4:mag

TIPS ON BREAKING INTO THE FIELD

MAC MALWARE. ARE YOU READY?

YOU'VE HEARD THE RUMORS, BUT HOW MUCH DO YOU REALLY KNOW ABOUT...

THE SECRET LIVES OF HARD DRIVES

Issue 1 Q2 2013

MORE LEADS. LESS TIME.

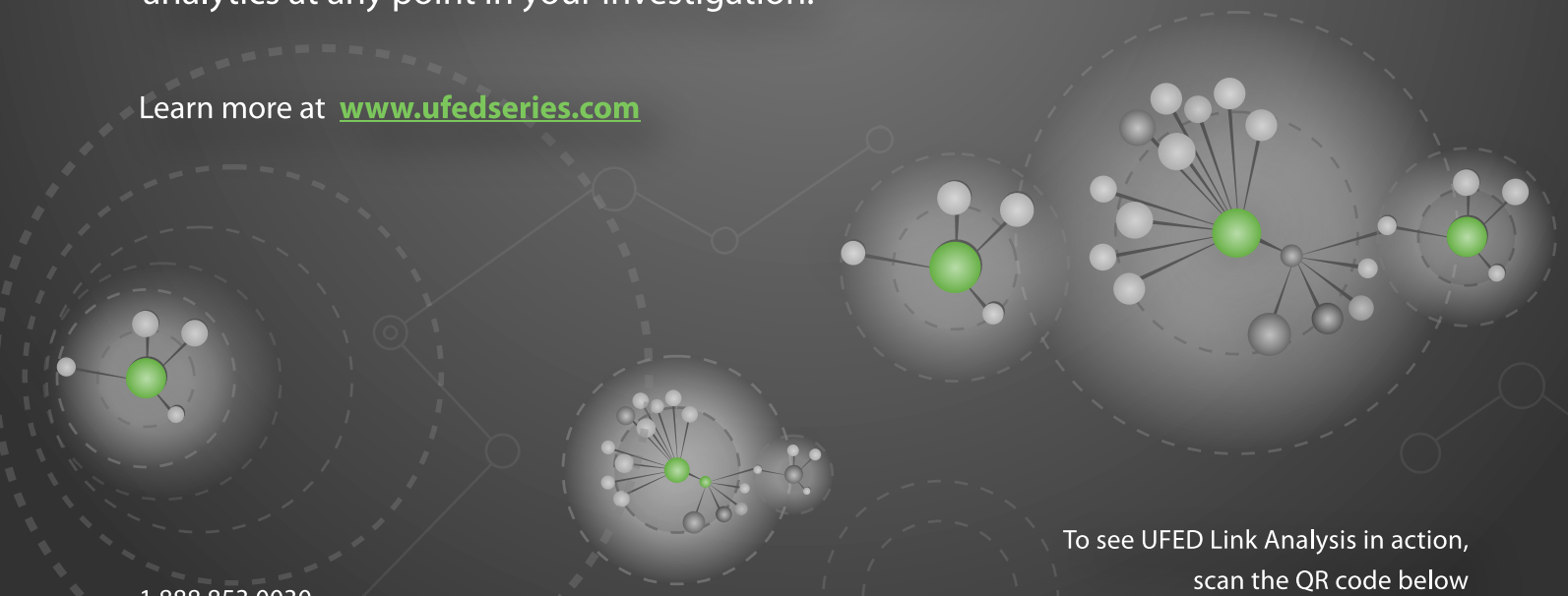
Extract, View & Act with Cellebrite UFED Series

Often, it's not so much what your subject knows – it's who they know. With **UFED Link Analysis**, put the data you extract to work:

- **Transform** isolated data into links between subjects and other entities
- **Visualize** the connection strength between individuals and **identify** key witnesses, victims and even suspects
- **Pinpoint** regular and irregular communication and location patterns
- **Drill down** to specific events in a subject's life
- **Plan** operations, interviews and directions for your investigation

UFED Series applications bring you data and timeline analytics at any point in your investigation.

