

# eForensics

## Magazine

COMPUTER

VOL.3NO.05 •

# Anti Forensics Techniques

Detection and Countermeasures

*CIRCUMVENTING DIGITAL  
FORENSICS*

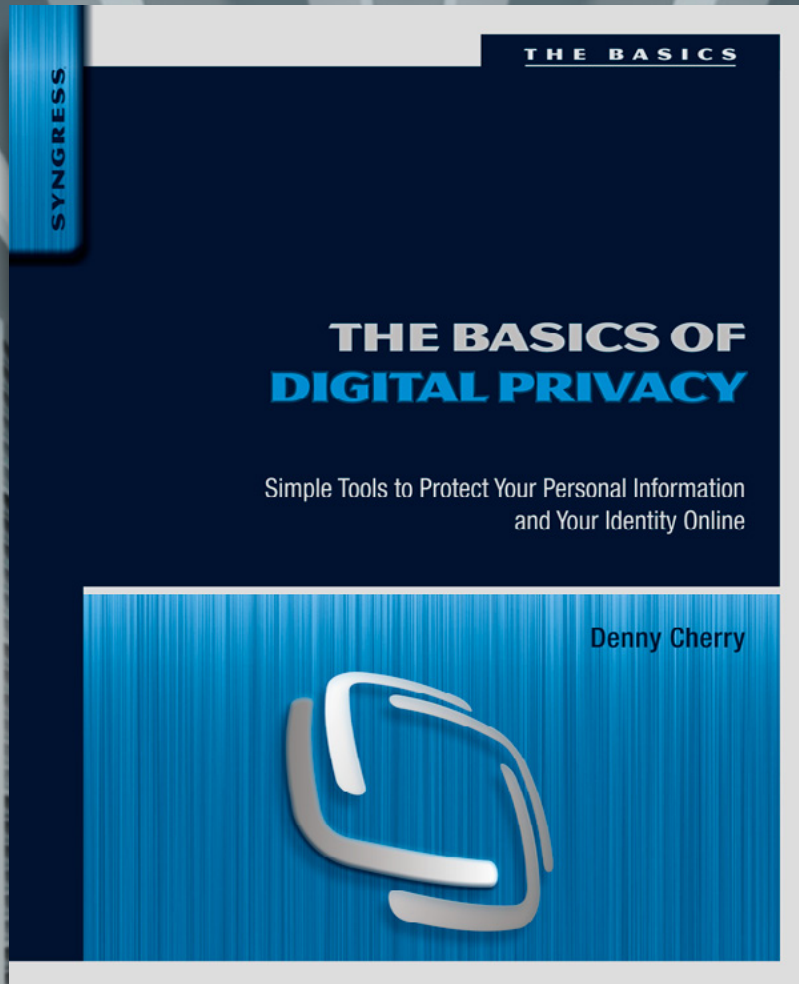
*MANIPULATING A GRACEFUL  
SHUTDOWN TO PREVENT  
EVIDENCE RECOVERY*

*A GENERAL APPROACH TO ANTI-  
FORENSIC ACTIVITY DETECTION*

*CRYPTOGRAPHIC CHOICES  
FOR MAC AND WINDOWS*

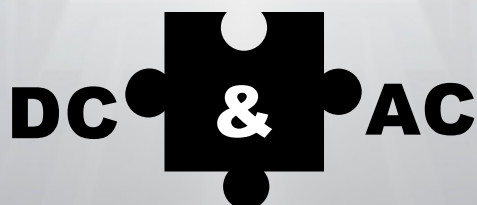
*ATTRIBUTION BEYOND  
THE IP ADDRESS*

*INVESTIGATING STEGANOGRAPHY  
IN SOCIAL NETWORKS*



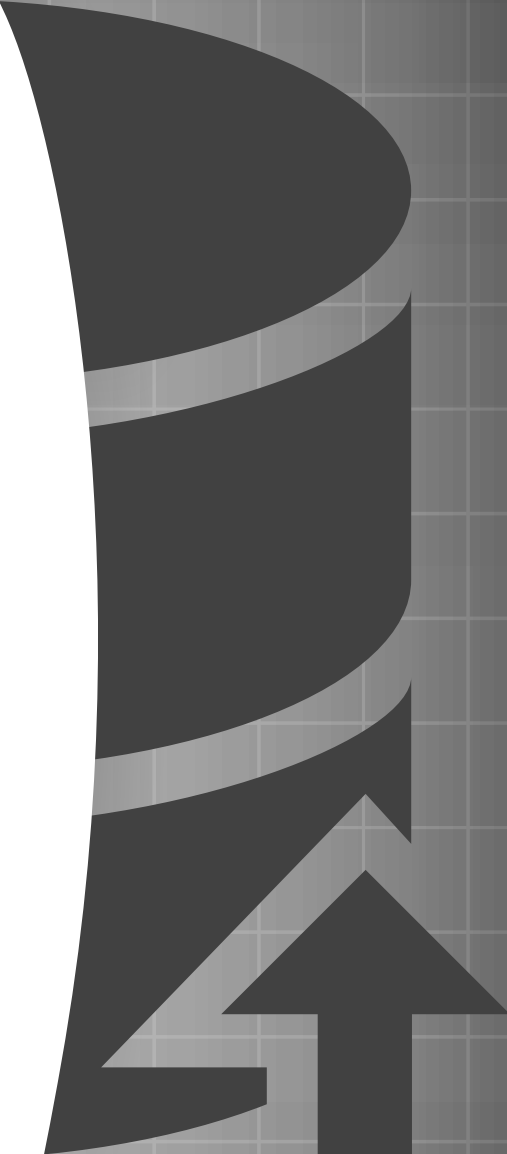
[www.basicsofdigitalprivacy.com](http://www.basicsofdigitalprivacy.com)

The most straightforward and up-to-date guide to privacy for anyone who goes online for work, school, or personal use



DENNY CHERRY & ASSOCIATES CONSULTING

# IS YOUR DATABASE... HEALTHY?



CRITICAL ALERT MONITORING  
DISASTER RECOVERY PLANNING  
SQL SERVER HEALTH CHECK  
VSPHERE / HYPER-V HEALTH CHECK  
STORAGE HEALTH CHECKS

AND MUCH MORE



[WWW.DCAC.CO](http://WWW.DCAC.CO)

**Editor:**

Renata Kwiatkowska  
[renata.kwiatkowska@software.com.pl](mailto:renata.kwiatkowska@software.com.pl)

**Betatesters/Proofreaders:**

Olivier.Caleff, JohanScholtz,  
Shirish Deshpande, Kishore P V,  
Elba Stevenson, Simohammed Serrhini,  
Massa Danilo, Jacopo Lazzari

**Senior Consultant/Publisher:**

Paweł Marciniak

**CEO:** Ewa Dudzic

[ewa.dudzic@software.com.pl](mailto:ewa.dudzic@software.com.pl)

**Production Director:** Andrzej Kuca

[andrzej.kuca@software.com.pl](mailto:andrzej.kuca@software.com.pl)

**Marketing Director:** Joanna Kretowicz

[joanna.kretowicz@eforensicsmag.com](mailto:joanna.kretowicz@eforensicsmag.com)

**Art Director:** Ireneusz Pogroszewski

[ireneusz.pogroszewski@software.com.pl](mailto:ireneusz.pogroszewski@software.com.pl)

**DTP:** Ireneusz Pogroszewski

**Publisher:** Hakin9 Media Sp. z o.o. SK

02-676 Warszawa, ul. Postępu 17D

Phone: 1 917 338 3631

[www.eforensicsmag.com](http://www.eforensicsmag.com)

**DISCLAIMER!**

*The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.*

## Dear Readers,

Digital forensic investigators and academics alike have long been discussing the potential implications of anti-forensic techniques on investigations. Within Anti-forensics, the equivalent is true. The attack may erase the first artifact, but leave 19 others behind. Perhaps the attacker thought they had done enough. Perhaps the attacker didn't realize the other 19 existed. You should know that it is near impossible to remove all forensic artifacts from a system and leave it functional. Let's give this a closer look. We are proud to present you our new issue focused on "Anti Forensics Techniques, Detection and Countermeasures".

I would like to thank you for the support and subscribing to our Magazine. You are always invited to visit our website, share your opinion with us and comment on our activity – we appreciate your feedback! And if you like our Magazine – don't forget to follow us on Facebook, LinkedIn and Twitter(@eForensics\_Mag).

If you have any wishes regarding our future topics do not hesitate but let us know. Feel free to drop us a line and contact our Editor in Chief Joanna at [joanna.kretowicz@eforensicsmag.com](mailto:joanna.kretowicz@eforensicsmag.com).

Enjoy your reading!  
Renata Kwiatkowska  
& eForensics Team

**ANTI-FORENSICS**

*by Mark Shelhart*

Forensics – from the Latin word Forensis means “scientific tests or techniques used in connection with the detection of crime.” All of us who read this magazine are aware of the many people who have motivation to thwart the forensic process (and the fine work that you do). No matter the reason, the bad guys (and girls) have valid reasons to want to cover their tracks. It may to covet their wrong doing like stealing company documents. Perhaps it’s to maintain their persistence (so they can keep stealing credit cards). Within this article we’re going to discuss ant-forensic methods, easy to hard. We’re not going to just hand you ‘how to” solve them, but work your brain in a way you can solve these ‘problems’ on your own.

08



**OPTICAL MEDIA DATA HIDING- TIPS, TECHNIQUES AND ISSUES**

*by Paul Crowley*

Data hiding is substantially different from encryption. Encryption puts the “container” with the data front and center in the examiner’s face and is a challenge. A well-executed encryption can be a serious blockade in that without the password being revealed in some manner the encrypted data is inaccessible. Unfortunately for the world of secrets, it turns out that in the face of this sort of challenge there are many, many ways of acquiring the password and gaining access to the data.

14



**EXAMPLE OF MANIPULATING A GRACEFUL SHUTDOWN TO PREVENT EVIDENCE RECOVERY**

*by Lance Cleghorn, M.S.*

When responding to a computer incident, many technology professionals feel compelled to shut down the computer in question through a graceful shutdown rather than remove power from the system and risk data corruption or loss of volatile data not committed to permanent storage. The operating procedure of completing a graceful shutdown has a myriad of vulnerabilities that could be utilized by the system owner or a third party actor to disrupt or destroy evidence and prevent forensic recovery. Removing the power from the system while running presents a far smaller risk than attempting to gracefully shutdown a system that the incident responder can never fully guarantee is under their control and impervious to sabotage.

24



**A GENERAL APPROACH TO ANTI-FORENSIC ACTIVITY DETECTION**

*by Joshua I. James, Moon Seong Kim, JaeYoung Choi, Sang Seob Lee, Eunjin Kim*

The first challenge with detection of ‘anti-forensic’ techniques and tools, however, is to understand what exactly anti-forensics is. A number of works have proposed definitions of anti-forensics,

30



a d v e r t i s e m e n t



**better safe than sorry**  
**[www.demyo.com](http://www.demyo.com)**

however, Harris gives one of the most comprehensive discussions on the topic, eventually defining anti-forensics as “any attempts to compromise the availability or usefulness of evidence to the forensics process” (Harris, 2006). Other definitions were given prior to this, but – as Harris points out – they focused on specific segments of anti-forensics. Harris’ definition may be suitable for a general understanding of anti-forensics, but gets us no closer to understanding different types of anti-forensics and their nuances.

## 36

### WHAT TO EXPECT WHEN YOU’RE ENCRYPTING CRYPTOGRAPHIC CHOICES FOR MAC AND WINDOWS

by Eric Vanderburg

Cryptography is an interesting field of study and it forms the basis of much of the communication the average person takes for granted as they use computers, networks and the Internet. Encryption is the process of making a message such as a data file or communication stream unreadable to anyone lacking the appropriate decryption key. Encryption uses mathematical formulas to modify the data in such a way that it would be extremely difficult to put back together without the key. The information is combined along with a different routine of information making it impossible for any user to decrypt unless the key and the routine are available.

## 42

### THE ROLE OF INTERNET SEARCHES IN COMPUTER FORENSIC EXAMINATIONS

by Edward J. Appel, Sr.

Today, most types of investigations are incomplete without including a forensic examination of computers, tablets, cell phones and other devices hosting suspects’ files and online activities. Pew’s Internet and American Life research shows that most Americans are online and frequently use the Internet for a variety of communications. Criminals use computers and smart phones for efficiency in their nefarious tasks, including conspiratorial messaging, meeting arrangements and record-keeping. Cybercrime is increasing, as many types of illegal acts move online, such as identity theft, fraud, misappropriated copyrighted software, movies and music, child pornography and account takeovers, often involving thousands and even millions of database files stolen or misused for the money.

## 46

### ATTRIBUTION BEYOND THE IP ADDRESS

by Dr. Char Sample & Dr. Andre Karamanian

Attribution with great confidence is very difficult to attain due to proxies and other anonymizing technologies. A new method that allows security experts to gain new insights into the attacker’s plans is needed. One such method would invoke the use of social sciences in a cross-discipline approach in order to both profile attackers and to anticipate their next steps. This article discusses the results of some early studies that use this cross-discipline approach and how the results may be understood within the context of Hofstede’s cultural dimensions framework. Hofstede’s dimensions provide explanations for human behaviors that are influenced by national culture; this in turn may provide valuable insights into attacker’s methods and next steps that can be used for both attribution and countermeasures.

## 52

### INVESTIGATING STEGANOGRAPHY IN SOCIAL NETWORKS: A “HOW-TO” FOR THE AVERAGE JOE

by April L. Tanner, Ph.D.

Are websites and applications making it easier for criminals to hide and share information on the Internet? Investigators would hope that this would not be the case; however, the reality is that it is quite easy to hide, send, and share information on the web. This presents a problem for forensic investigators given that, not only do they have to recover and examine evidential data contained on hard drives and other media, but they must also consider applications and other freely available tools that can compromise investigative attempts to acquire useful evidence in computer investigations.

## 58

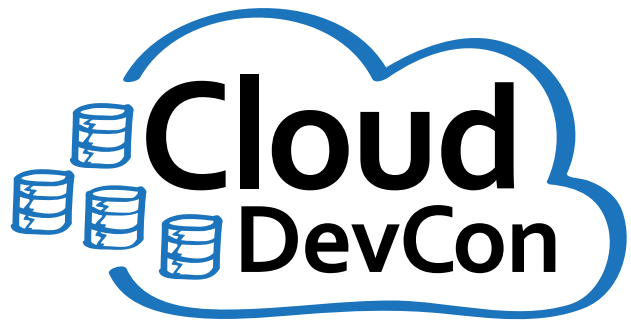
### CIRCUMVENTING DIGITAL FORENSICS

by Alexander R. Tambascia, D.Sc.

This paper is to cover ways to defeat digital forensics capabilities to recover personal identifiable information (PII), confidential information and/or property intellectual property on personal computer and laptop. This paper will look at simple mechanism, encryption; that can be used to defeat common digital forensic tools and forensic investigator abilities to collect stored and deleted information.

# Developing for Amazon Web Services?

## Attend Cloud DevCon!



June 23-25, 2014







San Francisco

Hyatt Regency Burlingame

[www.CloudDevCon.net](http://www.CloudDevCon.net)



### Attend Cloud DevCon to get practical training in AWS technologies

-  Develop and deploy applications to Amazon's cloud
-  Master AWS services such as Management Console, Elastic Beanstalk, OpsWorks, CloudFormation and more!
-  Learn how to integrate technologies and languages to leverage the cost savings of cloud computing with the systems you already have
-  Take your AWS knowledge to the next level – choose from **more than 55 tutorials and classes**, and put together your own custom program!
-  Improve your own skills and your marketability as an AWS expert
-  Discover HOW to better leverage AWS to help your organization today

Register Early  
and SAVE!

A BZ Media Event

CloudDevCon



Amazon Web Services and AWS are trademarks of Amazon.com, Inc.

# ANTI-FORENSICS

by Mark Shelhart

Forensics – from the Latin word Forensis means “scientific tests or techniques used in connection with the detection of crime.” All of us who read this magazine are aware of the many people who have motivation to thwart the forensic process (and the fine work that you do) No matter the reason, the bad guys (and girls) have valid reasons to want to cover their tracks. It may be to covet their wrong doing like stealing company documents. Perhaps it’s to maintain their persistence (so they can keep stealing credit cards). Within this article we’re going to discuss anti-forensic methods, easy to hard. We’re not going to just hand you ‘how to’ solve them, but work your brain in a way you can solve these ‘problems’ on your own.

## What you will learn:

- Anti-Forensics are often shallow
- The right thinking will quickly get you past the attacker’s efforts to hide.
- Some anti-forensics methods may not be solved, but that shouldn’t deter your case.

## What you should know:

- This article is meant for an investigator who is new to anti-forensics, but has experience with forensic tools and the operating system. The content is meant to help you understand “why” and “how” the attacker may cover their tracks.

Let’s be honest, humans have a tendency to be lazy. We will often do only what it takes to get the job done. Hackers are human and they do have a notion to just do the bare minimum to cover their tracks. In the movies, this is similar to wiping a fingerprint off the murder weapon, but NOT the doorknob. Within Anti-forensics, the equivalent is true. The attack may erase the first artifact, but leave 19 others behind. Perhaps the attacker thought they had done enough. Perhaps the attacker didn’t realize the other 19 existed. If there is anything to take away from this article, you should know that it is near impossible to remove all forensic artifacts from a system and leave it functional.

## LET’S DO THE TIMESTOMP

Alright, to the good stuff. Let’s talk about time-stomping. As the name implies this ‘trick’ changes the dates on files. So to the normal user and to the operating system, a file’s date can look to be from the past, from the future, or wherever you like. So as the bad guy, I could make the create date on my malware.exe to match the create date of the windows\system32 folder. As easy as this is to create, this one is pretty easy to detect. Perhaps not with the naked eye, but let’s take a working example and find our answers.










As an example, let’s look at Perfect KeyLogger. While this is a commercial tool with legitimate purposes, it is also a favorite of attackers because of how well it works at harvesting data. In my forensic realm of credit card hackers, there are a few persistent groups that try to covet this tool with time stomping. Have we been detecting it since 2008? Yes. Have they still been successful at

using it? Yes again. So if we put on our blinders, and just search for bpk.exe, we see created and written dates showing 2010.

 bpk.exe	11/22/10 05:41:28AM	11/22/10 05:41:28AM
---	---------------------	---------------------

**Figure 1.** Creation date of November 22, 2010

But being a good analyst. I've installed BPK in a test lab or I've googled the research that someone else (who I trust) has done. I know that BPK.exe comes with at least 8 files that I might use as my indicators of compromise (IOC).

	Name	File Created	Last Written
1	 pk.bin	11/15/11 09:20:24PM	11/15/11 09:20:24PM
2	 bpk.exe	11/22/10 05:41:28AM	11/22/10 05:41:28AM
3	 bpkhk.dll	11/22/10 05:41:28AM	11/22/10 05:41:28AM
4	 BPK.EXE-2FAFFB7E.pf	11/22/11 05:41:38AM	11/22/11 05:41:38AM
5	 bpk.exe	11/22/10 05:41:28AM	11/22/10 05:41:28AM
6	 bpk.dat	05/02/11 12:03:36PM	05/02/11 12:03:36PM
7	 bpk.dat	11/07/11 06:39:45AM	11/07/11 06:39:45AM
8	 bpkwb.dll	11/22/10 05:41:28AM	11/22/10 05:41:28AM
9		07/05/10 02:31:52AM	12/10/10 01:21:49PM

**Figure 2.** IOCS of Perfect KeyLogger

As you can see BPK.exe (line 5) shows 11/22/2010, but pk.bin (line 1) indicates a date of 11/15/11. Hmm. Which do I believe? What do I do? What could change the date?

## TIMESTOMP – REVEALED

In newer Microsoft Windows operating systems, the disk file system keeps a “master table” of all files. It's merely a list of all the files on the disk drive by name, their respective dates, and where they are located physically on the disk drive. This one simple file is the “road map” so that Windows can find the files on the hard drive. So Figure 2 above is very simplistic view of this “master file table”

So as the attacker, I am going to look for this master file table, which is named `$MFT`. For redundancy sake, this file has a mirror clone named `$MFTMIRR`. No, you can't just edit this file with notepad, but with a little bit of code, I can manipulate this `$MFT` to change the dates on my key logger to be whatever I like.

But what our attacker may not know, (or may not care about) is that Windows ALSO stores the dates of files in another section of the file system. The “Standard Information” is the date that most people, most attackers (and most forensic tools) reference. There is a second set of dates called the “File\_Name” attribute that store a second set of dates. Yes, another 4 lines of code could change these dates as well, but the attacker just doesn't seem to care.

So how do I do this technically, you ask? Well this problem has been solved many times in the past and the code is just waiting for you. If you are an Encase person, Lance Mueller has written an MFT EnScript for you. If you are a Perl person, Harlan Carvey has `mft.pl` that can do this for you as well. With either tool, you will quickly be able to see that bpk.exe was in fact installed in November of 2011, but appearing to be from 2010 to the un-suspecting user.

## THAT EXTRA IOC

As we mentioned before, our attacker took the effort to covert the date of bpk.exe and its sub-parts. But of course when the tool run, we can see the attacker left an extra part behind for us. If you look at line 4 above, a prefetch file was created. `Bpk.exe-2faffb7e.pf` has a date of 11/22/2011. This may be a good indicator the program was first executed on this system at this date and time.

## NAMING FILES AFTER WINDOWS FILES

As simple as this attack may be, it's a very common thing for attackers to name their malware after a file in the operating system. Even the best IT person may not catch a transposed filename. Easy ones might include things like `ca1c.exe` but they can get tougher. This attack along with a fresh MD5 (to evade anti-virus) can be a deadly combination. Let's look at the example below.

CSDVersion: Service Pack 3

Base	Size	Path
400000	41000	C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\rundll.exe
7c900000	b2000	C:\Windows\system32\ntdll.dll
7c800000	f6000	C:\Windows\system32\kernel32.dll
7e410000	91000	C:\Windows\system32\USER32.dll
77f10000	49000	C:\Windows\system32\GDI32.dll
71ab0000	17000	C:\Windows\system32\WS2_32.dll
77dd0000	9b000	C:\Windows\system32\ADVAPI32.dll
77e70000	93000	C:\Windows\system32\RPCRT4.dll
77fe0000	11000	C:\Windows\system32\Secur32.dll
77c10000	58000	C:\Windows\system32\msvcrt.dll
71aa0000	8000	C:\Windows\system32\WS2HELP.dll
76390000	1d000	C:\Windows\system32\IMM32.DLL
629c0000	9000	C:\Windows\system32\LPK.DLL
74d90000	6b000	C:\Windows\system32\USP10.dll
1e000000	24e000	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\_MEI17202\python27.dll

Figure 3. Rundll.exe instead of rundll32.exe

As I was looking at this memory dump my eyes immediately focused on the *python27.dll* in the bottom line. It doesn't belong on this government agency's computer I'm analyzing. But wait, I can't jump ahead. Looking at the top line I see it refers to *rundll.exe*. First off, the regular file is *rundll32.exe*. Secondly, there shouldn't be an .exe in the startup folder (it should normally be a link).

Upon further inspection into *rundll.exe* it gets worse. Not only is it named *rundll.exe*, but the code is actually set to recreate itself after each run. And when it recreates itself, it chooses a new name. Checking the .exe with strings we identified that the code renames itself to *win-control.exe*, or *java-insta.exe*, or *java-upd.exe*. For users who know HOW to open task manager, these names may still appear harmless.

## RENAMING – REVEALED

As easy as these attacks are to perform, identifying the IOCs can be just as easy. Regardless of toolset, there are some searches, or conditions you can create that will help you identify these attacks. These may include:

- Search files in the windows directory (and sub folders) for .exes with new dates
  - Time stamping and OS patches may slow you down
- Identify files that have the same MD5 hash, but different names
- Identifying files that do not have a matching "backup" in \dllcache.

## HACKER'S OUTPUT

Not too long ago, some of the bad guys were making it easy. They would put their output in plain text. So yes, when they would harvest credit cards, a simple "SEARCH" in my favorite forensic tool would find their loot. The output file often was in a new directory, which had an install date, which lead to the malware. An easy day's work. Attackers started to realize that stolen cards are worth money, and vulnerable targets aren't as plentiful as they once used to be. Staying hidden, from IT, and "card searching tools" were a wise investment.

So after our normal search patterns, we run into some artifacts pointing to new malware. Running Volatility against the memory dump we see that *cardgrab.exe* is running and has an open file named *card-help.chm*. Looking inside the file we see that it's got a bad signature for a CHM file, and there appears to contain gibberish.

```

__B_C_XUH]K_M____UE____DDKM'YUafSB]W]QDUAA^[U+.<,7&K7?1)E]G@#LK$JKJD]@[U]TBTI]U]TE]
__B    &__C__XUH]K_M____UE____GDJMQ\SDLKLK_U\CUS\YD_@ZT]UD]@[UZ]L
__B&__C__XUK_M____UE____DDKM'YWKDY]_1*&B2(+M,+BJK]]\TD]@[U]TEMPMEMDE]H^S]TE]@[
[____B    &__C__XUH]K_M____UE____GDJMQ^DSLKDDK_@UT]UE]@[U]TM^F

```

**Figure 4.** Encrypted Memory Dumper Output

## HACKER'S OUTPUT – REVEALED

The assumption at this point is that this file contains encrypted data. I don't know what type of encryption. I don't know the contents. So I start looking for clues that my forensic tools just don't 'see' there are some notable things, but what catches my eye is towards the end of line 3. I see a string with a pattern of TEMPMEM. After working enough cases, networking, and reading industry material, I recognized this string may be encoded with XOR. The XOR key just happens to be 'TEMPMEM'.

