://computer.howstuffworks.com/computer-forensic3.htm

Symantec Corporation. (n.d.). *PGP Encryption Products*. Retrieved May 13, 2011, from: http://www.symantec.com/business/theme.jsp?themeid=pgp

Symantec Corporation. (n.d.). *Whole Disk Encryption: Symantec Corporation*. Retrieved May 13, 2011, from: http://www.symantec.com/business/whole-disk-encryption

TechTarget. (2000, December). *Steganography*. Retrieved August 15, 2011, from: http://searchsecurity.techtarget.com/definition/steganography

TrueCrypt Developers Association. (2011, July 11). *System Encryption*. Retrieved August 14, 2011, from: http://www.truecrypt.org/docs/?s=version-history

TrueCrypt Developers Association. (n.d.). *Documentation: TrueCrypt Developers Association*. Retrieved May 13, 2011, from: http://www.truecrypt.org/docs/

Tyma, P. (2003, April 8). *Encryption, Hashing, and Obfuscation*. Retrieved June 20, 2011, from: http://www.zdnet.com/news/encryption-hashing-and-obfuscation/128604

United States of America v. Christopher R. Metsos, et al. (2010, June 1). Southern District, New York.

Vijayan, J. (2008, February 4). *Updated Encryption Tool for al-Qaeda Backers Improves on First Version, Researcher Says: Computerworld*. Retrieved May 13, 2011, from: http://www.computerworld.com/s/article/9060939/Updated_encryption_tool_for_al_Qaeda_backers_improves_on_first_version_researcher_says.

Wawro, A. (2009, November 19). *US Government Using PS3s to Crack Encryption, Catch Paedophiles*. Retrieved August 17, 2011, from: http://www.computerworlduk.com/news/security/17680/us-government-using-ps3s-to-crack-encryption-catch-paedophiles/

Wetstone Technologies, Inc. (n.d.). *Stego Suite™—Discover the Hidden*. Retrieved August 18, 2011, from: http://www.wetstonetech.com/product/stego-suite/

What Is Anti-Forensics.com? (n.d.). Retrieved August 14, 2011, from: http://www.anti-forensics.com/about-anti-forensics