Learn more at **www.ufedseries.com**



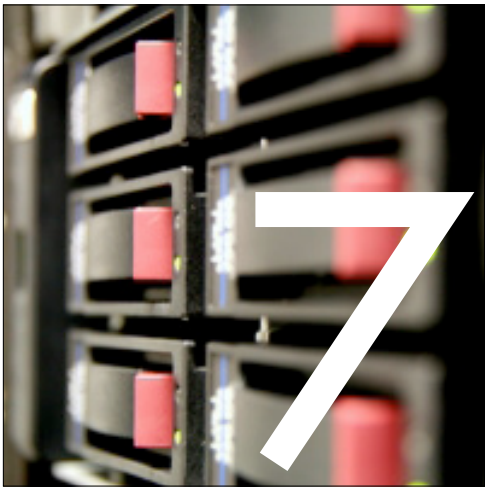
To see UFED Link Analysis in action, scan the QR code below

1.888.853.0030
forensicsales@cellebriteusa.com
www.facebook.com/CellebriteUFED
@CellebriteUSA

cellebrite
delivering mobile expertise

UFED series

4:HOME



contents

Contents Pictures Courtesy of http://www.flickr.com/photos/razor512/7695485686/
http://www.flickr.com/photos/zoliblog/2214058583/
Cover Photo Courtesy of http://www.flickr.com/photos/amagill/89623319/

4:EVENTS

Take a look at the events that are coming up for every forensicator's calendar

AccessData Users Conference - Las Vegas, NV - April 23-25

Lee Whitfield Teaching SANS 408 - Toronto, Canada - April 29 - May 4

Subtle Enough?

CEIC - Orlando, FL - May 19-22

Mobile Forensics World - Myrtle Beach, SC - Jun 2-5

FIRST Conference - Bangkok, Thailand - Jun 16-21

SANS Digital Forensics and Incident Respone Summit - Austin, TX - July 9-10

HTCIA International Conference - Summerlin, NV - September 8-11

SANS Forensics - Prague - October 6-12

Sleuthkit and Open Source Forensics Conference - Chantilly, VA - Nov 4-5

F3 Annual Workshop - Tortworth Court, UK - November 5-7

Have we missed anything?

If you know of something happening and you think that it would interest other forensicators please let us know by emailing lee@forensic4cast.com

Picture courtesy of http://www.flickr.com/photos/ter-burg/5808816530/

4:EDIT

Greetings to all and welcome to the first edition of 4:mag.

Five years ago I persuaded my brother, Simon, to record a new podcast for the digital forensics community. I didn't expect much response, the intention was, simply, to have some fun. Little did I know the amazing journey that awaited.

Here we are in 2013. The podcast has seen great success. Because of Forensic 4cast I have travelled to amazing places and met some really wonderful people. I really feel a part of this community and that is why I strive to give back, hence this magazine.

Anyone who knows me will testify to the fact that I don't like to stand still for more than 5 minutes. I always have several things on the go at once which often causes me to lose focus and become upset when things don't turn out exactly as planned. This magazine is one of those.

A year ago I came up with the concept; a completely free digital forensics magazine that, just like the 4cast awards, is completely community driven. Life got in the way until just recently. I felt the desire to get back into podcasting and to focus on getting this magazine out for everyone to read.

My goal is to publish once a quarter (and the occasional special edition) with only the best material. I want the magazine to be completely free to anyone that wants to read and learn. This means that anyone from people with a casual interest in forensics, to students, to seasoned professionals can have access to the highest quality articles available in the field.

I remember being a student, and then a new analyst, wanting to learn and grow but the cost of the magazines and periodicals seemed to be quite prohibitive.

I'm an open source kind of guy. I believe that knowledge is only attained because someone before you did the groundwork. Hardly ever do we see brand new theories or products that are completely original. Typically everything is born of something else.