Why did this happen? Because the data the attacker was stealing just happened to have a string of empty characters, therefore the XOR routine its own encryption key! A few lines of code later revealed that the file contained the following data:

```
memdump/POS.exe-880.dmp found (track1): B7424901298098763
```

```
memdump/POS.exe-880.dmp found (track2): 70928347276329298
```

```
memdump/POS.exe-880.dmp found (track1): B947993.....3453872
```

```
memdump/POS.exe-880.dmp found (track2): 94799384758675309
```

**Figure 5.** XOR encryption key

Needless to say this data indicated to us that the attacker had successfully found the data he wanted, parsed it down to just the bare minimum, and then encrypted it. This attack has long since evolved. We see attacks today where the attacker uses stronger encryption strings. We also see them use a unique key per victim. Yes there are times where the keys to unlock the data just aren't available. You're likely going to have cases that you cannot solve – at least not with just technology.

## OUT OF BAND FACT FINDING

Anti-Forensics is often about the attackers use of tools to stop your tools. Never forget you may have other avenues to crack the case. You know the attacker has gained access to the system. You know the attacker is exfiltrating data. You know it to be a large amount of data (more than just the computer name) is the system breached? I don't think that there is much doubt.

Can you report to law enforcement? Sure! You may have the IP address that the encrypted data is being sent to. If this were a POS system, could you determine how many credit cards were taken? Perhaps not. But, the bank and the card brands 'could' Even though the output file was encrypted, it still had a valid creation date (and so did the malware itself) At this point I'm hopeful I can report a date to the banks so that stolen cards can be turned off faster than the attacker can re-sell them on the black market.

## STRINGS WITHIN EXECUTABLES

Another aspect of forensics is the wealth of information you can find within the 'strings' of an executable. A profitable bad guy is going to realize that the same search we used earlier to find his output file, is the same search he uses to find card data. So it would not be uncommon to find a string like this within the body of an executable.

```
[^#](6011)|(65[0-9]{2,2})\.-?[0-9]{4,4}\.-?[0-9]{4,4}\.-?[0-9]{4,4}
```

**Figure 6.** An attacker's grep string within an .exe

Need a memory dumper within your malware. This one is free if you don't mind it being discovered quickly.

```

445 NUL Installing windows updates...
446 NUL Process Memory Dumper
447 NUL Made By: DiabloHorn (Proud Member of: KD-Team)
448 NUL Use as: memdump.exe -<options> [PID]
449 NUL Options:
450 NUL -? = Show this help
451 NUL -l = List all running processes
452 NUL -s = show info on Process like Path
453 NUL -f = Dump private process memory by PID
454 NUL -f = Full private dump of all running processes
455 NUL %s (PID: %u) Hex: %xh
456 NUL Enter Process Id: NUL %d NUL Module Snapshot Failed

```

Figure 7. xxxxxxxxxxxx

While it takes a bit of time to “search all executables for specific strings” any good forensic investigator can spot the tools like these. There’s many different tools to pull strings from an executable. Cygwin is quick and easy. If you need a GUI to do the same thing. Cuckoo Sandbox is a great tool to have in your bag of tricks.

## ANTI-FORENSICS OF STRINGS

A clever con man would never show his cards. A clever coder would never give hints about his code. If I’m going to write malware, I’m not going to leave any comments in the code when I am done. If I’m real good, I’m not going to use real words to name my variables, my functions, or any other object. So my code may be tough to read later, but I’m going to name my function `aaa()` instead of `searchforCC()`.

Some strings are hard to hide. If I need to search for credit cards, I need my search string somewhere. Well the clever attacker doesn’t put it in his code. He puts it on the internet and downloads it when the code runs. Not only does this keep ‘revealing strings’ out of his code, but it also allows him to change his search criteria on a whim (search for email addresses instead of credit card numbers)

## THE REVEAL

This is starting to move up in complexity, but it is certainly possible to solve. First, running the code in a sandbox may give you best indication. Another mention for Cuckoo. Its very nature is to allow malware to run and capture its every move. If your malware calls home and asks for a string to search for, Cuckoo should record that information for you to view.

If Cuckoo is not at your disposal (including malwr.com) there are other similar sites. If none of these are an option, your next best bet may be to investigate artifacts in memory. For a quick and dirty approach, you may be able to just ‘search’ for the string you want. But you may eventually be extracting executables and other files from memory in order to get values relative to your investigation. If searching memory gets you nowhere, don’t forget pagefile.sys. In some instances you may also have hiber.sys or a wealth of other memory and crash dumps from the system. While a memory dumper may be an attacker’s best friend, it can also be his biggest enemy when trying to stay unnoticed.

## WHO ARE THEY HIDING FROM?

When you are performing your investigation, try to keep in mind ‘why’ the attacker may be using the tool he or she may be using. If I’m in an Incident Response situation, I may be looking for tools that are evading detection by AV as well as IT. Perhaps a rootkit of some type.

If this is a case of computer trespassing or theft of data, I may be hiding from IT or some other outside forensic investigator. I might go through great efforts to delete files, and I might be good enough to delete my profile when I’m done or run some registry cleaner.

## ANTI-ANTI-FORENSICS

A good investigator is aware the operating system at hand and may be able to identify other artifacts that identify what has happened on the system. Some of these alternative methods might include:

- Internet Artifacts – Most users do not realize that their internet history can store information regarding while files they've accessed on the local hard drive. Internet history can be very volatile and often found as recoverable deleted files
- System Restore Points – After every install and uninstall the operating system may have made a log of changed files, but also archived a copy of the registry hives. These hives are a wealth of information regarding files and devices accessed by users.
- Antivirus Logs – Although the malware may be long gone, AV might have gotten a look at it. Even if it didn't show up as a "bad file", Antivirus logs may indicate when a file was loaded, its MD5 hash, and other processes it may have spawned.
- Memory – Unless a system has been rebooted, there is no predictable way to know how much information you will find within memory. If a user or a program touches a file, or communicates on the network, there is most likely several references recorded to memory. To our original point, it is not easy to covet every artifact the malware or your actions leave behind. The registry, for example, may be touched dozens of times by a single attack. If you are attacking a retail store with 1000+ stores, your malware has a high probability of running into many different versions of Microsoft Windows. The ability to test, capture, and remove all possible artifacts prior to a mass attack is near impossible. For you and I that means malware in our lab bears different fruit on different operating systems.

## ANOTHER PERSPECTIVE

If you recall, I pointed out that our hacker friends, like to be lazy. Perhaps not lazy, perhaps they just have better things to do. But do not forget that their opportunities to be successful are often 'vertical' to you horizontal approach to protect or investigate. Your average credit card thief can sit at a coffee shop in Panama and attack every hotel and restaurant in Houston. A single laptop can scan over a million IP addresses in less than 4 hours. In the matter of a day, this one attacker with one machine could have control over 200 different POS systems.

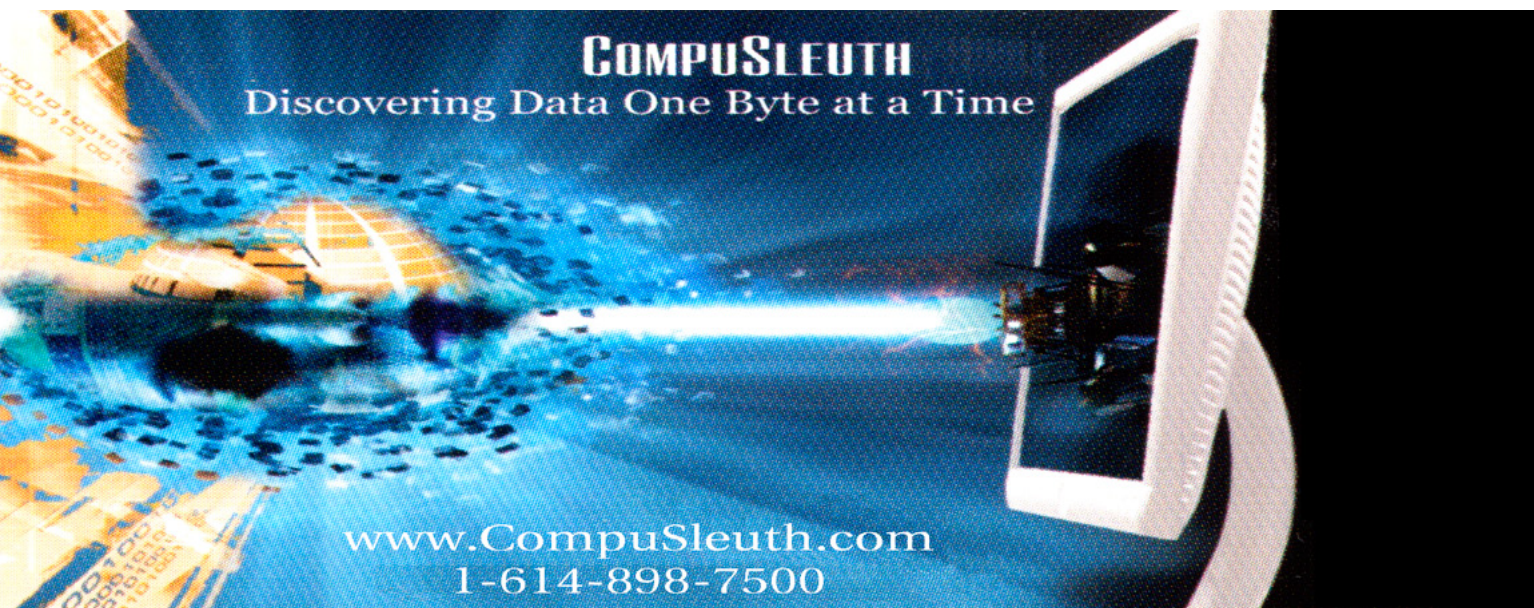
This same attack vector is true within a corporate environment. You may be a staff of 8 people protecting 20,000 workstations in 80 different geographic offices. Your work effort often requires human interaction. The attacker may have simply bought an \$800 exploit kit off of the internet.

It is not easy to stay on top of every attack tool that is in the underground. Knowledge sharing is critical for all of us and to the forensic community. Proper preventative measures and logging are also the keys to slowing the evolution of anti-forensics.

## ABOUT THE AUTHOR

*Mark Shelhart is an expert Forensic Investigations, EnCase and other examination software. He also specialises in Personnel interrogation and interviewing. He has more than 24 years of experience in digital forensics field.*

a d v e r t i s e m e n t



# OPTICAL MEDIA DATA HIDING- TIPS, TECHNIQUES AND ISSUES

by Paul Crowley

Most of the people reading this article will never encounter anything like what is described here. For the most part, criminals are lazy people and this stuff takes work and some knowledge. So for law enforcement this might be a little scary but the techniques here are just too much work. For people working in intelligence and counter terrorism, this might be a bit of a wakeup call because there certainly are people with the wherewithal and motivation to do the things described here. If you are thinking about how much stuff you could possibly be missing after reading this, you might want to think about procedures to identify such things without getting into the really hard stuff. If you are thinking that nobody would ever do these things, well, I hope you are right.

## What you will learn:

- This article describes techniques and tricks for hiding data “in plain sight” on optical media.
- Unlike hard disks, there actually are niches and crevices where data can be hidden away where it will not be found by a cursory examination of CDs and DVDs.

## What you should know:

- A basic idea of what a file system is, and how this relates to a user storing files on a hard disk with Windows or OS X.
- Knowing that hard disks (and CDs and DVDs) are divided up into sectors is important. You do not need to be intimately familiar with the inner workings of CDs and DVDs in order to make sense out of this article.

**D**ata hiding is substantially different from encryption. Encryption puts the “container” with the data front and center in the examiner’s face and is a challenge. A well-executed encryption can be a serious blockade in that without the password being revealed in some manner the encrypted data is inaccessible. Unfortunately for the world of secrets, it turns out that in the face of this sort of challenge there are many, many ways of acquiring the password and gaining access to the data.

The difference with data hiding is the person looking for the data may be fairly certain there is some data there, somewhere, but without being able to see it there is nothing to examine. The data might be there, or it might not. This eliminates the “challenge factor” with encryption where the examiner knows there is something there.

One example of data hiding is steganography, the art of hiding one piece of information inside another. Today, there are public-domain tools for using steganography, most of which leave artifacts which are now well-known and there are tools for detecting these artifacts. This makes these public-domain tools nearly useless but the concept is still a valuable one.

Many people think of ways to hide things on their computers and the most commonly used technique is simply one of folder obfuscation. You create a folder called “Boring stuff” and in that put 30 more folders, each one containing some text articles from the Internet. Add in a hidden folder that has the real stuff in it – or even further folders full of unimportant and irrelevant stuff. While this can work for keeping the (legal) porn collection away from the roommates, it falls apart quickly in the face of any real examination of the computer. There simply aren’t any “corners” where you can hide data on a hard disk where forensic examination tools will not find it quickly and easily.

### **SO WHAT ARE WAYS OF HIDING INFORMATION THAT WORK?**

Something that you might think of as being worthy of James Bond is now very possible – crack open the heel of a shoe and stick a micro SD card in. Or you could put it inside an electronic device, like a cheap radio. Or even a pen or a marker. These days you can find micro SD cards that hold up to 64GB which is a huge amount of data. They aren’t going to show up on most X-ray examinations because there is only a very tiny amount of metal involved and the plastic is transparent to X-rays. As long as the card is protected from the elements and physical damage it is extremely robust and will hold its contents for an average of seven years. The problem with this approach is that while it is unlikely it would be found by a cursory examination of someone and their belongings, if it is found it will be treated with the utmost suspicion. This then becomes a matter of making sure the physical object isn’t found rather than trying to hide data.

How about a way to hide data in plain sight, putting it with some other data that isn’t significant but serves to hide the important data? With steganography the obscuring data and the data being hidden are “mixed together”, but it is possible to both obscure the real data being hidden and keep the two sorts of data separate, or obscuring the data being hidden by disguising it as something else. What the computer user was trying with obfuscated folders can actually be done with optical media because it is quite different than hard disks. The remainder of this article is going to focus on how optical media is different and how it can be exploited for hiding information.

### **RENAMING THE FILE**

No discussion about hiding data would really be complete without at least mentioning this technique that is not exclusive to optical media. Let’s say you have a .ZIP file that contains a collection of data you would rather not have anyone find. Why can’t you just rename it to have an extension of .jpg, .doc or .xyz and be done with it? Wouldn’t that work?

Yes and no. If you are trying to hide this from someone who is just doing a cursory examination of a computer or piece of media they may not catch on that one of the files isn’t what it purports to be. If the computer or media is going to be subjected to a more intensive analysis it is doubtful that this would not be caught – probably because the file doesn’t have the correct header for the type of file it says it is. There are many software tools that will identify a file based on the headers or other content of the file and using any of them makes simply changing the extension pointless as a hiding technique. But, it must be said that to evaluate a large number of files on a hard disk is time consuming and there are clearly circumstances where the time is simply not available.

As long as the hard disk or piece of media containing such a file isn’t examined too closely, this can work. But it will not withstand much scrutiny at all and once such a file is found there will be motivation for an intensive examination of all the files.

### **OPTICAL MEDIA STRUCTURE IS DIFFERENT**

A mistake made by many forensic tools is to treat optical media the same as a hard disk when in reality the two are very, very different. Let’s review these differences:

- hard disks have a single sector size and type; CDs (but not DVDs) have multiple sector sizes and types. DVDs (of all types) have a single, fixed sector size and type,
- hard disks are fully supported by the native operating system for read and write; optical media is still read-only although tools for writing may be supplied with the operating system,

- today a computer hard disk is going to have at least 100,000 files on it and most of them are files belonging to either the operating system or software packages that the user acquired; recent versions of Microsoft Office, for example, have more than 5,000 files all by themselves; larger sizes of optical media can hold a lot of files, but usually less than 10,000 files and often 1,000 or even less,
- your average computer hard disk has a small number of partitions on it and only one file system per partition, different types of file systems are generally only found when multiple operating systems are present in different partitions, optical media has only a single partition but can have multiple sessions and multiple file systems within each session,
- hard disk file systems are pretty complex and have grown in features and performance over the last 20+ years whereas optical media file systems have changed very little over the same time and most are read-only and very simplistic.
- hard disks have a single sector size (512 or 4096, depending on the type of disk drive) and only one sector organization; DVDs and Blu-Ray discs have 2048 bytes per sector and only one sector organization; CDs are quite different in that they have a number of different sector sizes and sector organizations.

With these things in mind, a number of different scenarios for hiding information on optical media are going to be presented. Each one has different advantages and drawbacks and they will be presented in increasing order of difficulty to implement. However, none of these techniques require any programming skill or even extraordinary knowledge of the innards of operating systems or forensic tools. In most cases, these techniques are going to make it very difficult for a forensic examiner to even understand there is data hiding on the media, much less access it without understanding how the data got there in the first place. So let's look at some optical media data hiding techniques...

## MULTIPLE SESSIONS

One way to hide data on a disc is simply by using multiple sessions. You write the files you want to hide to the disc and then in the second session remove them from the directory structure. There are many different software tools for building CDs and DVDs and probably almost as many ways to specify you want to do this.

Now, when the disc is put in to a computer the first session is not shown, only the last is. The last session does not include the files that are hidden, so they are invisible. There is nothing that can be done with the operating system or with add-on tools, at least with recent versions of Windows. Linux and Macintosh computers are equally unable to show the hidden files.

The advantage of this approach is that it is very, very easy to do and if the examiner is simply relying on popping the disc into a computer to check it, it is pretty effective. If the files in the first session are pretty small there is very little to give this away, but if the hidden files are large by looking at information displayed about the disc (how much space is used) and information about the files (how much space is used) it can pretty readily be seen there is something odd going on. For example, if you have a disc that says 500MB is used but you can only see 100MB of files on the disc it fairly obvious the other 400MB is being used for something. This can then prompt the more complete examination of the disc with other tools.

Unfortunately, the way that most common forensic tools work they do not highlight what files are in each session, if they even pay attention to the multiple session structure of such a disc. This makes using these tools difficult for looking at information hidden in this manner. However, even consumer optical media tools are going to show the multiple sessions and the fact that there are files in the first session not carried forward to the next.

It is important to understand that the files in the first session are all still there and completely viable – they have not been “deleted” in any real sense, even though the tool used may have termed the operation being performed as “deleting” the files. What has happened is the first session is a complete file system that contains the files but a second file system has been added which obscures the first. In this second session the files from the first session are simply not there. Not deleted, but just not present. The first session is still there and still references these files. But, because of the way optical media is accessed by operating systems, the first session is obscured and only the second session is visible.

The problem for the recipient of such a disc is how do they access the files in the first session if the operating system will not see them? Again, even consumer optical media tools such as CD/DVD Diagnostic™ and ISO Buster are going to show the files and allow them to be copied from the disc.

While this technique doesn't stand up well against forensic examination, it does utterly defeat anyone looking at the disc with just Windows or OS X – unless they are looking for this and look to see if the used space on the disc corresponds with the space used by the visible files.

It should be noted that with some forensic tools the fact there is space used on the disc and isn't just binary zero will be disclosed saying there is "unallocated" space on the disc. This doesn't particularly help the examiner get at the file names and may imply that data carving is needed to access these files when it is not.

## **MULTIPLE FILE SYSTEM TRICKS**

You may not be aware, but the standard way of writing discs for Windows involves two completely separate file systems being present in every session: one using short, upper case 8.3 file names and one with longer, mixed-case file names. This is done for compatibility reasons for the most part.

The first file system is using a format known as ISO 9660 which specifies three levels of compatibility. For a file system to meet the most stringent level 1 requirements the file names may only use a subset of ASCII characters including upper case letters, numbers and a few punctuation symbols such as \$ and underscore. Discs which conform to ISO 9660 level 1 compatibility are generally readable on any computer with a CD or DVD drive of some sort. As this file system was defined in 1989 it is fairly simple to find all sorts of equipment using discs of this sort and not just consumer computers. For example, it would not be unusual to find an elevator controller running a proprietary operating system using ISO 9660 level 1 discs to update the programming.

Up until the release of Windows 95 in 1995 there was no problem with the 8.3 file name structure for ISO 9660 level 1 – while Windows allowed a somewhat expanded character set for file names, all file names were 8.3 in structure. When a disc utilized the expanded character set it technically became level 2 compatible but this was generally not a problem for interchanging discs between computers and even different operating systems. This all changed when Windows 95 was released.

A significant problem for users of optical media before Windows 95 was how characters outside of ASCII were handled. The standard was something called MBCS, or Multi-Byte Character Set where ASCII characters were mixed with escaped characters for other symbols. This caused all sorts of problems and limited file names to as few as four characters. Windows 95 introduced the concept of Unicode long file names allowing file names far more than 8 characters and allowing all of these characters to be chosen from any Unicode character. This was done by increasing the width of each character from eight bits to sixteen and eliminating any escape characters as were required with MBCS. An extension to ISO 9660 was introduced with Windows 95 called Joliet which allowed 64 character Unicode volume and file names but otherwise leaving the ISO 9660 standard unchanged.

Joliet was sort of an inside joke at the time. Another software company had released a different extension of ISO 9660 that was called Romeo in advance of the Windows 95 release. It was targeted for Windows NT which had introduced longer file names already but was not considered to be consumer-friendly. The joke was that the internal codename for Windows 95 was "Chicago" and "Joliet" is a city not very far from Chicago... so as a replacement for Romeo we got Juliette, or rather Joliet which fit in better with Chicago.

The intent originally was probably that a disc would have either an ISO 9660 or Joliet file system on it but that isn't the way it turned out. Since only Windows 95 – and not even the latest version of Windows NT – would read a Joliet file system and ISO 9660 was all about the ability to write a disc with any computer and have it readable by any other, all of the software for writing discs immediately implemented a strategy of writing both ISO 9660 and Joliet file systems to the same session. So each session of each disc has two complete file systems. One file system has 8.3 upper case file names and the other with 64 character Unicode file names. It turns out that Windows 95 (and all subsequent versions of Windows) automatically generates an 8.3 upper case file name to represent each Unicode file name, so this can be used for the ISO 9660 file name.

With two file systems having parallel directory structures you would think the operating system might give you a choice as to which one is to be displayed. This isn't the way Windows works – it simply chooses the Joliet directory structure if it is present. The ISO 9660 directory is invisible.

Most disc writing software automatically builds parallel directory structures without even allowing any user input into the process. However, there is a command line tool called “mkisofs” which is open source and freely downloadable which builds a disc image and provides the user with options to control the content of the ISO 9660 and Joliet directory structure. Suddenly, it is now possible to build a disc with the two directories not being identical. The disc image can then be written to a disc using any number of different tools for writing to optical media.

There might be some legitimate reasons for advanced users needing to do this sort of thing, but I have to admit that it would be pretty unusual to need this capability. However, I can think of many not-so-legitimate reasons for doing so. The way the command line options work is by allowing the exclusion of files from one directory structure or the other. So, if you were going to produce a disc containing files that needed to be hidden you could exclude them from the Joliet directory – which is the only one that Windows is going to display. It is also preferentially displayed by both OS X and Linux with recent versions of these operating systems.

The effect would be much like the multiple session disc – there would be content on the disc that was not shown. Only by specifically accessing the ISO 9660 directory structure on Linux or possibly OS X or through the use of optical media tools would these hidden files be seen. If they were of considerable size, just as in the case with the multiple session technique, there could be a hint that something odd was going on simply because of the space used on the disc not corresponding with the space used by the visible files on the disc.

An even simpler approach to this is to create a disc with both ISO 9660/Joliet and HFS or HFS+ file systems. Creating such a disc is trivial on a Macintosh computer and it can also be done under Linux, but the HFS or HFS+ file system is invisible to Windows. Today, nearly all forensic examiners and persons trying to quickly examine discs are using Windows. Because of this there is a high likelihood – probably above 90% – that an HFS file system on a disc will be completely ignored and invisible. Put the disc in any Macintosh computer and that file system will be immediately displayed. If you want to play the odds, just using Macintosh-specific computers, software and file formats will render your information unreadable by a hurried examiner using Windows.

Most forensic tools aren’t going to show this because in most cases the presence of multiple file systems is obscured from the examiner by the tool. The presence of the file may be indicated by there being “unallocated” space on the disc, but the examiner isn’t going to be presented with the correct file name and access to the file without doing some work – unnecessary work if both directory structures were shown to the examiner.

Unless the examiner is very much aware of this sort of technique being utilized, it is likely they will miss the alternate directory structure completely and may never see the file name. If the examiner is filtering discs by superficially checking them with Windows or OS X it is highly likely that they will not see anything on a disc like this. The intended recipient of such a disc, knowing what to look for, can then put it in to Linux where it is easy to switch between the Joliet and ISO 9660 directory structure on the disc and simply access the files by name. This is done by using the “nojoliet” option on the “mount” command to specify that the Joliet file system should be ignored and only the ISO 9660 file system should be utilized. On Windows, consumer optical media tools which display all available file systems can be used to display and access the contents of a disc like this. For example, the product CD/DVD Diagnostic can do this.

## **DELETED FILES ON DRAG-AND-DROP DISCS**

Software to utilize rewritable discs has become ubiquitous – it is even included with Windows now. What characterizes this software is that it enables optical media to be utilized as if it was a fully supported type of read-write media, such as a hard drive. There are two basic divisions of this software: that which supports write-once discs and that which supports only rewritable discs. While write-once discs are probably a bit more obvious for this technique, it does work with both sorts of discs and both sorts of software.

Obviously, once a file is written to a write-once disc it is there forever. There is no ability to remove, delete or destroy the original file – but it can be hidden from view. All of the current drag-and-drop writing software today simply removes the file from the directory structure to “delete” it. Therefore, the file is obviously still there.