So, on with the first issue. We have some great articles written by the best minds in the field (and Ken Johnson).

I love Gareth's article on hard drives. I think that this is especially pertinent because we're now starting to see proof-of-concept software coming through showing how some of these firmware features are being exploited. We will see more of these in the coming months I'm sure.

In Sarah's article we read that Apple computers may have had their day in the sun and, as a result, been burned. While Mac malware is not yet mainstream, it is certainly getting there.

I hope you enjoy these and the other articles we have compiled for your review. If you have any questions, comment, suggestions, or insults please send them to me at:

lee@forensic4cast.com

Thanks for taking the time to read. Enjoy!

Lee Whitfield

A Call to Action

Jesse Kornblum

Log the Data so we can do our Jobs

Computer forensic examiners don't have the resources necessary to answer the questions we are being asked. These are reasonable questions: How did the attacker get in? Which systems did they compromise? What data did they get? But answering those questions requires data which are not found in the logs we have. Instead we have to piece together answers based on data stores never intended for such purposes. With computer security holding such a prominent position right now, we should use this time to change what is being logged and how it's being stored. We can provide better results, make our jobs easier, and make the community safer.

Let's pretend that we find an unfamiliar executable on a compromised host. How did it get there? When did it get there? When was it run? What did it modify on the system? To answer those questions we have some timestamps, a Prefetch file, and perhaps a few registry keys, but that's it. Worse, all of these footprints are stored on the compromised host, where the attacker can either destroy or alter them. We are currently relying on these traces for our cases. But they may not be trustworthy, if available at all.

It's not just file system activity which is deficient. Right now browser history logs only record the requests for whole pages. Many user actions, such as clicks, drags, and "likes" are not logged. Pages which involve a lot of dynamic content, for example, can be difficult to reconstruct. A recent article by Chad Tilbury, for example, looked at extracting geolocation data, http://computer-forensics.sans.org/blog/2012/04/11/big-brother-forensics-device-tracking-using-browser-based-artifacts-part-2. The data of interest wasn't available in the browser history, however, but only the cache. The user committed an act which caused the browser to send data over the network. The response was received, parsed, and displayed, but nothing was written to the logs. An examiner working on such a system would have a hard time reconstructing what the user did. Never forget that the primary purpose of computer forensics is reconstructing what a user did. Sometimes that person is the victim, sometimes an attacker, sometimes both in the same case. But right now we do not have the resources necessary to effectively reconstruct their activities.

In those cases where there is some meaningful data recorded, it remains vulnerable to both deliberate and accidental destruction. The rise of anti-forensics has given us malfeasants who understand the Prefetch directory and wipe its contents during an intrusion. There are automated tools for setting timestamps to zero and injecting memory resident code. Even worse than destroying data, it's possible for somebody to alter the data in question. The complete absence of legitimate data is a sign that something out of the ordinary has happened. But when just the suspicious data are deleted, or altered to look legitimate, it can be a nightmare for the investigator. Not all of the destruction is malicious, of course. Data can be overwritten by legitimate users doing legitimate work, or by system administrators attempting to determine if an incident occurred. Keeping these data on the same computer which an attacker has compromised is making us vulnerable to such destruction and manipulation. In an age of cheap and abundant storage, there is simply no excuse for losing data because we didn't have a copy of it.

The solution to these problems is to change the data we have our computers store and how they store them. Answering the question "How did they get in", for example, would be much easier if we knew the time when each file on the system was created, modified, or executed. For each process, we'd like to know when it was executed, what process created it, any network access, and any registry and file modifications.

It would be foolish to record these rich data on a potentially compromised host. The attacker could easily change or destroy all of this evidence, leaving us in the same situation we are in now. The so-

lution is off-host storage for these data. Log data is generally plain text, which compresses well. Terabyte hard drives are now standard, and in general, it should not be a problem to retain all of these data for some time.