On rewriteable discs matters are a little more complicated in that it is possible the space occupied by a deleted file could be recovered and reused. A significant difference between rewritable discs and hard disks is that there is no penalty for writing to the same spot on a hard disk over and over. This is different with SSDs, but we can ignore that for this discussion. With optical rewriteable discs each spot has an average of about 10,000 write cycles, which means that there is a very definite cost to each time a spot is written to. Because of this, drag-and-drop writing software does not reuse space – at all – until the disc is full. With this in mind, it can be seen that in general a “deleted” file even on rewriteable discs is simply waiting to be found.

On both write-once and rewritable discs there are obsolete directories which contain pointers to the files which have been deleted. This information may be in sectors that are technically “available” for re-use on rewritable media, but until the disc fills up they are not actually reused. Finding these directories will allow complete recovery of the deleted files, including the file name.

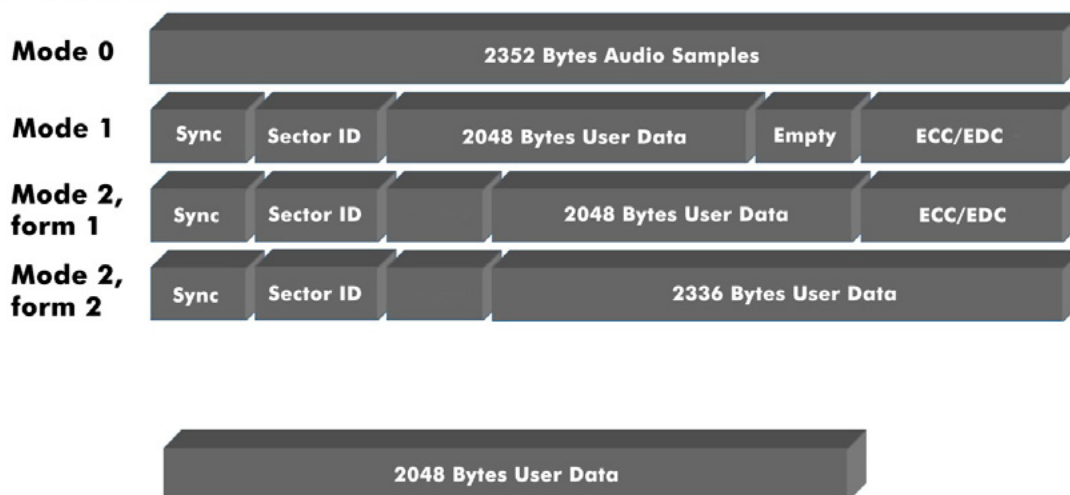
Today most forensic tools have basic support for the UDF file system, which is what is used for drag-and-drop discs. However, they may not analyze the disc to the extent needed to accurately determine what is and what is not “unallocated” space, nor do any common forensic tools automatically recover lost or deleted UDF files. Using these tools, therefore, is going to require quite a bit of work on the part of the examiner to locate such deleted files. As the UDF file system is pretty complicated, doing this by hand is difficult and error prone.

Consumer or forensic tools specific to optical media make this much simpler in that such deleted or lost files are automatically found and recovered. Without this sort of recovery capability, Windows, OS X and other operating systems are going to ignore the deleted files and not show them. If the files are exceptionally large and consume significant space on the disc it is possible that an examiner will notice the discrepancy between the space utilized by files and the space occupied on the disc, although in most cases the free space on the disc being reported by the operating system will include the deleted files. A casual examination of the disc with Windows or OS X is unlikely to present any information that would lead to suspecting there is anything hidden on the disc.

## SECTOR FORMATS

For the remainder of this article it is important to understand the various formats that CDs and DVDs use for sectors.

### CD Sectors



**Figure 1.** *Cd Sectors*

Referring to the illustration, mode 0 sectors are used for audio data and contain only 2352 bytes of audio samples.

Mode 1 sectors are used for data and are the “conventional” format that is seen with most data discs. The Sync portion of the header is 12 bytes that contain hexadecimal FF bytes and is used to identify the

beginning of a sector. The 4-byte sector ID follows this and this is followed by the 2048 bytes of user data. The area labeled “ECC/EDC” contains the error correction code and error detection code that is used to identify and correct errors that occur in reading the data from the disc.

Mode 2 is used with CD-XA discs and can appear as either form 1 or form 2. Mode 2 form 1 sectors are similar to mode 1 sectors except the empty space in mode 1 is relocated and contains the 8 bytes of sector type information and stream identification. Mode 2 form 2 sectors simply use the ECC/EDC error correction information area for additional data space in the sector, extending it to 2328 bytes in length.

DVDs, DVD HD and Blu-Ray sectors are all 2048 bytes in length with only a single sector format.

### **“NAKED” SECTOR UTILIZATION**

On a hard disk having software that just writes to sectors on the disc and trusting that there will be no intersection with the operating system or other software is pretty risky. Several copy-protection vendors have been burned by doing this sort of thing and today just the idea of commercial software doing this forbidden, mostly because of the disastrous history such efforts have had.

On optical media this is somewhat different. Not only are we dealing with a much smaller data area (5GB vs. 500GB, for example), but the operating system does not write to optical media directly. And, the file systems are much, much simpler and generally read-only on optical media. So once a disc is written there is no chance of some application or tool writing over the data, believing that they too “own” some space on the disc.

It is common for there to be quite a bit of space on discs that is not used for anything at all. The best equivalent on hard discs is the space which is discarded at the end of a partition to round up the beginning of the next partition but have the first partition contain full clusters. There is also some space which is not used following the boot sector before the first partition on hard discs. As mentioned, trying to utilize this space for other purpose on hard disks has led to serious issues in the past. But on optical discs there are areas which are not used because of either the way standards have been written or because of the way the writing software has been constructed.

For example, on ISO 9660 and Joliet discs the sectors 0 to 15 are not used by design. If an HFS or HFS+ file system is present then sector 0 will be used, but still sectors 1 to 15 are empty. Writing something in this area is perfectly safe and will be ignored by all forensic software, even that which is designed for optical media.

With UDF discs the area from sector 19 to 256 is undefined and can be used for any purpose. Often some of the control structures for the disc occupy sectors 32 to 47 and 64 to 79 and sometimes sectors 254 and 255 are used for other control information. It is therefore almost a certainty that from sector 80 to 253 could be used on a UDF disc to contain information that will not be used in any way. It is unlikely that this would be recognized as anything by most forensic software. This is not a great deal of space, but if the information to be hidden was simply a text file then compressing it with a ZIP tool might make it fit in a really, really small amount of space.

To access this data it would be necessary to know it was there. Some consumer optical media tools would be able to be used to access it. It would also be possible to copy from the disc using a tool such as “dd” on Linux reading from the “raw” device.

How would you get data to be written to a disc in this kind of area? One technique that works is by writing a disc image (or writing a disc and then copying it to an image file) and then altering the image file. An ISO 9660 image file is simply a copy of 2048-byte sectors from sector zero to the end of the disc. Overlaying information into sectors 1 to 15 and (on a UDF disc) sectors 80 to 253 is very simple to do with a tool like “dd” and dd implementations exist for just about all operating systems today.

### **WRITING DATA AS AUDIO SAMPLES**

A music CD consists of a stream of 4 byte stereo samples, left and right channels each containing 16 bits. These are stored in subcode blocks on the disc with 588 samples in each block. A subcode block is the fundamental unit of storage on a CD and is simply the grouping of the stream of 1s and 0s making up the data on the disc. The samples are played at 44,100 samples per second which requires 75 subcode

blocks to be read each second. This is the basic data rate of CDs or 1X and is how all audio players read CDs. It turns out that there are no requirements on the content of these audio samples, so in theory any sort of digital data could be written to a disc and treated as audio samples.

As there is no error correction or error detection (ECC/EDC) for audio data there would be none for this sort of data, but that is manageable as well. There are a number of techniques for storing data redundantly which would provide sufficient protection from errors so that if errors were encountered in reading the data they would be recovered from.

There are no forensic tools which would examine this sort of data. It would require someone to capture the audio samples and then examine the resulting digital data file. This is well beyond the scope of a cursory examination of the disc – which would reveal it to be a music disc. If someone played it the result would likely be discordant and possibly even damaging to speakers – in other words it would just sound like noise. This might raise the curiosity of someone doing a cursory examination of the disc, but their ability to access the data is likely to be zero without foreknowledge that there was indeed data to be obtained from such a disc. Only then would they have the tools handy to perform such an examination.

This is significantly different than simply renaming a data file to have an extension of .MP3. Such a file would not play at all. It would be more like taking a data file and treating it as audio samples and converting it to .MP3 format – but that would be a true conversion losing bits in the process. The idea of writing data to a CD as audio samples is probably something that would not occur to most people and because of this would be quite secure.

### UTILIZING CD-XA SECTOR FORMAT

In 1992 both CD-i and CD-XA disc formats were introduced. CD-i or CD Interactive was the technology underlying the new CD-i player from Philips that was promoted as the first interactive technology utilizing CDs. There were games written for this platform and it would also play movies, but it never achieved wide acceptance and disappeared quickly.

CD-XA on the other hand introduced a number of different things; the most notable was the concept of multisession recordable discs. It was initially intended to be a multimedia platform where video and audio programs could be mixed in with software. Towards this end there was space reserved for tagging each sector in a way so it could be identified as being part of a stream of audio or video data and supporting multiple, interleaved streams. This was the goal, but it never really materialized. Considerable effort was spent on supporting this in various devices, such as the PlayStation 1 game console – but it never really amounted to anything.

To support this, a completely new set of sector formats were introduced. Previously, sectors were either mode 0 (audio), or mode 1 (data). Now Mode 2 sectors were added in two different organizations: form 1 and form 2. Mode 2 form 1 sectors were just like the previous mode 1 data sectors with the exception that they included eight bytes of “header” information intended to identify the type of sector and the stream it belonged to. Mode 2 form 2 sectors were intended for multimedia content, usually video, where the error correction space was replaced by additional data space.

This ushered in a new series of applications for CDs, most notably the VCD or Video CD. This is a disc format where MPEG-1 video is stored on a CD using Mode 2 Form 2 sectors. With quality about the same as VHS this allows 60 minutes of video to be played from a single CD. This format was extremely popular in Asian countries where there was little penetration of DVD players until very recently. Instead, VCD players were available to play these discs and it was common to find shops with large numbers of two-disc sets for commercial movies.

Another application using CD-XA discs was the original Kodak PhotoCD architecture which stored multiple resolutions of photos on CD-XA discs. The reason for them being CD-XA was simply that multiple sessions were being used so a disc full of photos could be added to. Originally, multiple sessions were restricted to CD-XA format discs but this restriction was quickly removed and by 1994 all CD-ROM drives could read multisession discs without the CD-XA requirement. Today, nearly every photo processing facility can produce a disc with photos on it but these are a single resolution copy of each picture and do not follow the PhotoCD standard.

The fact that there was no error correction for this video data wasn't a major problem. At 24, 25 or 30 frames per second a single error would appear only as a brief flash on the screen at worst.

From a data hiding perspective, unless a program is using special commands to read the disc, a mode 2 form 1 disc appears identical to mode 1 – only the data is read. This means there is eight bytes available in every sector for other purposes. On a disc with 360,000 sectors on it this provides 2,880,000 bytes of data which is invisible – if you do not think to look for it or know it is there. It is rather fragmented and it is necessary to piece the 8-byte segments of data back together to have something usable, but it is utterly transparent and invisible.

A disc can be written using both mode 2 form 1 and form 2 sectors and this is the common way for a VCD or other disc containing multimedia content to be written. Mode 2 form 2 sectors cannot be read using ordinary commands because these sectors do not have the error correction information that is expected. However, should a mode 2 form 2 sector be attempted to be read the drive will simply return a read error the same as if there was damage or dirt on the disc. In most cases this will result in a disc simply being put aside and not examined further.

To write a disc containing mode 2 form 1 sectors with specific data in the sector header field it is necessary to utilize a “raw” disc image where the disc image is constructed and then the sector header information is overwritten with the data to be hidden in this manner. This is fairly complicated and probably is best done with some kind of specific program or script. Once the disc image has been altered, almost any “raw” image writing tool will be able to write the modified image to a disc. Today it is less common for CD and DVD writing software to support creation of multimedia discs other than VCDs. There are a few programs out there available for free downloading which will write discs with mode 2 form 2 sectors and these can be used to write any sort of data to discs.

## ADDITIONAL SUBCHANNELS ON CDS

Hard disks, thumb drives, SSDs and floppy disks all share the commonality that to the host computer they contain a single-dimensional structure of sectors that are either 512 or 4096 bytes in length. There is no other data on the disk other than perhaps some kind of control information. This is also the way DVDs and DVD-like discs (such as DVD HD and Blu-Ray) work, although with 2048 byte sectors.

DVDs do have some additional data known as the table of contents or TOC. This is simply a list of pointers to the beginning of sessions on the disc.

CDs, however, are different. There is a TOC, but there is also quite a bit more information that can be stored on a disc. The first thing of importance is that sectors can contain 2048, 2056, 2336, 2352 or 2448 bytes, depending on how the sector is being used. Several of these formats have additional data in parallel with the 2048 bytes of user data in each sector. This means that there can be the usual 2048 byte sector full of ordinary data with other data not as easily accessed but present and isolated from the 2048 bytes. The sector formats containing 2058 and 2336 bytes were previously described under the CD-XA heading.

CD technology was developed in the late 1970s and the first CD patents date from 1980. It took until 1982 for the first consumer audio CD players to reach the marketplace. At this time all CDs were for music and music alone. Music is stored in what are called “subcode blocks” which are really the parent structure for data sectors. Each subcode block can be treated as a data sector which holds 2352 bytes in audio samples with no error correction or error detection information. It took until about 1994 until CD-ROM drives began to commonly read audio tracks as data using special commands, but once that was done music CDs became easily copyable by anyone with a CD-ROM drive that supported such reading. Before that time there was no good way for the average person to digitally copy music from a CD.

It wasn't until 1985 or so that data was being placed on CDs and not until 1987 until the first standards appeared for representing files on a CD-ROM. The arrangement for putting data on a CD included substantial error correction and detection capabilities and utilized nearly 11% of the space in a sector for this purpose. Because of this, even with the expectation that there would be errors reading the data, the correct data was usually recoverable in the drive before sending it to the host computer. This is the origin of the 2048-byte data sector on optical media. The basic design of music CDs included some extra space that was not originally utilized but was intended for extending the music listening experience. One of these was Karaoke, which required the display of information, generally text, in addition to the playing

of the music. It is not clear when the first Karaoke CD players emerged, but the standards for doing this came out in the early 1980 with, according to Wikipedia the first disc using this standard being released in 1985. It turns out that in parallel with the audio samples a subcode block could store 576 bits of additional information, usually organized as 96 characters with 6 bits each. This information can follow a standard for drawing graphics on a TV screen with a resolution of 300x216 and 16 colors. A CD+G (named from CD plus Graphics) subcode block can be read by a supporting drive as 2352 bytes of audio samples plus 96 bytes of this additional information for a total of 2448 bytes. It turns out that the additional information, which is stored in the subcode channels R through W, can also be written with data sectors.

Information in the R-W subchannels is completely separate from the ordinary audio or data on the disc. There is no operating system support for accessing this data and it can only be read using special applications or optical media tools. It is possible to have a disc containing something innocuous, such as an installation of some software, and have something completely hidden in the R-W subchannels.

By utilizing the R-W subchannel space to store either 96 6-bit characters or 80 8-bit characters per sector this provides 207 million bits or 25,312KB of additional, hidden data storage on a full disc.

To store data using the R-W subchannels it is necessary to rearrange it so as to fit the 96 6-bit character arrangement and then distribute it into a disc image that has been collected as "raw" sector data with R-W subchannels. This is best done with some kind of programming tool, but it isn't all that complicated to do. It is just a matter of reading in an existing disc image sector by sector, modifying it and writing it back out. The disc image file can then be used to burn a new disc.

Understand that because placing data in either the R through W subchannels or in the Mode 2 eight bytes for stream id and type is completely transparent, it would be possible to have discs manufactured with this information in them. The final product could be music, video or data and there is no way to tell. Distributing such discs would be really no risk at all because nobody is going to find the hidden data unless they are looking for it.

If someone hands you a disc and you see nothing unusual on it, it just might have data stored in the R through W subchannels or in the 8 bytes for the stream id and type. If there is, you probably aren't going to find it without spending a lot of time seeing if there is anything there and trying to piece it back together if it looks like there might be something there. Because of the time required and the fact there are virtually no tools other than the most basic for accessing this information, it is very, very likely that whatever might be hidden there will remain hidden for all time.

## SUMMARY

If you are looking to keep some data secret and hidden away, encryption is one possibility but one that shouts out to the world "I've got a secret!" If you are looking for a far more subtle alternative, optical media has many ways of both physically and logically hiding information that may never occur to anyone not familiar with the differences between optical media and hard drives.

If you are a forensic examiner you should at least have a cursory understanding of how optical media is different and that really hiding data is possible. Then at least you will not be fooled by some of the simple tricks described here. Of course, if you are faced with some of the more complicated techniques nothing but a deep understanding of optical discs and a lot of time is going to help ferret out hidden data.

Fortunately for everyone in the forensic community, the number of times you might encounter something like this is very small. Most people have only a very limited understanding of what has been described here and using these techniques would make their data too hard to access on a daily basis. But one day you may be faced with a more sophisticated user with the goal of making sure the information they are transporting cannot be found. Hopefully, this article has given you some insight in you will be prepared for such an event.

## ABOUT THE AUTHOR

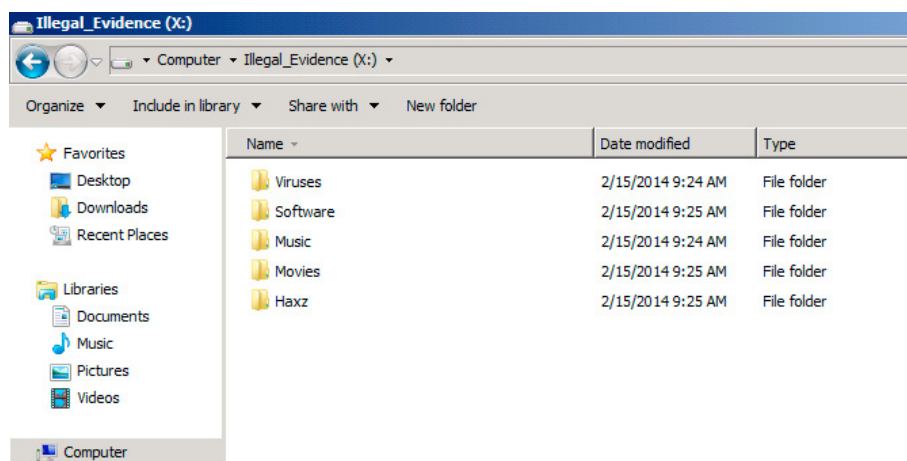
*Paul Crowley is a Founder and President of CD-ROM Productions, dba InfinaDyne. He is a Software publisher supplying consumers, government and law enforcement. He is Developing software since 1974 and a principle in a software company since 1992. Paul Crowley is a published author of the book CD and DVD Forensics. He is a Regular attendee at major US forensic trade shows.*

# EXAMPLE OF MANIPULATING A GRACEFUL SHUTDOWN TO PREVENT EVIDENCE RECOVERY

by Lance Cleghorn, M.S.

When responding to a computer incident, many technology professionals feel compelled to shut down the computer in question through a graceful shutdown rather than remove power from the system and risk data corruption or loss of volatile data not committed to permanent storage. The operating procedure of completing a graceful shutdown has a myriad of vulnerabilities that could be utilized by the system owner or a third party actor to disrupt or destroy evidence and prevent forensic recovery. Removing the power from the system while running presents a far smaller risk than attempting to gracefully shutdown a system that the incident responder can never fully guarantee is under their control and impervious to sabotage.

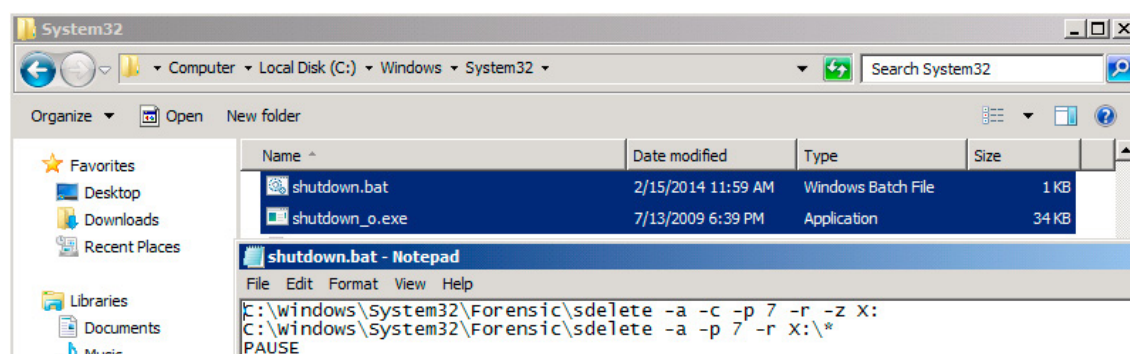
Many systems administrators and technology professionals would be cautious to simply remove the power from a running system. A well trained incident responder on the other hand will prioritize the collection of vital data for the forensic examiners. There is the distinct possibility that in many smaller organizations the first line incident responder may also be the system administrator. This paper aims to aid those professionals who may find themselves torn between their duty as an incident responder and as a systems administrator, by showing that once a system is involved in an incident it can no longer be trusted.



**Figure 1.** Example Drive Containing Evidence

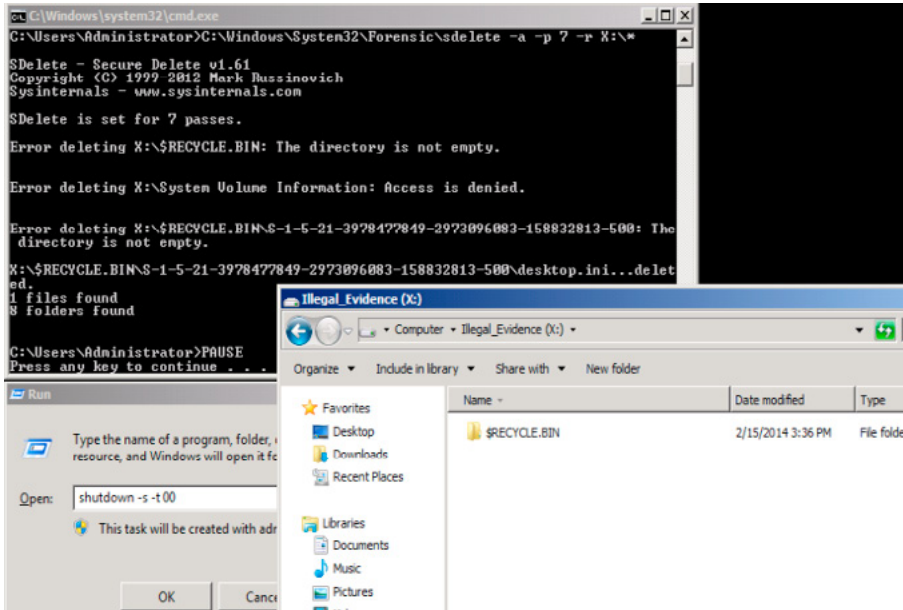
## MANIPULATING THE SHUTDOWN COMMAND

Even a user with little to no advanced training could easily implement a logic bomb script to destroy data like the incriminating folders and files shown in Figure 1. For example, the shutdown command in the system directory could be renamed and replaced with a batch script designed to forensically wipe incriminating data. Figure 2 shows an example of a script that could be used as a replacement for the shutdown command in the system directory. This example script uses Sysinternal's SDelete utility to forensically wipe the free/slack space on a partition and then remove all files and folders with seven passes of garbage data. [5] Once the script is added to the system directory using the shutdown name, any use of the command in the run dialogue, or through a command prompt will not call the Windows shutdown command but rather the script shown in Figure 2.



**Figure 2.** Replacing the Shutdown Command [5]

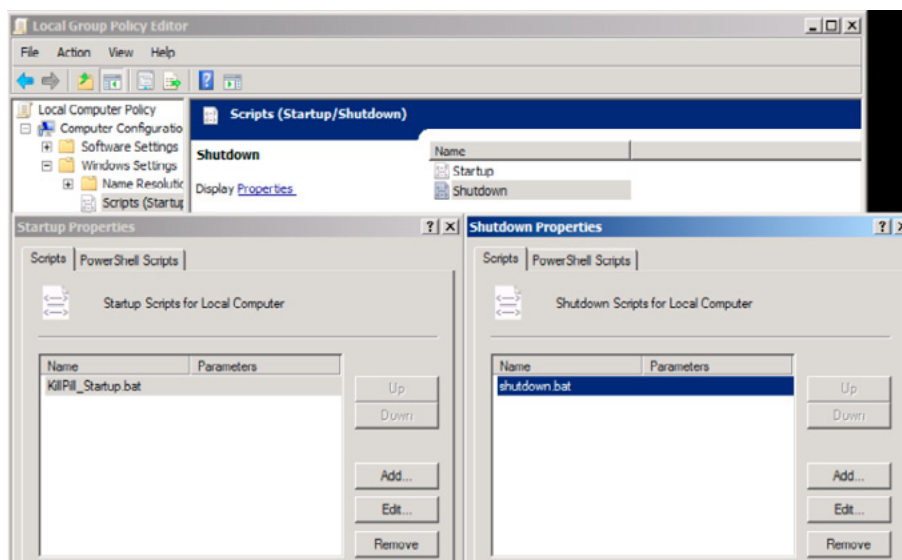
When an incident responder or an investigator attempts to shut down the system Figure 3 shows the unintended consequences of having the Illegal Evidence drive wiped clean using SDelete. [5] The responder may have only intended to gracefully shut down the system and reduce the risk of system corruption; however, they have now wiped out all the evidence that would have been vital to investigators and prosecutors. This script could be further refined to launch the SDelete command in a minimized window and then call the renamed shutdown command in an effort to subvert detection by the responder. [5] Simple trapping like replacing the shutdown command is something that incident responders are trained for and anticipate. To avoid this many incident responders leverage a trusted tool set. Even with a trusted tool set, an incident responder should still be wary of executing a graceful shutdown.