Perhaps the best analogy for these changes would be like installing video cameras on the computers. Video cameras do not prevent crime. No criminal was ever thwarted by being recorded. But they have proven invaluable for determining what happened. Reviewing the tape provides an unbiased picture of what happened even if there was no suspicion of an incident happening at the time.

Many times victims discover they have been compromised by third-party notification, and were in fact first compromised months earlier. Having a long-term record of what happened, stretching back months, could make the difference between being able to conduct an investigation or not.

Certainly a video camera, or its software equivalent on a host, is vulnerable to attack itself. But we should be able to detect the sudden lack of data from such a monitoring system, which in and of itself should cause an alarm. Smashing a video camera does not destroy the data it has gathered so far. There should not be a way for the attacker to destroy the logged data.

There are, of course, some issues with having such long-term and detailed records. Who gets to access them and when? Will employers use such records to monitor their own employees? Could they use such records to enforce policies, such as keeping users off social media or using systems for personal gain. Perhaps, yes. But those areas could also be motivation for them to call for and accept such logging. The nature of the impartial record is that it can be used by anybody for any purpose.

Let's not constrain ourselves to the types of logs which are kept today. When you dream, what kind of information would you like to have when you get that call, "We think we've been hacked." Remember that disk space is cheap right now. We could store a lot of information.

"Having a long-term record of what happened... could make the difference between being able to conduct an investigation or not"

Don't worry about the logistics of how it would work. Working on impossible problems are how breakthroughs are made.

Video cameras are not a perfect technology, of course, and the new logging solutions we develop will not be perfect either. They could be disabled, tampered with, or only show what happened in front of the lens. But having a picture of the situation, however limited, would still be better than fumbling around blind.

In full disclosure, I have been involved in developing a product which records some of the data described above. Whether you buy our product or somebody else's, I earnestly hope start logging more and better data. You are going to suffer a computer breach. It's not a question of 'if', but a question of 'when'. When that happens, me or somebody like me is going to get called in to answer those critical questions above. Because the safety of all of us depends on their ability to provide you those answers, I hope that you can find a way, any way, to record and maintain the information.

Author Biography

Jesse Kornblum is a Network Security Engineer for Facebook in Menlo Park, California. His work touches on a number of topics in computer forensics and computer security, including memory forensics, similarity, file carving, and disk imaging. Jesse has authored and currently maintains a number of widely used tools, including the Hashdeep suite of programs--including md5deep, the ssdeep program for fuzzy hashing, and the Foremost file carver. A graduate of the Massachusetts Institute of Technology, Mr. Kornblum previously served as a computer crime investigator for the Air Force and with the Department of Justice. Mr. Kornblum encourages you to learn about technology by playing "what does this button do?"

Save the Date!

SANS Forensics and Incident Response SUMMIT

AUSTIN, TEXAS

SUMMIT DATES: July 9-10, 2013

PRE-SUMMIT COURSE DATES: July 11-16, 2013

www.sans.org/event/dfir-summit-2013

COURSES OFFERED:

FOR408
Computer Forensic Investigations – Windows In-Depth
GIAC CERT: GCFE

FOR508
Advanced Computer Forensic Analysis & Incident Response
GIAC CERT: GCFA

FOR526
Windows Memory Forensics In-Depth

LEARN R.E.M

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GIAC CERT: GREM

AND MORE!

Device and Application Data from iOS Devices

Brian Moran

People interested in mobile device forensics often ask, "How can I tell where the phone was at a given time?" Most people in our field know that most mobile devices have services running that allow applications to determine the device's location. Locationally aware applications allow a better overall user experience by finding towers and data access points the device commonly sees. But this is just a very small part of why mobile devices permit location awareness. The main reason is to allow applications, data carriers, and even device manufacturers to build usage data, over time, to show what areas will probably be the best for advertising and other market saturation efforts to increase revenue from their clients.