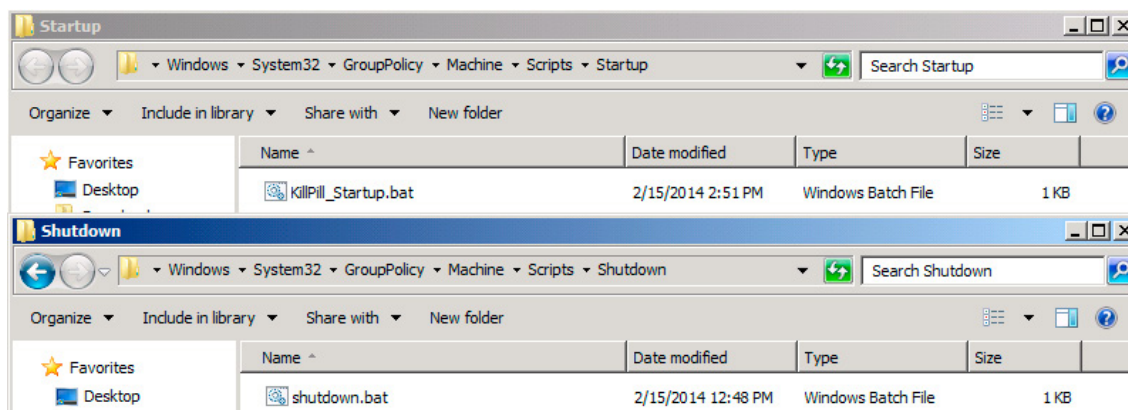
**Figure 3.** SDelete Forensically Wipes Evidence Drive [5]

## USING GROUP POLICY TO DESTROY EVIDENCE

To demonstrate how the operating system can be used to circumvent an incident responder's trusted tools, a series of batch scripts will interact through Windows group policy to destroy and obfuscate evidence. [3] Batch scripting and group policy are one way to circumvent trusted tools; however, other methods such as registry manipulation and visual basic scripting would be similarly effective. Figure 4 shows how using the local group policy editor a malicious actor could define scripts that will be run at startup and shutdown. [3] Implementing scripts through the group policy context is particularly concerning for an incident responder attempting a graceful shutdown because the shutdown script will run regardless of the method used to trigger the shutdown. Figure 5 shows the actual folders that contain the startup and shutdown scripts. The malicious actor would have to have a defined local Group Policy Object (GPO) in order for the script to execute, though once the GPO is defined the script may be manipulated in any way so long as the name is preserved. [3]



**Figure 4.** Local Group Policy Editor Startup/Shutdown Scripts [3]



**Figure 5.** Folders Containing the Startup/Shutdown Source Scripts

**Listing 1.** Malicious Startup Script that Populates a Shutdown Script [1,4,5]

```
Echo REM Wipe Encrypt Shutdown Script Active > C:\Windows\System32\GroupPolicy\Machine\Scripts\
Shutdown\shutdown.bat
Echo C:\Windows\System32\Forensic\sdelete -a -c -p 7 -r -z X: >> C:\Windows\System32\GroupPolicy\
Machine\Scripts\Shutdown\shutdown.bat
Echo C:\Windows\System32\Forensic\sdelete -a -p 7 -r X:* >> C:\Windows\System32\GroupPolicy\Machine\
Scripts\Shutdown\shutdown.bat
Echo START /WAIT C:\Windows\System32\Manage-bde -on X: -RecoveryPassword >> C:\Windows\System32\
GroupPolicy\Machine\Scripts\Shutdown\shutdown.bat
Echo C:\Windows\System32\Manage-bde -lock X: >> C:\Windows\System32\GroupPolicy\Machine\Scripts\
Shutdown\shutdown.bat
Echo exit >> C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown\shutdown.bat
```

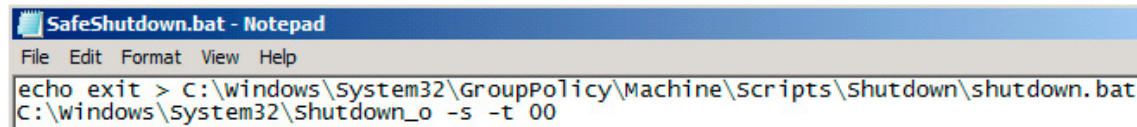
In this particular example a startup script named “KillPill\_Startup.bat” uses the *echo* command to populate the contents of the shutdown script which is aptly named ‘shutdown.bat’. Listing 1 shows the contents of “KillPill\_Startup.bat” the script itself begins by echoing a comment using the > redirect to clobber the current contents of the ‘shutdown.bat’ script. The subsequent lines use the >> redirect to append SDelete commands and commands using the Manage-bde utility which manipulates BitLocker drive encryption. [1,2,5] Note the use of the *START* command in line 4 of the script which will be discussed shortly. [4] Line 6 shows the full path to the “shutdown.bat” script which is cropped out of the other lines to keep the figure concise. After the “KillPill\_Startup.bat” script has been executed the “shutdown.bat” script will resemble Listing 2 with the notable change from the *exit* command to *PAUSE* which enables us to review the script’s output that would normally be discarded when the command window closes.

**Listing 2.** Armed Malicious Shutdown Script [1,4,5]

```
REM Wipe Encrypt Shutdown Script Active
C:\Windows\System32\Forensic\sdelete -a -c -p 7 -r -z X:
C:\Windows\System32\Forensic\sdelete -a -p 7 -r X:*
START /WAIT C:\Windows\System32\Manage-bde -on X: -RecoveryPassword
C:\Windows\System32\Manage-bde -lock X:
PAUSE
```

A clever malicious actor would not be content with having their illegal and incriminating content destroyed at every graceful shutdown, which is where the “SafeShutdown.bat” script shown in Figure 6 becomes particularly useful. This script uses the *echo* command with a > redirect to clobber the malicious contents of the armed “shutdown.bat” script. The “SafeShutdown.bat” script then uses calls the renamed “Shutdown\_o.exe” shutdown command from the system directory. “KillPill\_Startup.bat” then rearms “shutdown.bat” during the Windows operating system startup routine. This method allows the malicious actor to still preserve normal use of their system and ensure their illegal content is safeguarded. If an incident responder tries to initiate a graceful shutdown, even with a trusted tool,

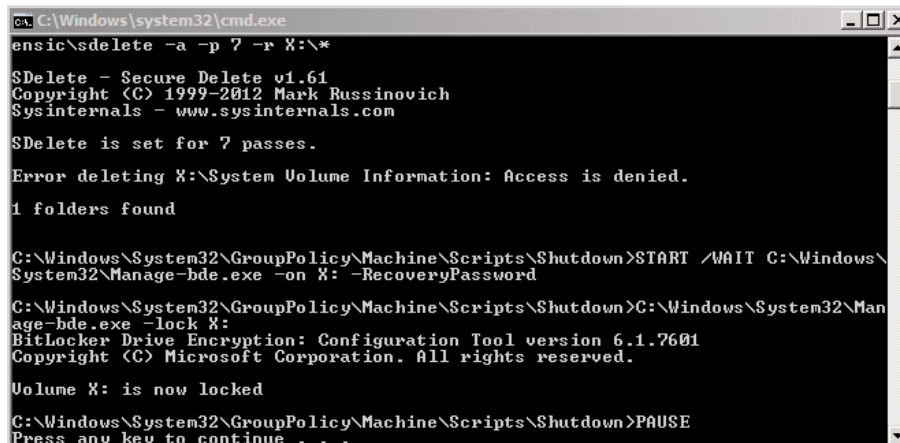
the armed 'shutdown.bat' script will execute during shutdown after the Windows splash screen has opened, thus obscuring the malicious script running in the background.



**Figure 6.** Disarming 'Safe' Shutdown Script

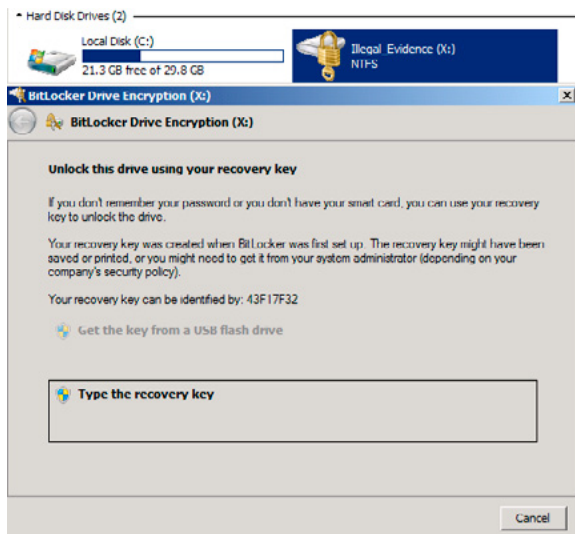
## FORENSIC DESTRUCTION AND EXAMINATION

Figure 7 shows the results of having the armed version of "shutdown.bat" run. The tail end of the SDelete commands are visible at the top and towards the bottom are the Manage-bde commands that manipulate BitLocker disk encryption. [1,2] In the command line that begins with the *START* command Manage-bde is used to turn encryption *on* for the Illegal Evidence drive X: shown back in Figure 1. [1,4] The *RecoveryPassword* switch creates a numerical key that allows the drive to be locked and unlocked, this switch pairs particularly well with the *START* command that opens the line in a separate command window. When the command that follows *START* is executed using the *WAIT* switch, the parent script waits for the particular command line to complete execution and close. For this line the output containing the *RecoveryPassword* is displayed in this window that immediately closes, thus destroying the numerical recovery key and preventing decryption. [1,4] A malicious actor might find this particularly appealing because they cannot possibly know the decryption key and cannot be ordered to divulge the information they do not know. The line following the *START* line locks the drive implementing the encryption solution and permanently renders the evidence unrecoverable. [1,4]



**Figure 7.** Scripted SDelete and BitLocker Drive Encryption [1,4,5]

A forensic technician attempting to recover the data at a later point would be presented with a screen similar to Figure 8. This figure shows the golden lock on the X: drive and BitLocker requesting the Recovery Key that was discarded by the *START* command when it completed execution. [2,4] The entire process of encrypting the drive would take an abnormally long time, especially in a drive of substantial size, and the incident responder may pull the plug prior to the full encryption taking place; however, a considerable amount of evidence could have been destroyed and a lawyer may be able to call into question the validity of the remaining data.



**Figure 8.** Encrypted and Locked Evidence Drive [2]

## CONCLUSIONS

Many incident responders are not formally trained; rather they are systems administrators who are required to perform incident response as an additional duty. A systems administrator would balk at the idea of removing power from a system by pulling the plug, but a well-trained incident responder may be required to consider the underlying implications of either course of action. Considering the incident responder is tasked with securely taking control of a system that they in reality have no way of fully understanding, the option of removing power may be the preferred course of action. Even when tasked with collection of volatile data, the incident responder should fully understand the operating system they are interrogating and watch for signs of destructive activity. The incident responder is the first line of defense against evidence destruction and they must ensure that the forensic examiner is given as much of the original evidence as possible. Part of this responsibility should revolve around knowing when to bypass a graceful shutdown in favor of removing power from the system.

## REFERENCES

- [1] Microsoft Corporation. (2013, August 21). Manage-bde. Retrieved from Microsoft TechNet: <http://technet.microsoft.com/en-us/library/ff829849.aspx>
- [2] Microsoft Corporation. (2014). BitLocker Drive Encryption. Retrieved from Windows: <http://windows.microsoft.com/en-us/windows7/products/features/bitlocker>
- [3] Microsoft Corporation. (2014). Group Policy. Retrieved from Microsoft TechNet: <http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx>
- [4] Microsoft Corporation. (2014). Start. Retrieved from Microsoft: <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/start.msp?mfr=true>
- [5] Russinovich, M. (2013, January 11). SDelete v1.61. Retrieved from Windows Sysinternals: <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>

## ABOUT THE AUTHOR



Lance Cleghorn A North Carolina native received a Bachelor of Science degree in Information Technology from East Carolina University. Graduating Suma Cum Laude Lance completed his undergraduate degree in 2012. As an undergraduate student Lance concentrated in Cisco networking technology. Lance was awarded a Master of Science in Information Security from East Carolina University in 2013, and has been published in PenTest Magazine and the Journal of Information Security. Lance holds several major industry certifications including the Associate of ISC2 towards a CISSP, CCNP, CompTIA Security+, EMCISA, and MCP. E-Mail: [CleghornL08@Outlook.com](mailto:CleghornL08@Outlook.com)  
LinkedIn: [www.linkedin.com/pub/lance-cleghorn/7a/393/86a/](http://www.linkedin.com/pub/lance-cleghorn/7a/393/86a/)

# A GENERAL APPROACH TO ANTI-FORENSIC ACTIVITY DETECTION

by Joshua I. James, Moon Seong Kim, JaeYoung Choi, Sang Seob Lee, Eunjin Kim

Digital forensic investigators and academics alike have long been discussing the potential implications of anti-forensic techniques on investigations. The actual use of anti-forensic techniques and the effect on investigations, however, is difficult to quantify. Indeed, there are some cases where what could be classified as anti-forensic techniques were blatantly used. For example, a criminal who accessed celebrity email accounts normally used a VPN/proxy specifically to hide his IP address from investigators (Daily Mail, 2011). However, by failing to use such techniques once, that gave investigators enough information to find his location. Similarly, Casey et al. (Casey, Fellows, Geiger, & Stellatos, 2011) gave a number of examples where full disk encryption either prevented further investigation, or proved to be a difficult obstacle to acquiring evidence.

## What you will learn:

- In this article you will learn about general types of anti-forensics with examples. A number of works dealing with the detection and implications of anti-forensics in digital forensics investigations will be discussed. We will then give a relatively simple method for investigators to build signatures of anti-forensic tools that may be used for automated anti-forensic trace detection.

## What you should know:

- 82% of surveyed investigators claimed to have encountered some form of anti-forensics during their investigations
- Slightly over half of surveyed investigators use automated anti-forensic detection tools
- Anti-forensic activities may create detectable action-traces in a suspect system
- Naive anti-forensic detection methods can be applied regardless of operating system

The challenge with detecting anti-forensic techniques is largely a challenge of the digital investigation process itself. Not only is the investigator normally working with a limited state of the system, but he or she must also contend with the trade-off between the depth of investigation and length of time an investigation takes. To cope with the challenge of time, interviewed investigators have been shown to normally examine a suspect system, and look for anything

‘unusual’ that might hint at anti-forensic techniques (J. I. James & Gladyshev, 2013). Further, they would conduct a ‘social analysis’ to determine if it was likely that a suspect had the technical knowledge to implement such techniques. Using their *experience* if something felt ‘off’ with the suspect system, they may attempt to conduct a more in-depth analysis specifically focusing on anti-forensics. However, if nothing unusual was found, the search would be abandoned relatively quickly since it is unknown whether evidence of anti-forensics actually does exist. Most of the investigation techniques discussed in the study, however, were highly manual processes. Essentially, if no evidence of anti-forensic techniques was found via a high-level analysis of a suspect system, investigators did not appear to feel justified in spending the time to do a more in-depth investigation.

In a survey of the Korean National Police involved in cybercrime investigation (“[BoB] Indicators of Anti-Forensics Investigator Survey (Korean),” 2013), 82% [n=11] of respondents claimed to have encountered some form of anti-forensics during their time as a digital forensic investigator. Instead of only manual anti-forensic trace investigation, 55% [n=11] of respondents claimed to use some form of anti-forensic detection tool. Despite the fact that not all investigators are using anti-forensic detection tools, 100% [n=11] respondents believe there is a need for more-advanced anti-forensic detection tools. Investigators primarily claimed that detection should focus on whether anti-forensic tools exist(ed) on the suspect system, and to what extent they had been used, e.g. installation only, portable, running, uninstalled, etc.

The first challenge with detection of ‘anti-forensic’ techniques and tools, however, is to understand what exactly anti-forensics is. A number of works have proposed definitions of anti-forensics, however, Harris gives one of the most comprehensive discussions on the topic, eventually defining anti-forensics as “any attempts to compromise the availability or usefulness of evidence to the forensics process” (Harris, 2006). Other definitions were given prior to this, but – as Harris points out – they focused on specific segments of anti-forensics. Harris’ definition may be suitable for a general understanding of anti-forensics, but gets us no closer to understanding different types of anti-forensics and their nuances.

A number of works have given overviews of anti-forensic techniques from a technical perspective (Garfinkel, 2007; Hilley, 2007), that included some categorization and technical description about the features of different categories. However, one of the most widely-accepted anti-forensic classification models was given by Rogers (Rogers, 2005). This model defined anti-forensic categories as data hiding, artifact wiping, trail obfuscation and attacks against computer forensics.

In the prior surveys, it is unclear what categories of anti-forensics techniques investigators are encountering more. Different techniques appear to be specific to the type of crime under investigation and the technical ability of the suspect (Casey et al., 2011; J. I. James & Gladyshev, 2013). For example, in child exploitation material (CEM) cases, attempts at ‘artifact wiping’ appear to be common, as are some types of rudimentary ‘data hiding’. In fewer cases, advanced data hiding and trail obfuscation may take place. Regardless of the type of crime, multiple categories of anti-forensics may be employed, each of which will be discussed in more detail. Data hiding is any attempt to make data or information difficult to access. Rogers defines sub-categories of data hiding as rootkits, unusual places, encryption and steganography.

A number of works have demonstrated rootkit concepts that are excellent for data hiding (Rutkowska, 2006; Thompson & Monroe, 2006). Some of these are potentially detectable within the operating system, with others (such as those similar to Blue Pill and SubVirt) may be difficult, or even impossible, to detect within the live system. Rootkits may be resident in memory only, they may create their own encrypted partitions on the disk, and may use many other approaches for data-hiding and persistence.

A more commonly-encountered method of data hiding seen by investigators is hiding data in ‘unusual places’. The usual suspects are memory, slack space, host protected area (HPA), hidden directories, meta-data modification, bad blocks, alternate data streams, hidden partitions, and many more (Huebner, Bem, & Wee, 2006). Investigators often claim to find nested directories several layers deep that may then contain relevant information. Many digital forensic investigation tools can handle most of these known challenges. For example, simple keyword or hash-based searches may find data using naïve hiding techniques. More advanced data hiding requires specialist tools, such as The Sleuth Kit’s ability to detect and remove HPA (Carrier, 2005). Likewise, some data discovery may require tools with different processing approaches, such as bulk extractor (Bradley & Garfinkel, 2013), which analyzes features of a suspect disk rather than parsing the file system(s) like many common digital investigation tools.

Much discussion and concern has been raised over the topic of encryption. Casey, et al. (Casey et al., 2011) argue that full disk encryption is a growing problem, and that legal and tactical approaches need to be developed to be able to handle the acquisition of data from live systems that are using disk encryption technologies. While encryption is sometimes encountered, and may have a drastic affect on the outcome of a case, many investigators in Ireland and South Korea claim that encryption is not yet encountered in the majority cases. Just like other forms of anti-forensics, however, it is unclear if encryption is not being used, or if it is not being detected. Certainly, disk encryption is becoming more available, with most major operating systems supporting some form of disk encryption. Further, many consumer computers also support hardware level disk encryption. These solutions, combined with easy-to-use encryption tools, such as TrueCrypt, give consumers many options for implementing encrypted storage. So far, however, many suspects are either not implementing encryption or are implementing it poorly/incorrectly, giving investigators the possibility to recover some – if not all – of the encrypted data.

Steganography is essentially hiding information within information. In digital investigations, the common example is hiding digital pictures, text or other documents within digital pictures, video, music files, etc. It could be used, for example, to attempt to hide CEM within an adult pornography collection, or to covertly send messages by embedding the message in a picture file and posting the picture in a public forum. Steganography in the wild is difficult to detect. While techniques to detect steganography are continually being developed, so too are the techniques to hide data within data more effectively. In terms of steganography detection on a suspect system, however, a number of tools have been developed to help investigators in post-mortem forensic investigations.

One tool, named FAUST, specifically targets traces created by specific anti-forensic tools within a suspect system whenever the tool is ran (Zax & Adelstein, 2009). They found that roughly half of the programs examined left behind traces in the suspect system. Instead of examining traces created by the steganography tools themselves, other methods attempt to detect if a file contains hidden data. Stegdetect, a popular steganography detection tool was found to have a high false positive rate (Khalind, Hernandez-Castro, & Aziz, 2013), which attests to the difficulty of steganography detection, even with known algorithms. Luckily for investigators, traces of steganography tools on a suspects system combined with steganography detection tools can, at least sometimes, point an investigator to suspicious files that potentially require more attention.

A commonly encountered method of anti-forensics is artifact wiping. It could be as simple as the user intentionally deleting files, or as complex as overwriting file data to make it difficult or impossible to recover. Many easy to use computer cleaning programs exist for all major operating systems. Indeed, such programs can have legitimate uses, such as freeing disk space. Many times, however, such programs are used to attempt to remove traces of criminal activity from the system. These tools, however, are not perfect. Geiger (Geiger, 2005) found that many anti-forensic tools did not completely remove all data, some data may still be recoverable, and the tools themselves sometimes created traces that may be used to understand what data was removed and when. Very basically, actions in a computer system generate a number of related traces, and complete deletion of all traces is difficult. Some methods, such as non-persistent virtual machines or operating systems of live CDs may result in no persistent traces being created. While this challenge has been discussed by investigators and academics, it does not appear to be of great concern. Again, the problem may exist, but is not being detected.

An example of trail obfuscation has already been given, where a criminal attempts to hide his or her location. This is normally done through a VPN or proxy service to attempt to make the source look like a different location. A suspect could also easily change his or her IP/MAC addresses to attempt to disguise their location or system. More advance methods use malware-infected computers to relay network traffic. Rogers (Rogers, 2005) also claims that log cleaners or even “misinformation” is used to attempt to obfuscate the trail. Indeed, if an attacker is aware of logs that are created because of their actions, modifying such logs may lead investigations down a wrong path if the logs are not verified. The use of trail obfuscation very much depends on the type of crime being committed. In this area too, obfuscation programs are becoming easier to use. For example the Tor and FreeNet networks have relatively simple user interfaces, and easy to follow instructions. While these systems are not without fault, they can make investigation of suspect activities more difficult.

Rogers' final category of anti-forensics are attacks against computer forensics. This method of anti-forensics attempts to attack the forensic investigation process. Since digital investigation relies on relatively

standardized processes, and most investigators use a small set of well-known tools, the tools themselves can be targeted to attempt to alter the reliability of the digital investigation process. Again, attacks against tools are not commonly reported by investigators, but some attacks do exist and all forensic investigation tools are theoretically vulnerable to such attacks.

Rogers makes the point that all of these categories of anti-forensics are not new. Many anti-forensic techniques that are used have been around a long time. In some cases, such as artifact wiping, it can be very easy to see if anti-forensics has been used. In other cases, however, detection can be much more difficult. What is known is that anti-forensics often relies on particular tools either directly or indirectly. This means that traces of such tools may be resident on a suspects system, as has been shown by Geiger (Geiger, 2005) and Zax & Adelstein (Zax & Adelstein, 2009).

Based on the previously discussed survey results, there is a need for an easy to use anti-forensic detection method to help an investigator quickly determine to what extent anti-forensic techniques may have been used on a suspect system. A relatively easy way for investigators to detect potential anti-forensic tools is by the traces that are created in the suspect system. For this reason, we recommend the creation of anti-forensic activity 'signatures', similar to those proposed by James, et al. (J. James, Gladyshev, & Zhu, 2010). Such signatures are more generic than those proposed by Zax & Adelstein. Instead of detecting signatures related only to the execution of particular tools, this method could also capture traces created by user activities where no specific tool is involved. The reconstruction of user activities using Windows Restore Point analysis, for example was given in Zhu, et al. (Zhu, James, & Gladyshev, 2009). Using this method, user actions such as website or command line activities could be reconstructed for a longer period of time than only looking at the final state of the system.

For this method, first we define a *signature* as a list of traces created in a system that are associated with a particular anti-forensic tool or technique. For example, when running an anti-forensic tool in a Windows system, a number of data sources, such as file content or meta-data and Registry entries may be updated. A signature is the collection of these updates, where each update constitutes one 'trace'.

A signature can be created by either 'snapshot analysis' or 'real-time monitoring'. Both methods could potentially be automated. In this work we will discuss real-time monitoring of a Windows system to determine traces related to an anti-forensic tool or technique. When the anti-forensic technique is executed by the suspect, a number of traces will be created in the suspect system depending on the objective of the technique. Traces could be updates to the Windows Registry, file contents, file meta-data, system logs, etc. Real time analysis can determine the files and Registry entries that are updated, but how such files and Registry entries are updated need to be specifically explored. Signatures of anti-forensics tools and techniques can be created using the following method:

- Create test system (Virtual Machine),
- Run file system logger (Process Monitor),
- Execute desired action (in test system)
  - Install
  - Run/Execute Anti-Forensic Technique
  - Uninstall
- Save file system logger output
- Filter log to reduce noise
- Extract usable unique signature
- Define traces in resulting signature as regular expressions for portability

Because such a method is generic, it can be used for any operating system. The creation or selection of a file system logger will determine how specific the signature is. Further, each action could potentially be detected to determine if a unique signature exists for such an action. In this case, the installation, execution and uninstallation of an anti-forensic program was selected. However, any action could potentially be modeled in terms of its underlying trace creation. For example, a user using a hexadecimal editor to modify a file header could be modeled using such a method.