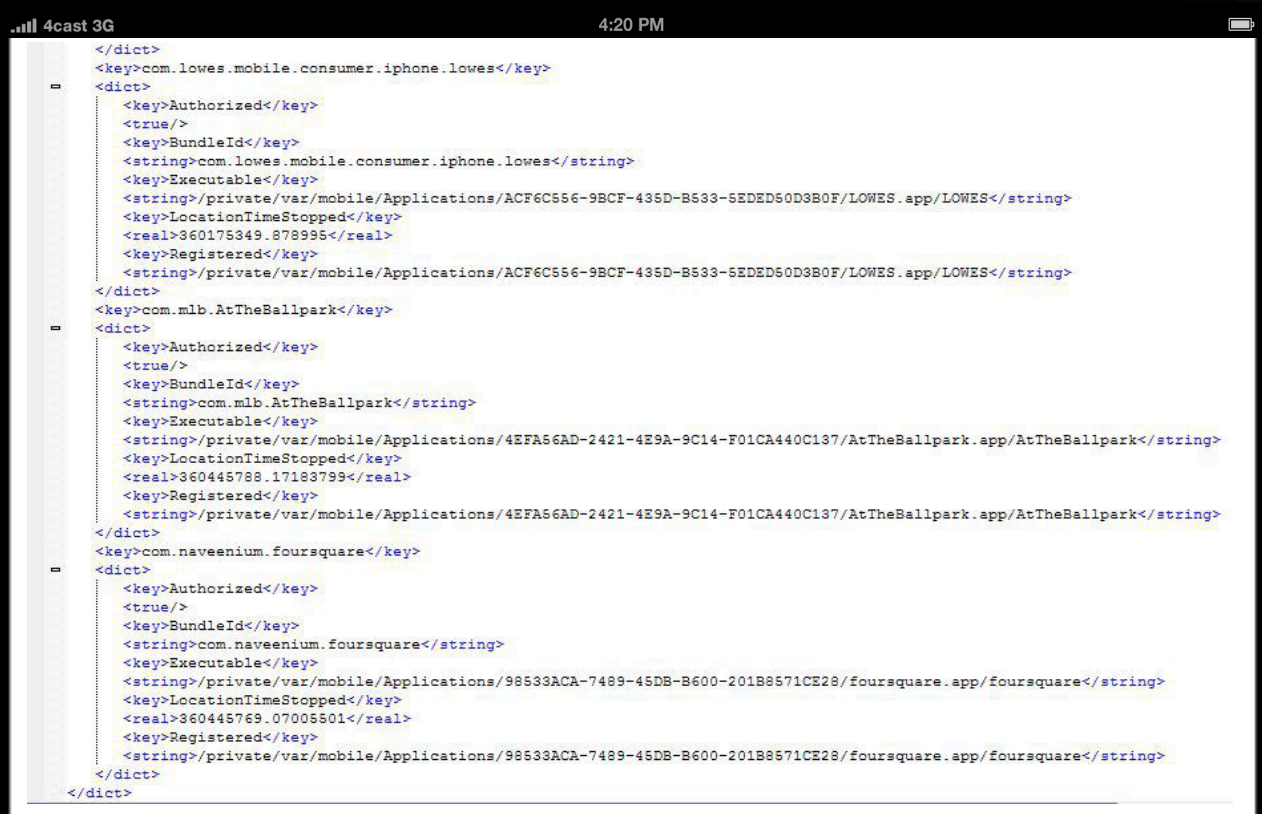
Happily for forensicators, this allows most devices to record such data, and we can usually correlate location with with other items on the handset to approach a more complete timeline of not only what happened at a given time, but also where the device was when events occurred. I offer one word of caution on this approach: realize that it shows only the location of the handset itself. It does not necessarily have the ability to show that the person the mobile device was definitively associated with was in that location as well.