We have had good success using Process Monitor (procmon) in Windows systems to monitor file system and Registry updates. A snapshot of the 'clean' system is created for easy system rollback after testing. Normally the test system has little, if any, non-default software installed.

The monitoring program is first used to create a baseline system activity log. Monitoring is enabled on the system for a selected period of time with no user activities running. The result is a log of system activities that can be considered as noise. The 'noise' log, should be saved for later use. Once a test system has been created, the action to test must be determined. In this case, the focus is on anti-forensic programs. In our case, signatures will be created specifically for the actions install, run/execute, and uninstall (where the anti-forensic tool can be installed/uninstalled). If the program was 'portable' or does not need to be installed, then install and uninstall will be skipped.

For each selected program, the file system (and Registry) monitor should be started, and each action relating to the specific program should be executed. After each action is executed, the monitor should be stopped, the log exported, and the log buffer cleared. Monitoring should be started again, and the next action in the sequence would be executed.

After all actions in the sequence are executed, and logs collected, the test system (virtual machine) would be reverted back to the original snapshot. In our studies we completed this process five times per identified application. The resulting Process Monitor logs are a collection of XML files that should be named according to the analyzed anti-forensics tool, and the action that was recorded.

The result of the prior step is five logs per action per anti-forensic program. Filtering of the logs can be done to count the number of times a particular traces was updated for a given action. Traces that are not updated at least once per action can either be discarded (if you are looking for 'always updated' traces), or analyzed further to determine the relation between the action and the trace. In some cases, these traces may be very relevant to the action but only show up once because a random file name is used for the trace on each execution of the action. We also recommend removing traces from the list that also exist in the previously-created 'noise' log. Some common system files may contain content related to the anti-forensic action, but other 'noise' traces are likely updated too often to produce reliable information relating to the specific action.

Another level of filtering is to check the resulting list of traces against a system that has not had any anti-forensic actions executed. Any traces that are detected in the 'clean' system must be false positives. Again, this may be due to shared-log file content being updated. Once noise and false positives are removed, the result is a list of objects that are mostly unique to the specific anti-forensic action. However, they may not be completely unique to the action. Each trace may be updated by either another action relating to the same application, or may potentially overlap with other currently-unknown applications. For this reason, detection of traces in the signature are only indicators of anti-forensics, and must be investigated further if found. Such a signature, however, can provide a fast, relatively automated way to detect traces related to a wide verity of anti-forensic applications and techniques.

As discussed in prior work (J. I. J. James, Gladyshev, & Zhu, 2011; Kang, Lee, & Lee, 2013) some form of generalization of traces within signatures needs to take place to allow for detection on other systems. We use Regular Expressions to generalize variables in signatures. Regular expressions are used for fields that are likely to change depending on system settings, while keeping the path name as specific as possible to ensure only the identified trace is returned by the regular expression. This will enable the same signatures to be used on similar systems, however, it should be noted that signatures are likely to be different depending on the operating system, and perhaps even the version of the anti-forensic program.

Signatures for anti-forensic programs and techniques could enable knowledge sharing between investigators about new types of anti-forensic tools or techniques that they have encountered. Investigators could then essentially scan a suspect system with all known signatures to quickly return any traces known to be associated with anti-forensic tools or techniques.

Digital investigators, at least within South Korea, are encountering the use of anti-forensic tools and techniques. Although it is difficult to determine the extent of the problem, investigators do see a need for better detection when such techniques are used on systems under investigation. This work has described a basic method for generally identifying whether anti-forensic tools exist, and – in some cases – to what extent those tools have been used. By focusing on anti-forensic action trace detection, such a method can quickly give an investigator more information about suspect systems. This can help to ensure investigators are better informed about the potential state of a suspect device rather than forcing them to rely only on their intuition.

## BIBLIOGRAPHY

- [BoB] Indicators of Anti-Forensics Investigator Survey (Korean). (2013). CybercrimeTech.com. Retrieved from <http://www.cybercrimetech.com/2013/12/bob-indicators-of-anti-forensics.html>
- Bradley, J. R., & Garfinkel, S. L. (2013). Bulk Extractor User Manual (p. 57). Retrieved from [http://digitalcorpora.org/downloads/bulk\\_extractor/BEUsersManual.pdf](http://digitalcorpora.org/downloads/bulk_extractor/BEUsersManual.pdf)
- Carrier, B. (2005). Removing Host Protected Areas (HPA) in Linux. The Sleuth Kit Informer. Retrieved from <http://www.sleuthkit.org/informer/sleuthkit-informer-20.txt>
- Casey, E., Fellows, G., Geiger, M., & Stellatos, G. (2011). The growing impact of full disk encryption on digital forensics. *Digital Investigation*, 8(2), 129–134. doi:10.1016/j.diin.2011.09.005
- Daily Mail. (2011). FBI arrests man who hacked emails of more than 50 celebrities and stole nude photos from Scarlett Johansson. Daily Mail. Retrieved from <http://www.dailymail.co.uk/news/article-2048359/Scarlett-Johansson-nude-photos-hacker-Christopher-Chaney-arrested-FBI.html>
- Garfinkel, S. (2007). Anti-forensics: Techniques, detection and countermeasures. In 2nd International Conference on i-Warfare and Security (pp. 77–84).
- Geiger, M. (2005). Evaluating Commercial Counter-Forensic Tools. DFRWS, 1–12. Retrieved from [https://www.dfrws.org/2005/proceedings/geiger\\_couterforensics.pdf](https://www.dfrws.org/2005/proceedings/geiger_couterforensics.pdf)
- Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, 3, 44–49. doi:10.1016/j.diin.2006.06.005
- Hilley, S. (2007). Anti-forensics with a small army of exploits. *Digital Investigation*, 4(1), 13–15. doi:10.1016/j.diin.2007.01.005
- Huebner, E., Bem, D., & Wee, C. K. (2006). Data hiding in the NTFS file system. *Digital Investigation*, 3(4), 211–226. doi:10.1016/j.diin.2006.10.005
- James, J., Gladyshev, P., & Zhu, Y. (2010). Signature Based Detection of User Events for Post-Mortem Forensic Analysis. 2nd International ICST Conference on Digital Forensics & Cyber Crime (ICDF2C). Abu Dhabi, UAE.
- James, J. I., & Gladyshev, P. (2013). A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. *Digital Investigation*, 10(2), 148–157. doi:10.1016/j.diin.2013.04.005
- James, J. I. J., Gladyshev, P., & Zhu, Y. (2011). Signature Based Detection of User Events for Post-Mortem Forensic Analysis. *Digital Forensics and Cyber Crime*, 53, 96–109. doi:10.1007/978-3-642-19513-6\_8
- Kang, J., Lee, S., & Lee, H. (2013). A Digital Forensic Framework for Automated User Activity Reconstruction. In R. H. Deng & T. Feng (Eds.), *Information Security Practice and Experience* (pp. 263–277). Springer Berlin Heidelberg. doi:10.1007/978-3-642-38033-4\_19
- Khalind, O. S., Hernandez-Castro, J. C., & Aziz, B. (2013). A study on the false positive rate of Stegdetect. *Digital Investigation*, 9(3-4), 235–245. doi:10.1016/j.diin.2013.01.004
- Rogers, M. K. (2005). Ant-Forensics. In Lockheed Martin. San Diego, California. Retrieved from [http://cyberforensics.purdue.edu/documents/AntiForensics\\_LockheedMartin09152005.pdf](http://cyberforensics.purdue.edu/documents/AntiForensics_LockheedMartin09152005.pdf)
- Rutkowska, J. (2006). Subverting VistaTM kernel for fun and profit. In Black Hat Briefings.
- Thompson, I., & Monroe, M. (2006). FragFS: An Advanced Data Hiding Technique. In Defcon 14.
- Zax, R., & Adelstein, F. (2009). FAUST: Forensic artifacts of uninstalled steganography tools. *Digital Investigation*, 6(1-2), 25–38. doi:10.1016/j.diin.2009.02.002
- Zhu, Y., James, J., & Gladyshev, P. (2009). A comparative methodology for the reconstruction of digital events using Windows Restore Points. *Digital Investigation*, 6(1-2), 8–15. doi:10.1016/j.diin.2009.02.004

## ABOUT THE AUTHORS

Joshua I. James, Moon Seong Kim, JaeYoung Choi, Sang Seob Lee, Eunjin Kim [jijames@sch.ac.kr](mailto:jijames@sch.ac.kr), [kite0327@nate.com](mailto:kite0327@nate.com), [ebp@nate.com](mailto:ebp@nate.com), [gjwjqzz2@gmail.com](mailto:gjwjqzz2@gmail.com), [wormhole1313@gmail.com](mailto:wormhole1313@gmail.com)

Dr. Joshua I. James is a lecturer and researcher with the SoonChunHyang University Digital Forensic Investigation Research Laboratory, and a mentor for the KITRI (한국정보기술연구원) 'Best of the Best' information security education program. His research interests are in automatic event reconstruction, Law Enforcement process automation, investigation capacity and Mutual Legal Assistance relating to digital evidence. For more information on research and current projects, please see <http://CybercrimeTech.com>.

Jaeyoung Choi is enrolled in computer engineering at Inha University. He is active in the NewHeart, Inha University Computer Security Club. He participated in the Incognito 2013 Hacking Conference, where he specialized in ARM exploitation. He has worked on Information Security Management for Small Businesses through the Best of the Best v2.0 Information Security Training Program, as well as contributing to the Open Source 'Indicator of Anti-Forensics (IoAF)' project.

Lee Sang Seob is a Computer Engineering student at Sejong University. He was selected to take part in the KITRI Best of the Best v2.0 Information Security Training Program. He also works as a KISA Cyber Security Expert. Currently Lee Sang Seob is participating in Pwn&Play as a forensic analyst.

Eunjin Kim is student at Pukyong University. She has presented on 'Bittorrent's illegal issues and analysis' at KUCIS (Korea University Club of Information Security) and lead the Best of the Best v2.0 project 'Indicators of Anti-Forensics' (IOAF). She also presented this project at a Microsoft Security conference promoted by hackme and Seoul Women's University Information Security club.

# WHAT TO EXPECT WHEN YOU'RE ENCRYPTING

## CRYPTOGRAPHIC CHOICES FOR MAC AND WINDOWS

by **Eric Vanderburg**

Cryptography is an interesting field of study and it forms the basis of much of the communication the average person takes for granted as they use computers, networks and the Internet. Encryption is the process of making a message such as a data file or communication stream unreadable to anyone lacking the appropriate decryption key. Encryption uses mathematical formulas to modify the data in such a way that it would be extremely difficult to put back together without the key.

### What you will learn:

- How vulnerabilities were discovered and patches released historically
- How vulnerabilities are being sold on the open market
- Motivations for the sale of vulnerabilities

### What you should know:

- The impact the vulnerabilities market has on secure computing
- The value of a new information commodity
- Ethics of intentionally building vulnerabilities into software

The information is combined along with a different routine of information making it impossible for any user to decrypt unless the key and the routine are available. Encryption has been used for thousands of years. The Caesar cypher is a method of scrambling text by substituting one character for another. Other early encryption methods used transposition where the order of characters were changed. As encryption became more mature, transposition and substitution were used in increasingly complex ways. Today, encryption methods are so complicated that most encryption and decryption operations are performed by computer.

Computers also make it easier for end users and companies to encrypt data such as data on cell phones or personal computers. The forensic investigator must also be able to decrypt files in order to analyze them. Both Apple Macintosh (Mac) and Microsoft Windows machines come with built-in encryption and there are a variety of 3<sup>rd</sup> party applications used for encryption as well. This article explores these forms of encryption and how they differ as well as how the forensic investigator can decrypt these files to work on them.

### WINDOWS ENCRYPTION

There are two types of built-in encryption features available for Microsoft Windows machines. They are BitLocker Drive Encryption and Encrypting File

System (EFS). There are major differences between these features. While BitLocker assists the users in securing the files and folders available in the hard drive, Encrypting File System protects individual files. BitLocker is also used to secure removable drives and media. As such, the major difference between the functionality of the two standards is the way they secure the files in the drive. BitLocker secures drives and EFS secures files and folders within a drive.

Another major difference is that, BitLocker secures files irrespective of the users associated with it, which means that all the users associated with the computer can turn on/off this feature. But Encrypted File System uses individual accounts and permissions while encrypting files. Users can encrypt only those files that belong to them. BitLocker uses a special microchip, called Trusted Platform Module (TPM) which is hardwired to the motherboard of machines that require all advanced encryption features. But EFS does not require any such additional hardware. Moreover, only administrators have the right to turn on/off BitLocker advanced encryption features, but EFS does not require administrative permissions. All individual users can encrypt their files if needed. EFS security keys are stored in the operating system making it accessible to hackers who have skills and expertise in reading the source code of operating system. But BitLocker keys prevent the operating system itself from booting making it impossible for using the hard drive from a different computer. As individual users, you can use both BitLocker and EFS for added security.

### **BITLOCKER**

BitLocker supports hard drives for Windows Vista and other recent Microsoft Windows operating systems. If you are using Windows XP, Windows 2000 and 2003, you will not be able to use BitLocker. Even though BitLocker services are available for Windows 7 and later editions, Windows 7 Home and Professional users cannot use the functionality. BitLocker encryption is available in 128 bit or 256 bit modes. The difference between these modes is in the amount of data that is uniquely used to generate cypher-text blocks. The larger the blocks, the harder it is to detect patterns in the encryption and to break encryption keys.

a d v e r t i s e m e n t



## **Web Based CRM & Business Applications for small and medium sized businesses**

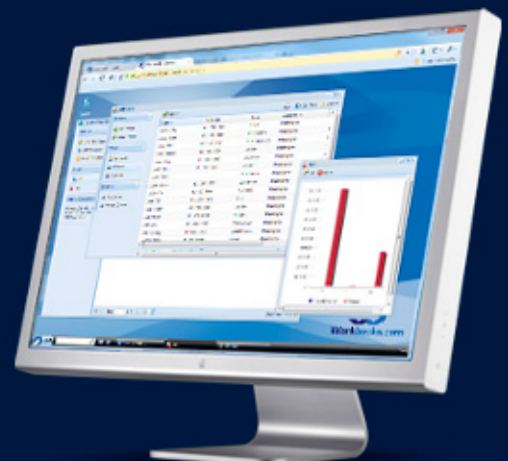
### **Find out how Workbooks CRM can help you**

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

**Contact Us to Find Out More**

+44(0) 118 3030 100

info@workbooks.com



There are two possible ways by which data on a BitLocker encrypted hard drive can be accessed offline. One way is to boot the system from another operating system and the other way is to use the hard drive in another machine. They are called offline attacks. BitLocker comes to your rescue in both the above hacking techniques. Since the entire hard drive is encrypted, both the above methods become useless and your data is protected. You may wonder if you can access your own data from another machine or operating system with such high end encryption techniques. Well, in such case, you will be sent a recovery key which can be used to access data. This ensures that, your data does not end up in wrong hands, but you need not work harder for accessing your data. An enhancement to BitLocker is BitLocker to Go, which can be used to encrypt files and folders in removable hard drives such as USB drives, thumb drives etc. The major factor that you need to consider is BitLocker cannot be enforced while the operating system is running. Since BitLocker can be used only for avoiding offline attacks, you need to rely on standard operating system security techniques in protecting your computer while it is running. The major attacks on your system during its running time may be from malicious users trying to access the machine either locally or using remote connection. In either ways, your operating system should provide you with strict user access permissions and password policy by which such attacks can be eliminated.

### ENCRYPTING FILE SYSTEM (EFS)

Encrypting File System (EFS) is relatively simpler and less effective than BitLocker, but it can be used to encrypt individual files on user level. The entire process is simpler that only a checkbox needs to be selected in order to turn on encryption. The checkbox is available in the file and folder properties. Users can also assign read/write permissions for various other users. The files are ready to use once they are opened. When the checkbox is unselected, the file becomes decrypted and any user can access them. EFS is available only certain versions of Windows 7 operating system. Windows 7 Home Basic, Home Premium and starter do not support EFS. There is an alternative for such Windows users where files can be decrypted using Cipher.exe command in the command prompt. An encrypted file can also be modified and copied to local system. The EFS certificated can also be imported and stored as back up files in local system.

### MAC ENCRYPTION

While Windows uses BitLocker and EFS encryption technologies, Apple Mac OS uses FileVault. FileVault can be used in encrypting the entire drive for privacy. FileVault version 1 requires Mac OS 10.3 Pather, Mac OS 10.4 Tiger, Mac OS 10.5 Leopard or Mac OS 10.6 Snow Leopard. FileVault 1 encrypted a user's home directory but it did not encrypt the entire drive. Users create a password that is used to decrypt the files. If this password is lost, a recovery key may be used as well to decrypt the files.

FileVault 2 expands the functionality of FileVault by using the Advanced Encryption Standard (AES) 256 bit keys. It can also be used to encrypt the entire drive. FileVault 2 uses significantly more CPU than FileVault and decryption can be performed with a password or recovery key similar to FileVault. FileVault 2 requires Mac OS 10.7 Lion, Mac OS 10.8 Mountain Lion or Mac OS 10.9 Mavericks installed in the system.

Enabling/Disabling FileVault is an easy task as one simply needs to navigate to System Preferences page and click on Security and Privacy. Click on FileVault tab in Security and Privacy page, to enable/disable the services. There may be situation when multiple user accounts are available in a system. In such cases, administrators need to decide which users are allowed to unlock the encrypted drive. Only those users who are given permission to unlock the drive can access the system. Thus users who do not have permission to unlock cannot login to the system. Only after authorized users unlock the drive, will other users be able to use the system.

Once the users are assigned permissions for unlocking the drive, a recovery key is displayed which comes in handy when users forget the password for unlocking the drive. The recovery key can be used in such situations to unlock the drive and set a new password. It is advisable that recovery key should be stored externally in secure places, other than storing the key in the system itself because, when the system is locked, the recovery key will also be encrypted and cannot be accessed when you forget the password. The recovery key can also be stored with Apple in the cloud. You will be given option for storing the recovery key with Apple once it is displayed. If you prefer to store the key with Apple, you will need to answer three secret questions. The answers you provide for the questions will be used for encrypting the recovery key which is sent to Apple. The only way by which you can retrieve the key from Apple is by answering the questions.

There are questions regarding when one would require using FileVault in their system? It depends on the sensitivity of data stored in the system and the level of mobility. For example, a desktop computer working as server will not require high level of protection but any laptop would require FileVault since there are chances that laptops get missed or stolen from any place. Also, highly sensitive data should always be encrypted to ensure restricted access. It is also important for you to copy files from one encrypted drive to another encrypted drive since Mac OS does not warn while files are copied from encrypted drive to insecure drive. Another important factor that you need to consider while encrypting your drives is that, you should not encrypt your back up drive with FileVault. This is because, if any problem occurs to your system drives, you will need to access backup drives from non-Mac machines, causing serious troubles. Any encrypted Mac drive is safe only until it is unlocked. Once it is unlocked, any user can access the drives and files stored in the drive. Hence, it is essential for you to use strong passwords that remain as a mystery to hackers.

### **SYMANTEC DRIVE ENCRYPTION**

Symantec encryption standard comes with complete protection of data present in the system. All the files including user files, hidden files, system files and swap files can be encrypted using Symantec Drive Encryption. This encryption standard can be used in any type of systems such as laptops, removable media etc. All the data encrypted in the system can be managed through Symantec Encryption Management.

There are many key features available in the standard such as machine recovery, user friendly and PGP strong. Some of the key benefits of Symantec Drive Encryption are silent deployment which is nothing but rolling out of data without end user involving in the process, multi-platform coverage so that all types of systems such as laptops, PC, drives etc, high performance in almost all operating systems including Windows, MAC OS X and Linux operating system. This standard is used in many organizations and is getting popular very rapidly. Since this standard is used worldwide, there is long term strategy in place which will benefit you. As mentioned above, all the operating systems including Windows 8, Windows 7, Windows XP, Server operating system, MAC OS, Ubuntu and Red Hat Linux operating systems. Many different keyboard languages are also supported including English, Belgian, Dutch and many more.

### **CHECKPOINT FULL DISK ENCRYPTION**

Check Point Full Disk Encryption is another set of standards for encryption of files and folders present in any of your computer systems, laptops, smart phones etc. All the files such as operating system files, deleted files, temporary files and important user data can be encrypted and used with ease and privacy. An additional feature available for users is pre boot authentication which ensures user identity, thereby assisting in high level data security along with encryption that ensures data is not lost.

There are many benefits of using Check Point Full Disk Protection. This standard is similar to all the standards discussed above and it provides all general encryption functionalities. The encryption functionality comes into picture when your laptops are stolen as it prevents unauthorized users from getting entry into the system. This encryption mechanism supports all certifications including common criteria and BITS. The software can be used in almost all platforms ranging from Microsoft Windows to Apple MAC. The software has been used in many organizations ranging from less than 1000 seats to more than 100,000 seats. The software has also been the leader in mobile data protection which is a rapidly developing field in information security and privacy. You will also be getting a centrally managed end user solution which works with other security software architectures as well.

### **CREDANT MOBILE GUARDIAN**

Mobile Guardian from Credant Technologies has been a leader in encryption software for the recent years. Their complete protection of data at administrator level along with easy to use controls and simple user interface, the software has been selling hot cakes across organizations. Many advanced features are supported in the software that makes it a best buy. Many positives have been identified with the software but there has not been any negative related to the software which makes it one of the best encryption software available in the market.

Starting from installation of the software to use of software at end level, the easy to use interface and controls make the process simpler. The wizard available for installation and securing data is simple and takes only a couple of minutes for the process to get completed. There is also proper documentation

related to configuration of software and encrypting data. Once the software is distributed and installed in end user systems, Credant provides either 24 hour service or standard day service to the customers.

Well, the difference between Windows and Apple MAC encryption standards were analyzed in the beginning of this passage followed by various other encryption standards. With so many options for the organizations and individual users to choose from, encryption is no longer a daunting task. All you need to do is, purchase the product from the vendor and sit back and enjoy protected data. There will be many more standards getting introduced in the near future which will make the process easier.

## DECRYPTING WITH ENCASE

With the need of digital forensics on the rise, many companies are striving hard to bring out products that investigate various computer systems, laptops etc. EnCase is one such product introduced by Guidance Software, which is a complete suite of forensics products aimed at bringing out hidden information, also allowing for file encryption etc. EnCase suite of products have been used in various forms of investigation and they are popular worldwide. The product is being used by almost 50% of Fortune 100 and Fortune 500 companies along with government agencies all around the globe. EnCase comes in three forms namely eDiscovery, Cyber security and Analytics. There are many advantages of using EnCase in a technology company since many cyber threats arise from such organizations. The latest of the EnCase suite of products is EnCase Forensic v7.08 which comes as the fastest forensic tool available in the market. The EnCase suite of Forensic tools can also be used for tablets, smart phones, removable media such as CD, DVDs, Pen Drive, Hard disks etc. The reports that are generated by the forensic tools are submitted to authorities requesting such analysis. The reports that are generated by the forensic tools are accepted in legal systems of many countries. The reports are generated based on the requirements of the clients, thereby helping them understand the findings in a granular manner.

Encase supports all the encryption standards that are discussed above. For example, Encase supports Microsoft's BitLocker and Encrypted File System. Apart from these two standards, Encase supports various other standards as well. Various other disk and volume encryption standards supported by Encase are McAfee Safeboot, PGP whole disk encryption, Full disk encryption, Utimaco Safeguard Easy and many more. Apart from Encrypting File System, Encase supports CREDANT mobile guardian and RMS.

## REFERENCES

- S. Bunting, "EnCase Computer Forensics: The Official EnCase Certified Examiner Study Guide, 3rd Edition" John Wiley & Sons, Indianapolis, Indiana, 2012
- "What's the difference between BitLocker Drive Encryption and Encrypting File System?", Microsoft, 2013, retrieved from <http://windows.microsoft.com/en-in/windows7/whats-the-difference-between-bitlocker-drive-encryption-and-encrypting-file-system>
- T. Kessler, "OS X FileVault Questions Answered," 2012, retrieved from [http://reviews.cnet.com/8301-13727\\_7-57398382-263/os-x-filevault-questions-answered/](http://reviews.cnet.com/8301-13727_7-57398382-263/os-x-filevault-questions-answered/)
- "How Drive Encryption Works", Symantec White Paper, Mountain View, CA, 2012

## ABOUT THE AUTHOR



**Eric A. Vanderburg, MBA, CISSP**

*Director, Information Systems and Security, JurInnov, Ltd.*

*Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.*



**NIGHT LION<sup>®</sup>**  
S E C U R I T Y

Information Security Risk Management  
24/7 Emergency Incident Response

**1.844.HACK.911**  
[www.NightLionSecurity.com](http://www.NightLionSecurity.com)

# THE ROLE OF INTERNET SEARCHES IN COMPUTER FORENSIC EXAMINATIONS

by Edward J. Appel, Sr.

Today, most types of investigations are incomplete without including a forensic examination of computers, tablets, cell phones and other devices hosting suspects' files and online activities. Pew's Internet and American Life research shows that most Americans are online and frequently use the Internet for a variety of communications. Criminals use computers and smart phones for efficiency in their nefarious tasks, including conspiratorial messaging, meeting arrangements and record-keeping. Cybercrime is increasing, as many types of illegal acts move online, such as identity theft, fraud, misappropriated copyrighted software, movies and music, child pornography and account takeovers, often involving thousands and even millions of database files stolen or misused for the money.

**A**fter over 40 years in law enforcement and private security, including private investigations, it is strange to me that we lock up currency in strong safes, but continue to allow high-dollar digital transactions with a minimum of security (e.g. mere user names and passwords). For decades, we have had robust encryption, biometric and multi-factor identification systems available, but they remain largely unused by banks, retailers, credit issuers and medical records keepers. In effect, when we moved from physical security to online security, we chose to replace steel bolted doors with hook and latch screen doors. No wonder cybercrime is skyrocketing!

Investigations of computing device content often reveal Internet activities by subjects that leave evidence and intelligence stored online. Even if they do not leave digital fingerprints, when people use computers in criminal activities, they are likely to act out online as well. In doing so, they often attempt to

conceal their identity and engage in “anonymous” posts, messages and offsite data storage. Therefore, Internet searches are a logical part of most investigations.

Fencing of stolen property, offsite concealment of contraband such as child pornography or copyrighted materials, conspiratorial communications and records of illegal transactions are just a few of the types of Internet data to be found. Profiles and attributes of subjects are revealed on the Web. Discovering a subject's postings and other references online can provide valuable information for an investigation, including additional evidence, associates, related activities and locations. Search techniques should include a skilled use of multiple search engines, meta searches, automated searching, and a list of online resources chosen for the likelihood of providing references to the subject.

The most important search techniques involve:

- learning to use browsers, search engines like Google, Bing and DogPile, and search tools like Copernic Agent Professional,
- assembling a list of URLs and databases accessible online that can be queried for any reference to the subject,
- based on a subject's known activities, user names and online presence, discovering and querying websites likely to provide references (e.g. professional associations, hobbies, education, employment, social networking),
- finding references to a subject in postings of family, friends and associates,
- efficiently filtering, analyzing and assembling information into succinct reports,
- capturing images of Internet pages that include evidence, intelligence or useful information (such as by printing a PDF copy of the page).

Investigations often require that the subject does not become aware of investigators' interest until it is time for an arrest or other appropriate action. Evidence is crucial to prosecution, and it seems one can never have enough to satisfy prosecutors. Collecting and preserving digital evidence require knowledge of proper techniques. When online evidence is collected, such as items from Web pages or database files, replicas that are digitally signed and securely stored should be acquired and preserved. As this process is continuing, non-alerting searches are required. Many websites (e.g. social networking and professional networking sites) alert account holders when someone visits or views their profiles. Servers often store the Internet Protocol (IP) addresses of users. Therefore, appropriate techniques are required for non-alerting Internet searches.

Among the key techniques and services that online investigators need to acquire are:

- anonymizing proxies through which searches can be done without leaving behind the IP address of the user,
- sandboxes capable of acquiring online content while minimizing the risk of downloading malicious code, adware or the like onto the searcher's computer,
- automated search tools that use not only search and metasearch engines, but also query databases likely to have references to the subject; an example: USA.gov, the portal for the US Federal Government, allows a user to search literally hundreds of databases for references to a subject; at present, the most cost-effective such generally-available, off-the-shelf tool is Copernic Agent Professional,
- using separate computers for investigative searching than for other purposes,
- using assumed identities for investigations in appropriate, ethical ways,
- protocols for assembling and reporting search results.

Search terms are critical to the process of Datamining, because each database must be queried in the appropriate manner and without asking the right question, an investigator will not get the right answers. Computers are quite literal, and only answer correctly-asked questions. Search terms for a person or entity should include variations of the subject's name and nicknames, names of known associates and relatives, user names, email addresses, and names in conjunction with terms describing the subject's known interests and activities. Known past associations, including groups, employers, schools, hobbies and the like should be included in searches. Likely chat group logs should be searched. Social networking, photo, video and group hobby sites should be surveyed for profiles and posts by or relating to the subject. Remember that even if the subject did not post, someone else might post about the subject.

Google, the most-used search engine, and others like Bing and Yahoo (which use virtually the same processors for searches) like to show thousands or millions of search results. The user is left with the realization that the most popular and ad-related references are shown on top. The algorithms used in search engines are after all keyed to selling you something. A few techniques can ease the pain of overwhelming search results: Learn “Google hacks,” i.e. the ways to focus in on a subject. If a popular entertainer’s name is similar to the subject’s, try eliminating references to that person (e.g. Michael Jackson -singer, -pop star). This is an illustration of learning how best to employ the tools that come with Google’s (and other search engines’) applications. Other examples include using quotes to find discreet instances of a person’s name (e.g. “Michael Jackson”) and using known attributes to find references to someone (e.g. “John Doe” Yale). Reviewing many references can be expedited by starting with the first few pages of results, then going to the end of the references presented. Also, changing the number of results displayed on a page (e.g. from ten to fifty or a hundred) can speed up the review. Again, the more an investigator knows about how to use search tools, the better the results. At this point in time, no automated system can substitute for diligent research.

Sometimes, discovering the true identity of a person, or establishing attribution for illicit activities online are part of investigations. These types of investigations can be stymied by truly clever malicious actors. However, it is sometimes possible to identify someone online because they might have the same email or user name on file on another website or database. Clues to the identity of “anonymous” actors can be found, including their IP address, an email address or a chat room where they may be found. It may be possible to engage such subjects in a dialogue using an appropriate undercover identity. One example that comes to mind is the famous US football player who corresponded online with a male individual who pretended to be a female and started an online love affair. When the truth came out, the football player was quite embarrassed, but anyone can be deceived on the Internet. When deception is a necessary part of online investigations, ethical controls should ensure that the investigator does not engage in illegal or illicit acts, and only uses the deception to establish attribution and gather evidence. Preserving copies of all communications with a subject is a key part of evidence collection.

Conducting the most thorough and detailed search also requires rigorous analysis of the results. Reviewing the content of references to a subject often reveals other potential sources of information, and other online search approaches that can be rewarding. It behooves an investigator to realize that information online is like that in any database: it may be true or false, it may or may not be about the subject, and it may or may not be posted by the person who appears to have posted it. Inaccuracies in databases and online abound. Therefore, each item should be taken with a grain of salt. Verification of references is a precise art that most often lacks the precision desired. Sometimes, the only way to verify that the subject posted an item is to find evidence both online and in the computer forensic examination of the subject’s machine. Sometimes, the subject’s own admission is the only certain verification.

The question of cybervetting is often raised in discussions of online investigations. Like professional detective work of all kinds, cybervetting requires skills and abilities that can only be acquired through training (including self-training) and experience. Recognizing evidence, intelligence and information of value is the key to all types of investigations, but is important in background investigations conducted online because of the possibility that the subject did not post the material, or that the references are not to the subject. Understanding the principles of discrimination, privacy, other legal issues and ethical fairness is critical to cybervetting – either for candidates for employment or current employees.

Current US standards for background investigations using standard offline techniques, such as interviews and records reviews, are adequate for cybervetting, and include notice, consent and the opportunity for redress when derogatory references could result in an adverse decision. The US’ Adjudication Guidelines for Access to Classified Information provide a fair and ethical approach for interpreting results of cybervetting, when combined with other investigative results. Of course, guidelines for business would be adapted to eliminate some national security issues like loyalty to country, and possibly to include some issues relevant to the firm, such as the nature of experience in the skills required.

Reports of online investigations should distinguish identifiable references from possible references with no verification that they relate to the subject. Often, references to a name without other identifiers can provide leads to an investigator who is uncertain whether the item actually refers to the subject. It is sometimes possible to use a name-only reference as intelligence, while acknowledging that it may not be identifiable with the subject.

Reports of online investigations should provide a complete record of the process and the findings, including:

- date and description of the investigation done,
- source URLs for every reference found,
- images captured from those Web pages containing evidence, intelligence or related information, in a stable form (e.g. PDF format),
- summary of each finding, followed by key details Attachments can contain the full content in the image of the source page,
- the report should be in clear language, stand on its own and be suitable for presentation in court or proceeding, as a part of the evidence presented in the case,
- where necessary, explanations or comments on findings that require an explanation for those who are not technically-trained or may not understand the website, posting, reliability or relevance of the finding to the purpose of the investigation.

Computer forensic investigators work hand-in-hand with detectives in investigations of all types, and often, detectives themselves are trained in computer forensics Competence in Internet searching does not automatically mean that an investigator is prepared to use search skills in a formal online investigation It is one thing to be “good at finding things online,” and quite another to apply those skills along with appropriate protocols to cases Knowing when a search has been comprehensive and thorough can be difficult, because of the large number of false or dubious references Avoiding mistakes like connecting with websites hosting malicious code, alerting the subject to investigators’ interest and downloading malicious content requires experience and the right tools Again, there is no substitute for training, experience and the right protocols Just because everyone uses search tools in their everyday lives does not mean that they know how to apply the right search techniques in a formal investigation.

As with all types of investigations that blend the skills and techniques needed for a successful outcome, online searching must be combined with the computer forensic examination, the interviews and physical evidence collection, surveillance and other investigative techniques The need for specialization in investigations has resulted in concentrated training for computer forensic examiners Detectives for generations have received additional training in such specialties as fingerprinting, photography, interview techniques, crime scene processing, technical and physical surveillance, and many more Online investigations are equally deserving of additional training and experience, because they are at least a sub-specialty of computer forensic examination and/or network forensics.

### ABOUT THE AUTHOR

---

*Edward J. Appel, Sr. is Principal/Owner of iNameCheck ([www.inamecheck.com](http://www.inamecheck.com)), a 28-year veteran of the FBI (where he specialized in counterintelligence, cryptography and anti-terrorism), corporate security management, non-profit efforts to unite law enforcement, academia, private security and government in high-tech crime investigations, and is author of a book, *Internet Searches for Vetting, Investigations and Open-Source Intelligence* and co-authored the study conducted by the International Association of Chiefs of Police and the US Defense Department’s Personnel Security Research Center titled *Developing a Cybervetting Strategy for Law Enforcement*.*

---

# ATTRIBUTION BEYOND THE IP ADDRESS

**by Dr. Char Sample & Dr. Andre Karamanian**

Attribution with great confidence is very difficult to attain due to proxies and other anonymizing technologies. A new method that allows security experts to gain new insights into the attacker's plans is needed. One such method would invoke the use of social sciences in a cross-discipline approach in order to both profile attackers and to anticipate their next steps. This article discusses the results of some early studies that use this cross-discipline approach and how the results may be understood within the context of Hofstede's cultural dimensions framework. Hofstede's dimensions provide explanations for human behaviors that are influenced by national culture; this in turn may provide valuable insights into attacker's methods and next steps that can be used for both attribution and countermeasures.

Attribution with certainty continues to bedevil security experts. O'Harrow (2012), and former NSA director as well as Director of National Intelligence, McConnell (2010) acknowledged that cyber-warfare is part of the current Internet age, and they acknowledged it is actively occurring as a front against the United States. Goldsmith (2010) noted that attack attribution, through technical means alone is insufficient.

Comer (1991) discussed the distributed, packet switched nature of the Internet and how this Schudel and Smith (2008) identified the difficulty of attribution of attacks because of the broad availability of interconnected systems afforded by the modern Internet. This led to the observations Zhang, Persaud, Johson, and Guan (2005) discussed, where hackers were able to use several hosts to obfuscate the true source of an attack by technological means alone. Attackers move to new technologies that promise to hide their

identities and discard these technologies when identities can be known, one such example would be the use of TOR (Guitton, 2013). The technical cat-and-mouse game continues with each side making incremental changes; however, an alternative approach relies on a paradigm shift to determine the source of an attack. Non-technical means may provide a method to attribute attacks if consistent and quantitative results can support this premise. Sample (2013) puts forth the hypothesis that cyber attacks may have a non-technical component that attackers are unable to control. Sample (2013) based her research, in part, on the work of Hofstede, Hofstede and Minkov (2010) who stated that culture is an unavoidable part of human programming. Hofstede et al. (2010) argued that culture forms the foundation of a group's values. These values, in turn, affected all of the individual's practices (Hofstede, 2010).

## KNOWLEDGE GAINED

The goal of this article is to introduce the reader to a new approach for attributing attacks. This research is very new and offers a great deal of promise for both attack attribution and potential attack countermeasures. The knowledge gained by the reader will provide background information and explanations that the reader may use when setting up and conducting his own research. This knowledge may be applied to any number of accurately attributed intrusion sets in order to provide a possible explanation of the attackers behaviors, and motives. Ultimately, as this research matures, the goal is to provide attribution insights and countermeasure suggestions.

## KNOWLEDGE KNOWN

The authors assume: Behavioral scientists (Bargh & Morsella, 2008; Baumeister & Masicampo, 2010; Buchtel & Norezayan, 2008; Evans, 2008; Gifford, 2005; Guess, 2004; Guss 2011; Guss & Dörner, 2011; Hofstede et al., 2010, Minkov, 2011, 2013; Nisbett, Peng, Choi, & Norenzayan, 2001; Payne, Samper, Bettman, & Luce, 2009) noted the inescapable and habitual role of culture in cognition. Hofstede et al. (2010) went further by stating unlearning these habits is more difficult than learning the behavior. Guss & Dörner (2011) observed that cultural habits influenced perception, and decisions, imperceptibly to the individual.

Guss & Dörner (2011) further determined that when forced to abandon cultural processing norms individuals become more anxious and tentative in their decision-making, in short they do not trust themselves. In the cyber world where information and decisions require rapid ingestion and decision-making reliance on automatic thought processes is necessary (Butler, 2013). Since the both the conscious and unconscious (automatic) thought process is culturally influenced, the likelihood of cultural markers being inadvertently left behind is significant.

Sample (2013) hypothesized and inferred that the claim of cultural markers being inadvertently left behind by attackers was statistically significant. Sample & Karamanian (2014) hypothesized and showed that a correlation exists between the attacker's cultural dimension values and the propensity to engage in certain attack behaviors. Both studies were quantitative in nature and relied on Hofstede's definitions of culture.

Hofstede et al. (2010) identified six cultural dimensions. These dimensions are power distance index (PDI), individualism vs. collectivism (IVC), masculine vs. feminine (M/F), uncertainty avoidance index (UAI), long-term orientation vs. short-term orientation (LTOvSTO), and indulgence vs restraint (IVR). These dimensions are quantified and indexed by Hofstede's research, providing a measurable approach to determining cultural influence.

## POWER DISTANCE INDEX (PDI)

Hofstede et al. (2010) defined high PDI as a system where those in power make decisions, without necessarily consulting with subordinates. The subordinates are in turn expecting the decision maker to make choices with a parental mentality. However, the parent has the entitlements that a child may not. Like the parent child relationship, in a high PDI culture, Hofstede et al. (2010) observed protection expected to be provided by the person in power and loyalty by the subordinate. One important consideration with the high PDI cultures is that the members of society are comfortable with the unequal distribution of power.

Conversely, Hofstede et al. (2010) defined a low power distance culture, as one where positions of authority are more a matter of convenience rather than prestige, for example someone has to specialize in making resource management decisions. The approach of those managing resources, as defined by Hofstede et al. (2010), is consultative. Those in power are not afforded any special allowances or privileges as those whom they manage. The members of society are egalitarian in nature, are comfortable challenging authority and expect a democratic distribution of power.

One behavioural aspect of this dimension that Sample (2013) and Sample & Karamanian (2014) have focused on is in-group loyalty. Woo, Kim and Dominick. (2004) said, “defacing the out-groups’ Web sites with aggressive messages or violent threats may strengthen the feelings of identification or self-esteem the hackers have with their own group” (p.68). A nationalistic, patriotic themed website defacement allows for a show of loyalty in high PDI societies, according to Sample (2013) and Sample & Karamanian (2014), especially when the country feels threatened.

Sample’s initial study (2013) found strong evidence in support of the hypothesis that these attacks are statistically related to high PDI countries. Sample (2013) compared two groups, a control group of the general population and a group of attackers who had participated in nationalistic, patriotic themed website defacements. Mean values were compared for each group and tested for statistical significance. The results showed statistical significance for both PDI and IVC dimensions.

A follow-on study was performed by Sample and Karamanian (2014) where they examined two months of nationalistic, patriotic themed website defacements at [www.zone-h.org](http://www.zone-h.org). This second study was correlational and examined the dimensional scores against the number of attacks from the specific countries. The results of this correlational study showed a strong correlation between PDI and the number of attacks. Additionally, Sample & Karamanian (2014) observed strong correlations between collectivism and the number of these website defacements. Finally, a strong correlation was found between the number of defacements and STO.

### INDIVIDUALISM VERSUS COLLECTIVISM (IVC)

Hofstede et al. (2010) identified the majority of people live in a collectivist society. A collectivist society places the needs of the group over the needs of the individual. Hofstede et al. (2010) identified in a collectivist culture there is still the concept of the first and third person, but with collectivists the first person is the pronoun we and the third person they. This is the pluralisation of identity, most simply put, identification by group. This is a diametric opposite with the individualist society, which still examines first and third person, but focuses on the singular. Individuals from individualistic societies are comfortable making snap decisions where those from collectivist societies are not; they feel the need to consult the other group members (Guss & Dorner 2011, Hofstede et al., 2010).

At this point in time the authors would like to point out that PDI and IVC appear to have some overlapping behaviours; however, they occur for different reasons. For example, in both cases the need to obtain approval from others in order to take action (Hofstede et al, 2010, Sample & Karamanian 2014). However, in the high PDI environment the need to obtain approval reflects the need to request permission. In the collectivist society the need to obtain approval is based in maintaining harmony with the group (Hofstede et al. 2010). These distinctions are significant when activities occur as acts of war or cyber events.

### MASCULINE VERSUS FEMININE (M/F)

Hofstede et al. (2010) identified the masculine versus feminine culture as not only distinct to gender roles, but also aggression. Masculine societies also focused on performance and achievement through assertiveness. Feminine societies value achievement that occurs through cooperation and nurturing (Hofstede et al. 2010). Non-confrontational behaviour is a trait that associates with feminine societies. In the cyber realm this would suggest that non-confrontational crime, those crimes that do not rely on interacting with the victim may be more attractive to feminine countries. Konte, Feamster & Jung (2008) examined “fast flux” DNS behaviours, and found that the country with the most fast flux DNS registrations was Russia, a country that scores on the feminine end of the dimensional pole.

### UNCERTAINTY AVOIDANCE INDEX (UAI)

Hofstede et al. (2010) postulated that uncertainty about the future is part of the human condition. Hofstede et al. (2010) identified the uncertainty avoidance index as how this uncertainty is addressed and measured across a continuum called. Hofstede et al. (2010) identified cultures with high UAI try to avoid change, and prefer structured, rules. This structure is a need experienced by its members, and having a structure in place, even if it is not one that produces tangible results, meets the needs of its members.

In terms of cyber behaviours this dimension may be the most fascinating for various reasons. Hofstede et al. (2010) noted that countries that are uncomfortable with uncertainty go to great lengths to avoid uncertain outcomes, even at the expense of the quality of those outcomes, i.e. it is more important to have

a structure in place that provides situational knowledge and knowledge outcomes, rather than high quality outcomes with little information. In fact, Hofstede et al. (2010) used the precise timeliness of German trains as an example when discussing high UAI behaviours. When precision and UAI are examined in the cyber realm some examples come to mind. The precision of Stuxnet and the association of the US and Israel (Nakashima, Miller, and Tate, 2012) with this malware provides a potential example. The very precise attacking of the centrifuge suggests a potential association with high UAI. While the US has a low to medium UAI score of 46 Israel scores 81 in this same dimension.

On the other end of the UAI pole, low uncertainty avoidance may be more inclined to choose attack vectors with uncertain outcomes. For example, Flame used a form of a probabilistic attack by relying on a collision, Flame has been informally attributed to the US and Israel (Nakashima et al., 2013), scored 46 and 81 respectively, this might suggest that the US role may have been in some way related to the choice of this attack vector. As large number of phishing schemes (Brody, Mulig and Kimball, 2007) have been attributed to the US and China, 46 and 30 respectively. Even spear phishing, known for targeting specific users, has an uncertain outcome since there is no guarantee that the user will actually click on the link.

Brute force attacks rely on exhausting all possible outcomes (www.cs.virginia.edu) this might imply that high UAI countries may be more likely to choose this type of attack than their low UAI counterparts. A recent talk given by fraud investigator Tom Trusty at COSAC 2013 discussed cyber crime in the financial sector. During this talk Trusty noted that the most common countries that were engaging in brute force attacks against financial institutions were Romania (90), Russia (95), Spain (86), Mexico (82) and Italy (75). These scores appear to affirm the UAI link, however, a formal study is needed before such statements can be made with confidence.

As noted earlier this dimension is particularly compelling in the cyber environment. The UAI dimension may also have ramifications in coding practices. Hofstede et al. (2010) noted that in the educational environments that in high UAI countries students were trained that only one correct answer exists for a question, whereas in low UAI environments allow for more than one correct answer. This has led researchers Sample and Karamanian to wonder if certain coding problems such as race conditions or unhandled exceptions are related to UAI dimensional scores.

## **LONG-TERM ORIENTATION VERSUS SHORT-TERM ORIENTATION (LTOVSTO)**

Hofstede et al. (2010) identified surprising patterns in long-term orientation (LTO). As one may expect patterns such as delay of gratification may be expected. However, Hofstede et al. (2010) identified humility as a characteristic that accompanied cultures with high LTO. In the cyber environment this dimension offers several areas of analysis both strategic and tactical. On the tactical front attacks that impact the infrastructure such as “fast flux” behaviours (Konte et al., 2008) and route hijacking (Labovitz, 2010) appear to relate to LTO values. Infrastructure attacks, when successful are difficult to determine, in part due to the implicit trust in the infrastructure. The countries referred to in these examples: Russia (81), Germany (83), China (87), Slovakia (77), US (26), Korea (100), Taiwan (93), Japan (86), and Ukraine (86) are, with the exception of the US, overwhelmingly LTO valued. When Sample & Karamanian (2014) examined nationalistic, patriotic themed website defacements a strong correlation with STO values. Sample & Karamanian (2014) observed that more than half, 865, of the 1492 nationalistic, patriotic themed website defacements were attributed to STO countries. This correlation was an incidental observation in that study and suggested the need for additional research regarding this dimension.

Strategically speaking, examination of intrusion sets may provide greater insight to this dimension. Buchtel & Norezayan (2008) observed that Eastern thinking relies on a more holistic approach and Western thinking can move between direct and holistic approaches adapting as necessary. In cyber terms this would suggest that when the target is known and a time limitation exists that westerners may rely on a more direct approach and easterners would rely on the holistic approach.

## **INDULGENCE VERSUS RESTRAINT (IVR)**

Hofstede et al. (2010) identified cultures valued leisure time, happiness and a sense of control of the choices. A restrained society was identified as one that had several rigid acceptable behavioural cultural norms (Hofstede, 2010). Unsurprisingly, Hofstede et al. (2010) associated happiness with higher IVR countries.

This dimension deals in part with how comfortable attackers will be in showing some panache. Therefore, coding practices may provide an interesting research area of study. Inefficiently coded software or even

certain comments left in the code might indicate the coder's cultural background. Even though code is often times re-used the re-use is not always the same, other features may be added on, thus providing potential insight to the attacker's cultural leanings.

Attacks that may display a humorous element are suggestive of an indulgent society. The MI6 modification of the Al Qaeda Bomb Making Website (Gardham, 2011) reflected a sense of indulgence, and humour. Great Britain is considered a rather indulgent society with a score of 69. Great Britain's partner in this adventure was the indulgent US with a score of 68.

Hofstede's dimensions may lack precision in defining behaviors; certain overlapping behaviors do exist (i.e. humility with femininity and long-term orientation, or considering the feelings and well being of others over self are present in collectivism and femininity (Hofstede et al. (2010).) However, these variations may be dealt with through various analytic methods.

## IMPLICATIONS FOR FORENSICS

As discussed earlier, technical means are not sufficient for forensics of network based attacks. Progress on the technical front has typically been incremental, thus leading to a technical cat-and-mouse game. As seen in the discussion of dimensions, for reasons identified a priori, examples exist that illustrate cyber attackers leaving behind distinct signatures based on their unconscious programming, i.e. their cultural backgrounds. As such, attribution by means of technical analysis can be referenced against identified cultural markers for a match. Cultural markers can be used in addition to technical means to either verify attribution or to add an additional data point in uncertain cases.

Sample and Karamanian (2014) identified one group of cultural markers in nationalistic, patriotic attacks. The study by Sample and Karamanian (2014) lends support to the assertion by Woo et al. (2004) about these attacks and loyalty. An interesting application to forensics would be a technical analysis of such a nationalistic, patriotic attack point to a different country than the culture markers. If the analysis points to such a contradiction, then explanatory research should be pursued.

Various aspects of forensics offer opportunities for the application of culture as a potential overlay. For example, the study of victims, in addition to examining historical data about the relationship between the victim and attacker culture may provide some insight in this area. Can inferences be made that cyber warriors might attack countries with similar cultural profiles? If so, which cultural traits are the traits that are the predictors?

In order to determine predictors cultural traits or markers will require application across cultural dimensions based on attack behaviors. The results will support mappings between specific cultural values and individual attacks. Presently the work by Sample (2013) and Sample & Karmanian (2014) have shown that not only are certain values associated with nationalistic, patriotic-themed website defacements. The research in both cases showed a striking lack of activity with these attacks in low PDI countries. The examination of behaviors and non-behaviors provides valuable inputs for use in building profiles.

The mapping of cultural markers to attacks by countries is a form of profiling that allows for using past behavior to predict future events. Cultural markers offer the promise of being able to extend attribution beyond IP addresses. This research supports the hope of a larger than incremental improvement in attribution methods. Cultural markers also offer the ability to point forensic analysts toward likely suspects when no other clues exist. These markers provide a link between the technical and social sciences this link is easily understood by both technical analysts and social scientists. This cross-discipline approach offers the promise of moving attribution efforts forward in a rapid manner.

## FUTURE RESEARCH

This line of research has yielded strong quantitative results (Sample & Karamanian, 2014). However, this line of research is still in its infancy. Much of the future research has been identified in the descriptions of cyber behaviors with the cultural dimension. As noted earlier, these data points are interesting but not large enough to constitute a full study. Expansion of those examples provides initial study launches.

Beyond the already identified areas additional attributed attack information is required. Additional attack signatures must be identified and examined in the cultural markers framework defined by Hofstede. This could lead to the construction of a library of attack types and their corresponding cultural signatures.

Once such a library is constructed, this research is expected to quantitatively examine cultural markers for predictive capabilities. This additional analysis would allow for accurate anticipation of attacker behaviors; thereby, allowing for defense infrastructure that are predictive and anticipatory in nature.

## REFERENCES

- Bargh, J. A., & Morsella, E. (2008). The unconscious mind, *Perspectives on Psychological Science*, 3(1), 73-79. Retrieved from <http://www.ncbi.nlm.nih.gov/pmc/articles/pmc2440575/>
- Baumeister, R.F., and Masicampo, E.J. (2010). Conscious thought is for facilitating social and cultural interactions: How mental simulations serve the animal-culture interface, *Psychological Review*, 117(5), 945-971.
- Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, 11(3), 43-56.
- Buchtel, E. E. & Norenzayan, A. (2008). Which should you use, intuition or logic? Cultural differences in injunctive norms about reasoning. *Asian Journal of Social Psychology*, 2(4), 64-273. doi:10.1111/j.1467\_839x.2008.00266.x.
- Butler, S. C. (2013). Refocusing Cyber Warfare Thought. *Air & Space Power Journal*, 27(1), 44-57.
- Comer, D.C. (1991). *Internetworking with TCP/IP Volume I, Principles, protocols, and architecture*. Englewood Cliffs, NJ: Prentice Hall Inc.
- Evans, J. S. B. T. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review Psychology*, 59, 255-278.
- Gardham, D. (2011, June 2). Mi6 attacks al-Qaeda in 'operation cupcake'. *The Telegraph*. Retrieved from <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8553366/Mi6-attacks-al-Qaeda-in-Operation-Cupcake.html> on May 5, 2012.
- Gifford Jr., A. (2005). The role of culture and meaning in rational choice. *Journal of Bioeconomics*, 7, 129-155. doi: 10.1007/s10818-005-0495-9.
- Goldsmith, J. (2011, November 27). The pervasive cyberthreat that goes unchallenged. *The Washington Post*, p. A23.
- Guitton, C. (2013). A review of the available content on Tor hidden services: The case against further development. *Computers In Human Behavior*, 29(6), 2805-2815. doi:10.1016/j.chb.2013.07.031
- Guess, C. D. (2004). Decision making in individualistic and collectivist cultures. *Online Readings in Psychology and Culture*, 4. Retrieved from <http://scholarworks.gvsu.edu/orpc/vol4/iss1/3>.
- Guss, C. D. (2011). Fire and ice: Testing a model on culture and complex problem solving. *Journal of Cross-Cultural Psychology*, 42(7), 1279 – 1298. doi: 10.1177/0022022110383320
- Guss, C. D., & Dörner, D. (2011). Cultural differences in dynamic decision-making strategies in a non-linear, time-delayed task. *Cognitive Systems Research*, 12(3), 365-376. Retrieved from <http://dx.doi.org/10.1016/j.cogsys.2010.12.003>
- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations*, New York, NY: McGraw-Hill Publishing.
- Konte, M., Feamster, N., and Jung, J. (2008). Fast flux service networks: Dynamics and roles in hosting online scams. *ACM Internet Measurements Conference*. Retrieved from the Georgia Tech on October 16, 2012.
- Labovitz, C. (2010). China hijacks 15% of internet traffic? *The Arbor Networks IT Security Blog*, November 19, 2010. Retrieved from: <http://www.arbornetworks.com/asert/2010/11/china-hijacks-15-of-internet-traffic/>
- McConnell, M. (2010, February 28). How to win the cyber-war we're losing, *The Washington Post*, p. B01. Retrieved from <http://www.cyberdialogue.ca/wpcontent/uploads/2011/03/Mike-McConnell-How-to-Win-the-Cyberwar-Were-Losing.pdf>
- Minkov, M. (2013). *Cross-cultural analysis*. Thousand Oaks, CA: Sage Publications.
- Minkov, M. (2011). *Cultural differences in a globalizing world*. WA, UK: Emerald Group Publishing Limited.
- Nakashima, E., Miller, G., and Tate, J. (2012, June 19). U.S., Israel developed flame computer virus to slow Iranian nuclear efforts, officials say. *The Washington Post*. Retrieved from [http://articles.washingtonpost.com/2012-06-19/world/35460741\\_1\\_stuxnet-computer-virus-malware](http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware) on July 2, 2012.
- Nisbett, R.E., Peng, K., Choi, I., & Norenzayan, A. (2001). Culture and systems of thought: holistic versus analytic cognition. *Psychological review*, 108(2), 291. Retrieved from <http://samjna.thejeffcho.com/wpcontent/uploads/2007/06/Nisbett,%20et%20al-%202001.pdf>
- O'Harrow Jr., R. (2012, June 4). Everyday machines vulnerable to hacking, *The Washington Post*, pp. A1, A8-A9.
- Payne, J. W., Samper, A., Bettman, J. R. & Luce, M. F. (2009). Boundary conditions on unconscious thought in complex decision making. *Psychological Science*, 19: (1118-1123). doi: 10.1111/j.1467-9280.2008.02212.x. Retrieved from <http://pss.sagepub.com/content/19/11/1118>
- Sample, C. (2013, July). Applicability of Cultural Markers in Computer Network Attack Attribution", *Proceedings of the 12th European Conference on Information Warfare and Security*, University of Jyväskylä, Finland, July 11-12, 2013, 361-369.
- Sample, C., Karamanian, A. (2014, March). Hofstede's Cultural Markers in Computer Network Attack Behaviours. *International Conference of Cyberwar and Security (ICCWS 2014)*. Lafayette, Indiana, March 24-25, 2014.
- Trusty, T. (2013, October). The Wit, Wisdom, and Policies of VapidBank, *20th International Computer Security Symposium and 5th SABSA World Congress*, September 29 – October 3, 2013, Naas, Ireland.
- University of Virginia, Computer Science System Administration Database (2013). Retrieved from: [http://www.cs.virginia.edu/~csadmin/gen\\_support/brute\\_force.php](http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php)
- Woo, H. J., Kim, & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*, 6, 63-82.
- Zhang, L., Persaud, A., Johnson, A., & Guan, Y. (2005, February). Stepping stone attack attribution in non-cooperative IP networks. *Proceedings of the 25th IEEE International Performance Computing and Communications Conference*, (IPCCC, 2006). Retrieved from [http://archives.ece.iastate.edu/archive/00000135/01/Chaff\\_with\\_proof.pdf](http://archives.ece.iastate.edu/archive/00000135/01/Chaff_with_proof.pdf)
- Zone-h website. Retrieved from [www.zone-h.org](http://www.zone-h.org)

## ABOUT THE AUTHOR

*Dr. Char Sample. Academically and professionally experienced cyber security professional with over 19 years of experience in network security and software engineering. Internet security experiences include expertise with firewalls, IDS, IPS, Anomaly Detection, DNS, DNSSEC, Mail, routing, authentication, encryption, secure network architectures, cloud computing (IaaS, PaaS) and Unix internals. Experienced in designing and developing Internet security products. Additional experiences in relating cultural influences in computer network attack behaviors.*

## INVESTIGATING STEGANOGRAPHY IN SOCIAL NETWORKS:

# A “HOW-TO” FOR THE AVERAGE JOE

by April L. Tanner, Ph.D.

Are websites and applications making it easier for criminals to hide and share information on the Internet? Investigators would hope that this would not be the case; however, the reality is that it is quite easy to hide, send, and share information on the web. This presents a problem for forensic investigators given that, not only do they have to recover and examine evidential data contained on hard drives and other media, but they must also consider applications and other freely available tools that can compromise investigative attempts to acquire useful evidence in computer investigations.

**What you will learn:**

- The challenges faced by digital forensic investigators when dealing with antiforensics tools and techniques,
- The importance of knowing what information is unknowingly shared on social networking sites,
- What tools can be used to hide and encrypt data within files, and
- How to perform your own analysis of social networking sites utilizing both antiforensic and digital forensic tools and techniques.

**What you should know:**

- Understand the challenges faced by digital forensic investigators when encountering antiforensic tools and techniques,
- Understand that sensitive information can reside in files and why it is important to know how to protect this information from being shared unintentionally via social networks,
- Understand the need to analyze social networking sites, and
- Be able to perform your own analysis of social networking sites utilizing freely available tools and techniques.

Digital forensics involves the identification, collection, examination, and preservation of digital data for use in court. Computer forensic tools such as Encase and the Forensic Toolkit (FTK) were designed specifically to assist forensic examiners with their examinations. On the contrary, antiforensic techniques and tools have been created as countermeasures to the goals of digital forensics. At the DFRWS workshop in August 2007, a definition for Antiforensics was stated as “any attempts to compromise the availability of or usefulness of evidence to the forensics process” [10]. According to Sartin, the information black market is continually growing and is leading to the growth of compromised data occurrences [8]. Additionally, the information black market has led to the creation of antiforensics, one of computer forensics most significant challenges. Antiforensics techniques can make or break a case depending on the successfulness of the techniques used in making the evidence data difficult or impossible to examine. Antiforensic techniques include destroying evidence, eliminating sources, counterfeiting evidence, and hiding evidence [4]; furthermore, some security research groups have found ways to exploit weaknesses in digital forensic programs. For instance, they have created programs that acquires hashes from the NT Security manager (SAM) file without accessing

the hard drive, have hidden files within the slack space of the NT File System (NTFS), have defeated file signature detectors by allowing the user to mask and unmask files as any type, and have successfully been able to alter the four NTFS file times (modified, access, creation, and entry update) [1,2,7].

In relation to antifoensics, our previous research evaluated whether popular social networking sites protected their users' picture metadata by performing an experiment to determine whether this metadata was accessible after it had been downloaded from various social networking websites [11]. Metadata is data that is hidden or not readily seen; it is information contained within the file such as name, GPS location, date and time, make and model of the digital device used, network settings, and more. Metadata can be useful to both criminals and computer forensic professionals, especially given how connected individuals have become through social networking sites. Millions, if not billions, of photos are shared each day; for this reason, it is important to become more aware of what data is actually shared because an image file may not just contain an image only. In addition, metadata-containing photos were uploaded and downloaded to several social networking sites such as Facebook, Flickr, Twitter, MySpace, and others [11]. It was found that many of these sites are taking the necessary steps to protect its users' metadata by stripping the metadata from the files placed on their sites; however, there were some sites that did not completely remove all of the metadata [11]. The findings from this research led us to question whether steganographic files could persist in social networking sites.

Steganography is an antifoensic method that involves concealing the details of an object within another object. Steganography is commonly used to hide messages in pictures using the least significant bit (LSB) method. Several computer and mobile tools are available that will hide information such as QuickStego, Invisible Secrets, MP3Stego, MobiStego, Stegais, Secret Letter, and many more. Given that the steganographic files hide information in the LSB, we questioned whether these social networking sites strip the hidden file data from a file containing steganography (also known as a stegoed file)? Could forensic examiners acquire hidden information from images downloaded from these sites? Can social networking sites be used as covert communication channels for terrorists? It was reported that during the raid on Osama Bin Laden's compound, several computer hard drives were recovered that contained quite a few pornographic videos. Using computer forensics tools and techniques, it was found that many of the videos contained steganographically hidden messages that were used to communicate with terrorist cells [5]. With the increased placement of videos and images on these sites, this issue should be of high concern to law enforcement officials. In this article, we present steps for determining if social networking sites are preventing the sharing of steganographic files by actively stripping the hidden files from files downloaded from their sites and use hashing utilities and steganographic tools to verify our findings; however, we will only present one social networking site in this article, but this technique and the same tools can be used on other social networking sites.

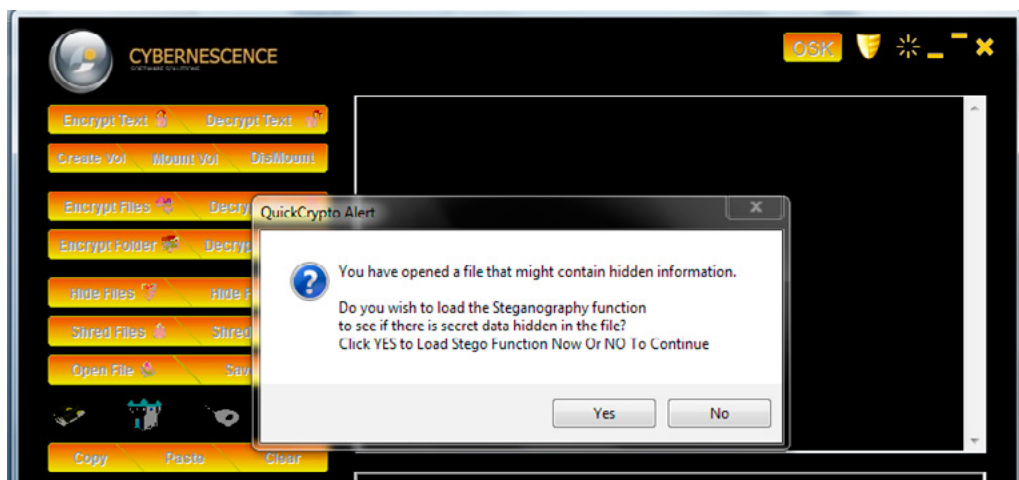
First, a social networking site should be chosen. In order to examine a chosen social network site, a steganographic tool is required for hiding and recovering the hidden files, and a hashing tool is needed to verify whether the uploaded/downloaded file has been modified. Facebook, a popular social networking site, will be examined to determine its ability to strip steganography or steg from a file [6]. Next, a steganographic file must be created using steganographic software. QuickCrypto, which is freely downloadable software that allows the hiding of text/images within files, as shown in Figure 1, will be used [3].



**Figure 1.** Screenshot of QuickCrypto Software Tool

In a digital forensic investigation, it is customary for investigators to authenticate evidence files by calculating and recording the hash values prior to imaging. After the evidence has been imaged, the hash value is recalculated and recorded. The initial hash value is then compared to the hash value after it has been imaged. Obtaining the same hash values prior to and after imaging indicate that the evidence has not been changed. So, in following with digital forensic procedure, HashCalc will be used to calculate the hash value for the file that would contain the image prior to uploading and immediately after downloading the file [9]. This tool is useful for verifying if the file has been modified. From this point forward, a general overview of the steps taken to analyze the social network will be presented.

After the tools and social network have been identified the next step requires the selection and hashing of the file, also called the carrier file, which will contain the hidden image. In QuickCrypto, the “Open File” tab is selected. A new screen appeared, as shown in Figure 2, that indicated that a file, also called a carrier file, was selected and will be opened. The jellyfish.jpg carrier file was selected as the carrier file; the initial hash value was calculated. Selecting “Yes” in Figure 2 loaded the steganography function and opened a new screen containing the jellyfish.jpg carrier file shown in Figure 3.



**Figure 2.** Screenshot of QuickCrypto Steganographic Function Options

Within the Steganography box, the “Hide File” option was selected and the Chrysanthemum.jpg file was chosen. After the file was selected, a notification provided confirmation that the carrier file contained the hidden file as shown in Figure 3.

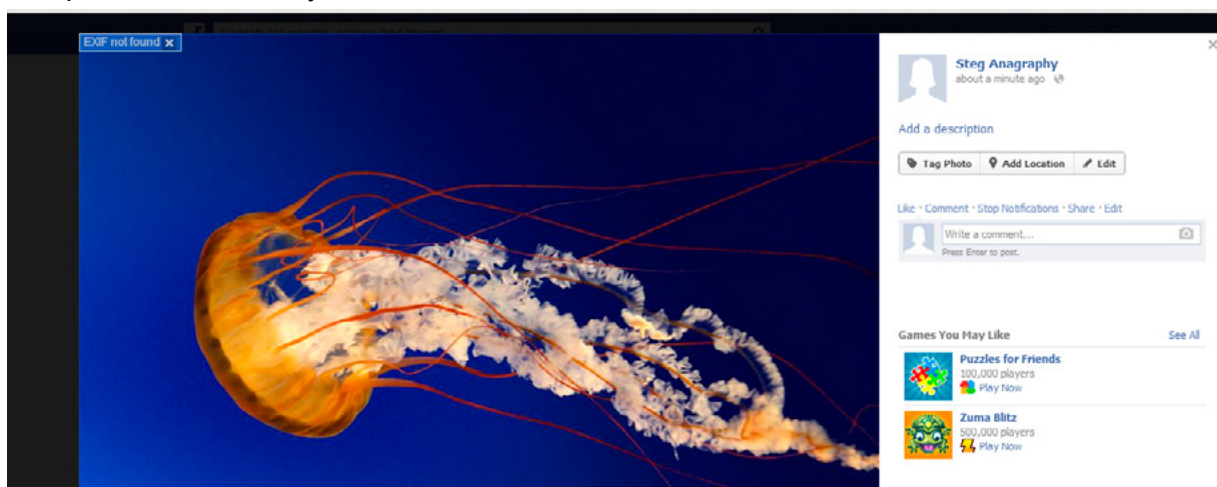


**Figure 3.** Screenshot of Carrier File (jellyfish.jpg) and Notification of Hidden File (Chrysanthemum.jpg)

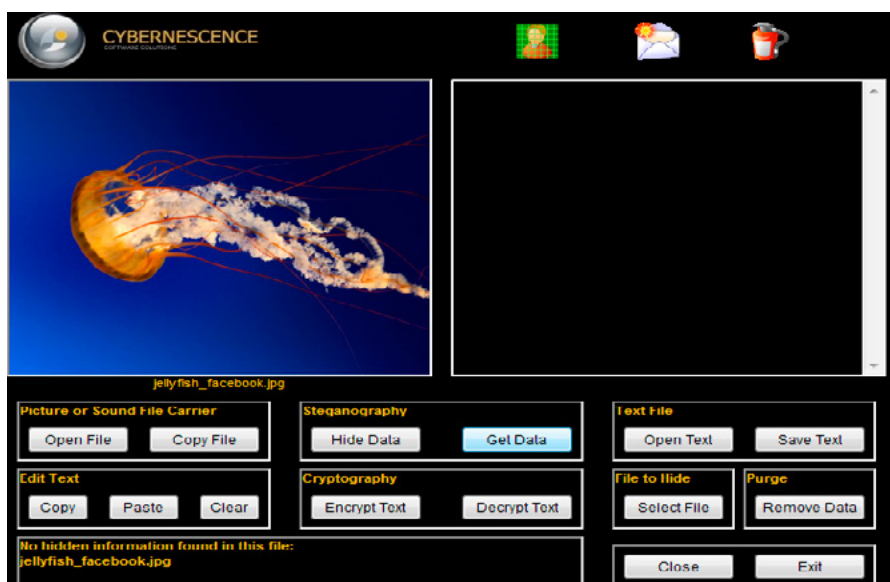
**Table 1.** Hash Values for Jellyfish.jpg file Before and After File Hidden Within It

	Before File Hidden	After File Hidden
MD5	5a44c7ba5bbe4ec867233d67e4806848	5a44c7ba5bbe4ec867233d67e4806848
SHA1	3b15be84aff20b322a93c0b9aaa62e25ad33b4b4	3b15be84aff20b322a93c0b9aaa62e25ad33b4b4

The hash value of the jellyfish.jpg file was again calculated. Even after the carrier file was implanted with the hidden file, the hash values did not change, as shown in Table 1. Next, the stegoed image was uploaded to Facebook. Facebook was viewed using the Chrome browser. Chrome has an extension that allows its users to view EXIF data or metadata contained within files. When used in Facebook, the EXIF extension indicated that no metadata was present in the file. From this information, one can infer that the file does not contain any metadata and that when files are uploaded, the hidden information is wiped simultaneously.

**Figure 4.** Screenshot of the Jellyfish.jpg Carrier File in Facebook Prior to Download

The carrier file, in Figure 4, was downloaded from Facebook and saved as jellyfish\_facebook.jpg. Then, the hash value was calculated for the file to determine if modifications were made to it by Facebook. As indicated in Table 2, the hash values for the carrier file prior to uploading it into Facebook and after downloading it from Facebook differed; this provided an initial indication that the file had been modified and/or that file hidden in the jellyfish\_facebook.jpg may have been removed. Additional analysis of the file was needed to determine if the file remained; therefore, QuickCrypto was used to verify if the hidden file was still present.

**Figure 5.** Screenshot Indicating that Jellyfish\_facebook.jpg Does Not Contain Hidden Information

**Table 2.** Hash Values of Jellyfish.jpg File Prior To and After Download from Facebook

	Hash Value Prior to Upload	Hash Value After Download
MD5	5a44c7ba5bbe4ec867233d67e4806848	5fdd1afb48d0a3ad2fd7a8bb7b1a91fa
SHA1	3b15be84aff20b322a93c0b9aaa62e25ad33b4b4	074a25cc0be889da275be2560c3b2f0986a8ef72

After uploading the jellyfish\_facebook.jpg file to QuickCrypto, the “Get Data” option was selected. The purpose of the Get Data function was to retrieve hidden information from the carrier file; however, no data was recovered as was shown in Figure 5.

In conclusion, it was shown that Facebook does remove hidden data from files containing steganography. This finding is important because it prevents terrorists from utilizing the Facebook application for their criminal endeavors. Although only one social network and one tool were examined, other steganography tools and other social networking sites could be tested as well. In [11], several social networking sites were shown to remove metadata from images uploaded to those sites. One can conclude that this data stripping mechanism in Facebook is applied to all files uploaded to and downloaded from its site. Currently, we are testing other tools and other social networks to determine if those social networking sites are applying a similar data stripping mechanism to steganography files uploaded to their sites. Although social networking sites are assisting forensic investigators in the fight against antiforeshenics, several other antiforeshenics tools and methods are still being utilized. These tools can be used to modify digital forensic tools, encrypt data, and shred files such as history files, content files, temporary internet files, files contained in the recycle bin, cookies, and typed URLs. Additional research is needed to address such tools and identify new techniques and tools that can assist investigators in the battle against antiforeshenics tools, techniques, and methods.

## REFERENCES

- [1] “Antiforeshenics – Subverting Justice with Exploitation,” Computer Fraud & Security, vol. 2007, no.2, Feb. 2007, pp. 16-18.
- [2] H. Berghel, “Hiding Data, Forensics, and Anti-Forensics,” Communications of the ACM, vol. 50, no. 4, April 2007, pp. 15-20.
- [3] Cybernescence, “QuickCrypto”, <http://quickcrypto.com/>.
- [4] A. Distefano, G. Me, and F. Pace, “Android Anti-forensics through Local Paradigm,” Science Direct, August 2010, <http://www.sciencedirect.com/science/article/pii/S1742287610000381>.
- [5] C. Easttom, System Forensics, Investigation, and Response, Second Edition, Jones and Bartlett Learning, 2014.
- [6] Facebook, <http://www.facebook.com>.
- [7] D. Forte and R. Power, “A Tour through the Realm of Anti-Forensics,” Computer Fraud & Security, vol. 2007, no. 6, Jun. 2007, pp.18-20.
- [8] B. Sartin, “Anti-Forensics – Distorting the Evidence,” Computer Fraud & Security, vol. 2006, no.5, May 2006, pp.4-6.
- [9] Slavasoft, HashCalc, <http://www.slavasoft.com/hashcalc/>.
- [10] A. Tanner, A Concept Mapping Case Domain Modeling Approach for Digital Forensic Investigations, dissertation, Mississippi State University, December 2010.
- [11] A. Tanner, S. Jefferson, G. Skelton, “Revealing the Unseen in Social Networking Sites: Is Your Metadata Protected?” International Journal of Multidisciplinary in Cryptology and Information Security, vol. 2, no. 4, August 2013, pp. 15-21.

## ABOUT THE AUTHOR

Dr. April Tanner holds a BS (2003) from Tougaloo College and MS (2005) and PhD (2010) in Computer Science from Mississippi State University. Her research has resulted in the publication of a monograph, one book chapter, five refereed journal papers, and one refereed conference publication. Prior to joining JSU as an Assistant Professor, she worked as a research assistant at Mississippi State University, as a research associate at JSU, and served as a senior academic member of Cyber Crime Fusion Center, located in Jackson, MS. In this role, she developed and taught courses for law enforcement students and wounded warriors in support of the National Forensics Training Center. Dr. Tanner has served as a reviewer for professional journals and organizations such as International Joint Conference on Computer, Information, and System Sciences, and Engineering (CISSE), the Journal of Digital Forensics, Security and Law (JDFSL), and the National Science Foundation (NSF). Her research interests include digital forensics, knowledge mapping, computer security, intelligence analysis, and information assurance.

# Total Cyber Security Solution

## Analyze, Cure, Prevent



### TOTAL CYBER SECURITY SOLUTION

Frogteam|Security unique solution allows organizations, companies and security administrators to:

- **Analyze** organization cyber assets (Cloud:Scope).
- **Cure** using Sec:Cure by correlating analysis results with an easy to use fix module (Sec:Cure).
- **Prevent** using Signa:Gen - TCS Cyber Seal is a sophisticated active and live client that is able to detect and prevent different cyber-attacks techniques and vectors.

### Three easy steps To Secure Your Assets!

Our total solution enable you to Analyze, Cure and Prevent from cyber security threats and vulnerabilities



## Why TCS Cyber Seal is important?

TCS Cyber Seal helps building consumer's trust. With the majority of shoppers' continued concern when providing personal data online - using the Signa:Gen for websites' seal of security will help you concentrate on expanding your business. Signa:Gen - TCS Cyber Seal product objective is to ensure the safety of e-commerce business over the internet. This can be achieved through independent check by the appointed organization which certifies qualified merchant(s) or company(s).



For more information visit our website at: <http://www.frogteam-security.com>

Frogteam|Security Ltd  
E-mail: [info@frogteam-security.com](mailto:info@frogteam-security.com)  
Website: [www.frogteam-security.com](http://www.frogteam-security.com)

Corporate Headquarters  
1875 Century Park East #700  
Los Angeles, California 90067,  
United States  
Tel: +1 (408) 504-4903

**Special Offer for eForensics members**  
Scan this QR barcode to register  
with mobile now and get Special  
Offer of 10% discount.



# CIRCUMVENTING DIGITAL FORENSICS

by Alexander R. Tambascia, D.Sc.

This paper is to cover ways to defeat digital forensics capabilities to recover personal identifiable information (PII), confidential information and/or property intellectual property on personal computer and laptop. This paper will look at simple mechanism, encryption; that can be used to defeat common digital forensic tools and forensic investigator abilities to collect stored and deleted information.

## What you will learn:

- How implement target encryption to maintain network management of critical systems while being able to defeat digital forensic capabilities to retrieve private and trade secret data from compromised hard disk drives.

## What you should know:

- Law enforcement are not the only ones who use digital forensic tools to retrieve data

This paper is not intended to endorse, promote or support any nefarious, criminal or prohibited activity that anti-forensics could be used promote crime or hide from legal authorities. This paper is strictly provided as research and as a means to protect personal and intellectual property from unauthorized retrieval.

## INTRODUCTION

In an age where all critical information is stored in electronic format the ability to protect and store that information from unauthorized access is becoming critical. The increase in industrial espionage, the ability to steal intellectual property, and the ability to steal personal identifiable information (PII) has become extremely easier as compared to when this information as stored in physical secure locations under guard. Many data thieves will use digital forensics tools to acquire this information, it has naïve if not arrogant to believe that only law enforce entities are using these tools in order to solve crimes. These tools are used by industrial spies, criminals, and hackers to retrieve this information as well. As such, counter measures need to be implemented in order to preserve and protect this information from unauthorized access. This paper will discuss some mechanisms that could be implemented to the defeat most common digital forensics tools. This paper is focused on the actual implementation of anti-forensic mechanisms and is not an overview of possible mechanisms that could be used to defeat a forensic investigator.

## HISTORICAL CONTEXT

When looking at the events at history that would require the ability to defeat digital forensics the following historical events occurred where hard drives have been stolen containing personal data.

05 FEB 2014: Hard drive with patient data was stolen from Dr. K. Min YI office in San Jose California [1]

20 DEC 2013: Legal firm's backup data stored on a hard drive was stolen during a home burglary [1]

07 NOV 2013: Two hard drives from Washington State University containing student information [1]

04 NOV 2013: Contractor for University Hospital, Cleveland, Ohio misplaced a hard drive that was later stolen that contained patient data [1]

03 OCT 2013: Hard drive was missing from Mercy Health System with health plan information including names. Numbers and addresses [1]

05 SEPT 2013: Employee stole hard drive with patient information [1]

03 SEPT 2013: InterContinental Mark Hopkins San Francisco reported that a burglary on 04 JUL that resulted in the exposure of guest information including names, addresses, and credit/debit card information. [1]

24 JUN 2013: A laptop and portable drive was stolen from an undercover officer for the King's County Sheriff's department, the drive was unencrypted and held names, addresses and social security numbers. [1]

There are an additional 50+ incidents of hard drives that were stolen from 2013-2010 that contained either personal or corporate information [1]. Many of these cases there was no evidence that the data that was stolen was used in any illegal activity; however, if any of the data thieves had EnCase, BackTrack or any other forensic tool the data could easily be extracted from those stolen hard drives. Also just because there may be no hard evidence that the data contained on those drives may not have been compromised does not mean it has not been compromised and that data could be stored for use for a later date and time.

## PREVIOUS LITERATURE/WORKS

In conducting research for this paper, there is very little research in the area of anti-forensics. Much of the research that exists focuses more on the actual conduct of digital forensics on digital media. Out of the limited research that has been done in the area of anti-forensics are the following:

- Garfinkel, S. "Anti-Forensics: Techniques, Detection and Countermeasures" Naval Postgraduate School, Monterey Ca. [2] This paper is more of a descriptive of methods and tools that can be used to frustrate digital forensic investigators. However the paper falls short on really testing or identifying which techniques work better than others. This paper provides a good starting point for focusing anti-forensic research but can't be used for any definitive actions to defeat forensics investigators.
- Kessler, G.C. "Anti-Forensics and the Digital Investigator" Australian Digital Forensics Conference, Perth Western Australia. [3] This paper was very similar to the "Anti-Forensics: Techniques, Detection and Countermeasures" however this paper had a lot more detail, but also feel short on conducting actual empirical research to test the methods listed in the paper. However, this paper does an excellent work in exploring the various methods that could be used to defeat a forensic investigator.
- Valli, C. & Jones, A. "A UK and Australian Study of Hard Disk Disposal" Australian Digital Forensics Conference, Perth Western Australia. [4] This paper outlined the poor hard disk cleansing/purging of disposed hard drives that have been repurposed. The paper exposed that "supposedly" purge drives had critical data remove off them by using forensic gathering tools.
- Al-Ahmad, W. "A Detailed Strategy for Managing Corporation Cyber War Security" International Journal of Cyber-Security and Digital Forensics, Kuwait. [5] This paper shows by using forensic as a gathering method can be a vital tool for corporate espionage in the acquiring information from the target organization. This paper discussed the value of information and how easily a spy can retrieve that information from the organization.

## LIMITATIONS & ASSUMPTIONS

This paper is only focused on one anti-forensic mechanism, that mechanism being the use of encryption. As such, this paper does not present that one anti-forensic mechanism is better than other anti-forensic mechanism, but merely explores the use of targeted encryption as a useful anti-forensic tool. The built-in encryption capability of BitLocker [6] because of the hardware requirements of the Trusted Platform Module (TPM), as such TrueCrypt [7] is being used as the drive encryption software. The assumption is being made that the

baseline for all experimentation will be made against a whole disk encryption as the baseline to compare the effectiveness of targeted encryption over whole disk encryption. The focus will be on preserving and protecting intellectual property from industrial espionage and data thieves from using forensics to retrieve data from stolen hard drives. The intent is not to hide nefarious activities from law enforcement. The Backtrack forensic scan being conducted is not an in-depth deep drive scan, but merely a simple scan to see if secret files, and internet history is still visible to a digital forensic tool after the targeted encrypted approach.

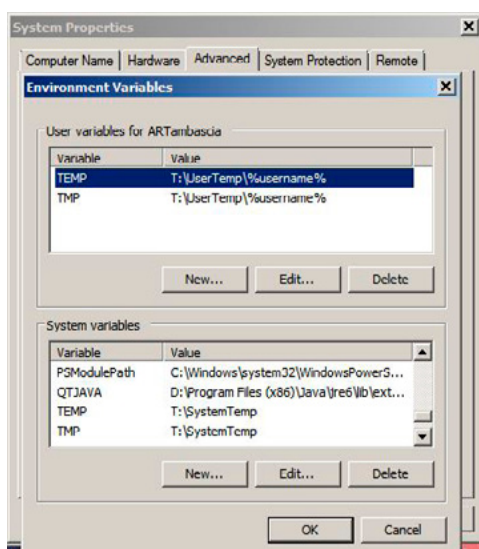
## APPROACH/METHODOLOGY

There are various methods and approaches that can be used to defeat digital forensic capabilities. This paper will focus on one of the methods, that method being the use of encryption. Now it is well known that full disk encryption can defeat any forensic tool because it renders the whole disk unreadable to the collection tool(s) unless the forensic investigator knows the key/passphrase to unlock the disk. The whole disk approach is very much like using a strategic nuclear warhead to take out a small tactical stronghold. However, the problem with whole disk is that it makes network management of workstations extremely difficult especially when normal patching is applied over the network that requires reboot of the workstation. As such, critical installs could be hung up because the workstation is a held state until the operator inputs the passphrase to allow the workstation to continue with the boot process [8]. AS such whole disk encryption although very good at protecting data is also a management nightmare for information technology departments to manage systems remotely.

The approach being that is being explored is a more tactical approach of targeting key areas of a Windows 7 Operating system, encrypting key user data areas and testing If this approach will prevent the ability of an individual to retrieve data even though they [the investigator] has full unencrypted access to the rest of the hard drive. The hypothesis is by taking a more target approach that critical data can be protected from forensic attempts should the workstation become physically compromised while maintaining network manageability. The materials being used are:

- A licensed copy of Microsoft Windows 7 Ultimate 64-Bit,
- TrueCrypt [7],
- Backtrack [9],
- Mozilla FireFox 24.0,
- McAfee Total Protection Suite.

After acquiring the tools needed to conduct the experimentation to test the hypothesis, several configuration changes had to be made after installation of Windows 7 and TrueCrypt in order to encrypt key data/user areas of operating systems. The Encrypted drive that created was given the Drive Letter and label of "T:" and "EncryptedDrive" respectively. In referring to Figure 1, the first step was pointing all temp files for user and system to the new T: drive. This was performed by going to my computer clicking properties; then clicking Advance System Settings; Environment Variables:



**Figure 1.** Temp Files repointing to T: drive

After pointing the temp settings to T: drive the next step was making some Windows registry edits to further ensure that temporary and data files would be stored in the encrypted drive. Refer to Figure 2 on the registry settings that needed to be changed to point to the T: drive. The registry key that is shown in Figure 2 is “HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders” within Windows Registry Editor (opened in Administrator Mode).

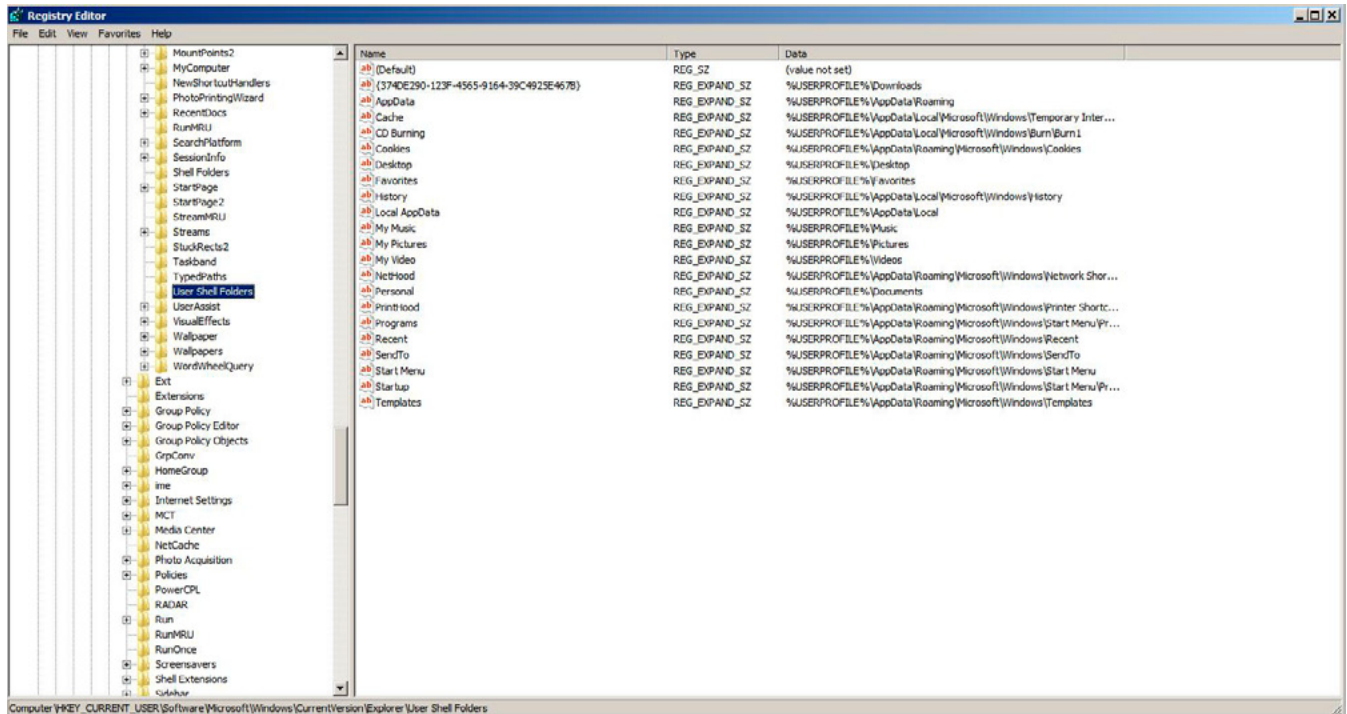


Figure 2. Registry edits to point user files to T: drive

a d v e r t i s e m e n t



INTERNATIONAL EXHIBITION & CONFERENCE ON INTERNET OF THINGS  
TRANSFORMING BUSINESSES, GOVERNMENTS AND SOCIETIES

21-22 April 2014  
SINGAPORE EXPO  
CONVENTION & EXHIBITION CENTRE

# Asia's Premier End-to-End IoT / M2M Conference & Exhibition

Showcasing IoT / M2M Tech Suppliers To a Potential Audience Of 18,000 SIs, App Developers and Consultants From Across Asia

For more information, please visit [internetofthingsasia.com](http://internetofthingsasia.com) or email [info@internetofthingsasia.com](mailto:info@internetofthingsasia.com)

Organized By



Founding Members



Silver Sponsor

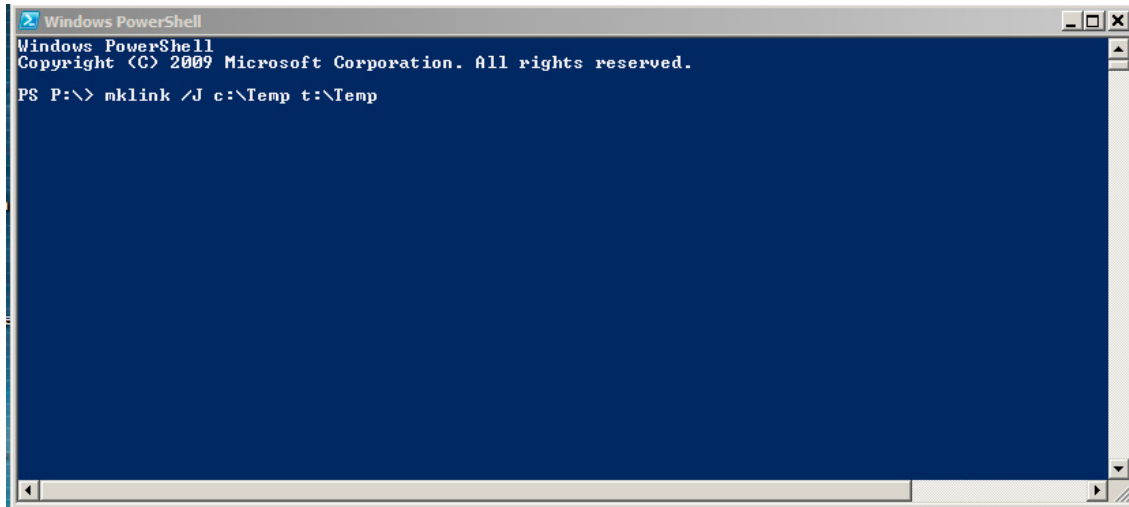


Supported By



Nikkei Business Publications, Inc.


To further ensure that no temp files would be stored on the unencrypted portion of the drive symbolic links were created on the unencrypted drive that would point to the encrypted drive. The command set used is shown in Figure3 & 4.



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS P:\> mklink /J c:\Temp t:\Temp
```

**Figure 3.** Hard Symbolic Link from unencrypted drive to encrypted drive T: for root temp folder

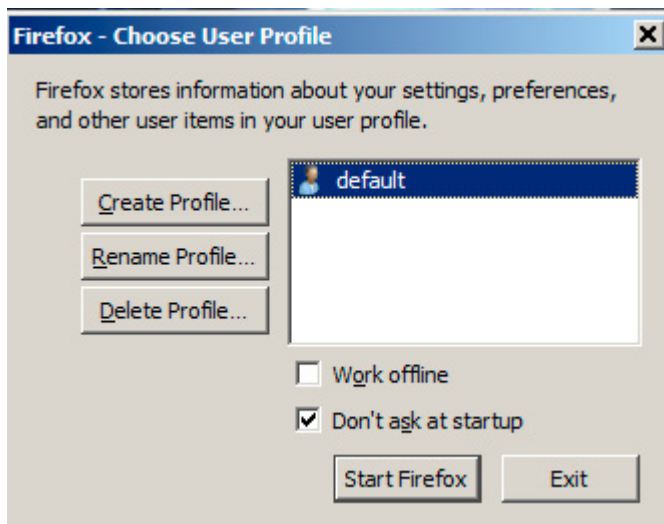


```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS P:\> mklink /J c:\Windows\Temp t:\Temp
```

**Figure 4.** Hard Symbolic Link from unencrypted drive to encrypted drive T: for windows temp folder

After making the operating system changes, using Mozilla Profile Manager [10], figure 5, to create a default Firefox profile that would be stored on the encrypted T: drive which would also include all the temporary browsing files.



**Figure 5.** Mozilla Profile Manager

The default Windows Internet Explorer temporary files was addressed when the registry edits were made as shown in Figure 2. The final step two steps after making all these changes was to reboot the Windows 7 machine. After rebooting the Windows 7 machine, then next step was to removed and erase using the shredder tool that comes with the McAfee Total Protection Suite to secure erase files off a machine, after running the shredder tool, another reboot was performed and the system was verified that all default temp folders and files were no longer existent in default locations and that all temp files were being written to the encrypted drive T:.

In order to prepare the machine for experimentation, several experimental documents of both Microsoft Word and Microsoft Excel format were created using the default application and default save locations (which due to the registry changes now point to the T: drive) named WordDoc-Secret###.docx and ExcelDoc-Secret###.xlsx format. Also using both Internet Explorer and Mozilla Firefox went to several websites of wide variety to generate a history, cookie files and image files in the browsing temp locations for both software suites.

## EXPERIMENTATION RESULTS

The system was fully able to be managed remotely the system. The targeted disk encryption did not in any way interfere with updates and patches that require reboots. The system rebooted remotely and was able to be accessed after each application of required updates. There were, however, two Microsoft updates KB2719857 and KB2732487 updates that would not install even with the hard symbolic links that pointed to the secure T: encrypted drive. Outside of those two outlier updates everything else worked normally. When compared to the baseline several updates would hang due to the stall in the reboot process that would require the passphrase to be entered at each boot up the workstation to allow the reboot process to proceed. Also, both approaches are not transparent to the user in both cases of the baseline whole disk encryption and targeted encryption the user must enter the passphrase to open the encrypted area to the operating system and the user. After logging into the user profile, the passcode must be entered in order to allow the operating system and applications to have access to the encrypted t:\ drive otherwise all critical windows functions would error out when attempted to be opened if the T:\ was not made accessible first. The drive was pulled from the workstation placed into external HDD Docking station [11] and connected to a laptop running BackTrack [9] liveCD and was scanned to see what information could be retrieved. The information collected was able to obtain what files were opened and was able to pull the file names WordDoc-Secret01.docx, WordDoc-Secret02.docx, ExcelDoc-Secret01.xlsx, and ExcelDoc-Secret02.xlsx however, those were only pointers/shortcut files the actual files could not be found on the drive or accessed. No internet temporary files or browsing history was able to be found. The history that the applications Microsoft Word, Microsoft Excel, Firefox and Internet Explorer were opened and accessed but no further information was obtained from the Backtrack scan when it completed. Table 1 shows the effectiveness of this approach as compared to the whole disk encryption baseline.

**Table 1.** Comparison of Targeted Encryption vs. Baseline

	Whole Disk Encryption(Baseline)	Targeted Encryption
Forensically Scan the Whole Disk	O	X
Maintain Network Management of Workstation	O	X
Protect Secret Files	X	X
Protect Temporary Files	X	X
Transparent to User	O	O
Greater Chance of Misconfiguration	O	X

X=Success or "Applies to" O=Not Successful or "Does not Apply"

## CONCLUSION

In conclusion, the experiment did prove the hypothesis as a feasible approach to securing private data while at the same time maintaining the ability to remotely manage the workstation over the network. However, the results collected do indicate that using the target approach runs a significant risk of misconfiguration and not all of the critical data and temporary files being stored on the encrypted part of the hard disk. Unlike the whole disk encryption that runs a very low risk of misconfiguration but sacrifices network manageability. Neither approach provides an ease of use for the user/operator; both approaches require some form of user input in order to access the critical data areas of the drive. The experiment conducted did show that critical data and other private data can be protected without comprising security. It is important to note, that the experiment explored only one mechanism of anti-forensics, that being the use of encryption. There are other mechanisms that can be used as anti-forensic mechanism that have not been explored in this paper. As such, this paper should be used as a comprehensive anti-forensic paper; but as academic research paper exploring one mechanism. This paper was written to provide some hard data points on anti-forensic mechanism that could be implemented to defeat a forensic investigator (lawful or otherwise). Current literature [2] [3] [4] [5] to this point merely pointed out the feasibility of anti-forensic mechanisms but none of the previous literature to date ever conducted physical experimentation to test those mechanism against a forensic tool, in this case, BackTrack. The intent is that the data collected and presented in this paper will provide academic information to researchers to broaden the subject area for all.

## REFERENCES

- [1] Privacy Rights Clearing House, "Chronology of Data Breaches," Privacy Rights Clearing House, 2014.
- [2] S. Garfinkel, "Anti-Forensics: Techniques, Detection and Countermeasures," Naval Postgraduate School, Monterey.
- [3] G. C. Kessler, "Anti-Forensics and the Digital Investigator," in Australian Digital Forensics Conference, Perth, 2007.
- [4] C. Valli and A. Jones, "A UK and Australian Study of Hard Disk Disposal," in Computer, Network and Information Forensics Conference, Perth, 2005.
- [5] W. Al-Ahmad, "A Detailed Strategy for Managing Corporation Cyber War Security," in International Journal of Cyber-Security and Digital Forensics (IJCSDF), Kuwait, 2013.
- [6] Microsoft Corporation, "Hardware requirements for BitLocker Drive Encryption," Microsoft Corporation, [Online]. Available: <http://windows.microsoft.com/en-us/windows-vista/hardware-requirements-for-bitlocker-drive-encryption>. [Accessed 01 Feb 2014].
- [7] "TrueCrypt," [Online]. Available: <http://www.truecrypt.org/>. [Accessed 01 FEB 2014].
- [8] DESlock Limited, "DESlock+ User Manual," Deslock Limited, Somerset, 2013.
- [9] "BackTrack," BackTrack, [Online]. Available: BackTrack. [Accessed 01 FEB 2014].
- [10] Mozilla Support, "Use the Profile Manager to create and remove Firefox profiles," Mozilla, [Online]. Available: <https://support.mozilla.org/en-US/kb/profile-manager-create-and-remove-firefox-profiles>. [Accessed 01 Feb 2014].
- [11] StarTech, "USB to SATA IDE Hard Drive Docking Station for 2.5in or 3.5in HDD Dock," Startech, [Online]. Available: <http://www.startech.com/HDD/Docking/USB-to-SATA-IDE-Hard-Drive-Docking-Station-for-25in-or-35in-HDD~UNIDOCK2U>. [Accessed 04 Feb 2014].

## ABOUT THE AUTHOR

Dr. Alexander R. Tambascia, D.Sc. is a career Army officer currently serving in the United States Army Reserves as a Cyber Operations Officer. He earned his Doctorate of Science in Computer Science at Colorado Technical University. He holds several certifications, which include: MCSE, MCSE+Security, MCITP, CEH, CHFI. Security+, Linux+, JNCIS to name a few certifications he currently holds. He has also participated in the writing of the Security+ and CEH exams. Dr. Tambascia is also an active member of the Cyber Security Forum Initiative – Cyber Warfare Division. Dr. Tambascia focuses his research topics on IPv6, Security, nanotechnology and weapon systems; his current research papers and future papers can be found at <https://coloradotech.academia.edu/AlexanderTambascia>.



Penetration Testing



HP ArcSight Consultancy



SIEM Deployments



## CYBER SECURITY EXPERTS

From security assessment services to complex SIEM deployments, we have the experience to deliver an unrivaled service.

Visit our website to discover how we can help you develop advanced threat detection capabilities within your enterprise

UPDATE  
NOW WITH  
**STIG**  
AUDITING

“IN SOME CASES  
**nipper studio**  
HAS VIRTUALLY  
**REMOVED**  
the **NEED FOR** a  
**MANUAL AUDIT**”  
CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at [www.titania.com](http://www.titania.com)



[www.titania.com](http://www.titania.com)



**Dr.WEB®**  
since 1992



# Dr.Web 9.0 for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search



© Doctor Web  
2003 — 2013



**www.drweb.com**

**Free 30-day trial:** <https://download.drweb.com>

**New features in Dr.Web 9.0 for Windows:** <http://products.drweb.com/9>

**FREE bonus — Dr.Web Mobile Security:**  
<https://download.drweb.com/android>