In this article I cover iOS devices—in this case, an iPhone 4s running iOS 5.1.1. 1 I made an iTunes backup of the device. (You can, however, choose to use whatever methodology you would like: the same basic principles apply.) The file we are most interested is "clients.plist" under the "Root" domain, in the path "/Library/Caches/locationd/". If you are looking strictly at an iTunes backup folder, the filename you are interested in is "a690d7769cce8904ca2b67320b107c8fe5f79412". (This follows the standard iOS backup file naming mechanism of computing the SHA1 of the DomainPath, which in this case the SHA1 of "RootDomain-Library/Caches/locationd/clients.plist" does indeed equal a690d7769cce8904ca2b67320b107c8fe5f79412).

Having identified our file of interest, we can look at the data stored within the property list file and determine what applications or services were locationally aware, the last time that the location for that application was stopped, and the path to where that application resided on the device. In the photo below, you can see that some of the location aware applications that were installed on the iPhone were "Lowes", "MLB At the Ballpark", and "foursquare":

<Screenshot of clients.plist/a690d7769cce8904ca2b67320b107c8fe5f79412>

Since we have identified the filenames/paths of interest, we can do a date/timestamp conversion on the associ-



ated data to determine when the applications were last updated. (The timestamps are the number of seconds since 1 January 2001):

Lowes - 360175349.878995 = Thu, 31 May 2012 16:42:29 GMT

MLB At the Ballpark - 360445788.17183799 = Sun, 03 Jun 2012 19:49:48 GMT

Foursquare - 360445769.07005501 = Sun, 03 Jun 2012 19:49:29 GMT

After following this analytic path, we have timestamps associated with the locationally awareprograms. Now we can look to see what data within the applications were last updated aroundour timeframe of interest, or—even-better yet—we can analyze and correlate data to attributeuser activity and the location of the device itself to a specific time or place.

Author Biography

Brian Moran is digital forensic analyst with CyberPoint International in Baltimore, Maryland. Hegot his start in the DFIR/mobile device exploitation field while serving in Iraq as a member of theUS Air Force in 2004, and has been fortunate enough to have continued working in the field for the past nine years.

He transitioned to the civilian workforce in 2012, and has since been an incident responder inseveral high profile data breach cases. He also has spoken at several DFIR events and served asan instructor for Cellebrite Certification classes. His proudest accomplishment, however, is beingnamed co-winner of the 2012 Forensic 4Cast Unofficial Awards for the Best Photoshop of Lee Whitfield.

cyberpoint is a cyber security company. We're in the business of protecting what's invaluable to you.

What we do (a few highlights)

Malware Analysis & Reverse Engineering

Risk Analysis & Vulnerability Assessments

Strategic Planning & Policy Development

Digital Forensics & Incident Response

Machine Learning & Expert Systems Research

Foreign Technology Evaluation, FOCI Mitigation

Secure Network Engineering

High Performance Computing & Big Data

Mobile Security

CyberPoint delivers innovative, leading-edge cyber security services, solutions, and products to customers worldwide.

We discover the threats and vulnerabilities that expose data, systems, and infrastructure to compromise and design defenses that provide critical protection. Our approach is tailored to meet the individual needs of our customers, reduce risks, and ensure ongoing protection in a world of continuously emerging and advanced cyber threats. At CyberPoint, we are always learning, exploring, and looking for new ways to put our knowledge and experience to work.

We seek out hard problems, develop new products and solutions, and drive innovation in the field of cyber security.

cyberpoint

www.cyberpoint.com

Taking a Byte out of Apple Computers

An Introduction to Mac Malware

Sarah Edwards

Picture courtesy of http://www.flickr.com/photos/davidgsteadman/3496323709/

I am a huge Mac fan who, at the moment, is primarily focused on Windows intrusion investigations – I could only hope to work more Mac cases. (Though the non-forensic nerd in me hopes to never work Mac intrusions!) The month of April in 2012 was a turning point in Mac malware awareness. If you have been on the Internet in any way, you have likely heard about the Flashback malware affecting approximately 600,000 Mac users.

I want to introduce the basics of Mac intrusion analysis with a few Mac malware samples. Fortunately for us, these malware samples use many of the same types of locations found on compromised Windows systems.

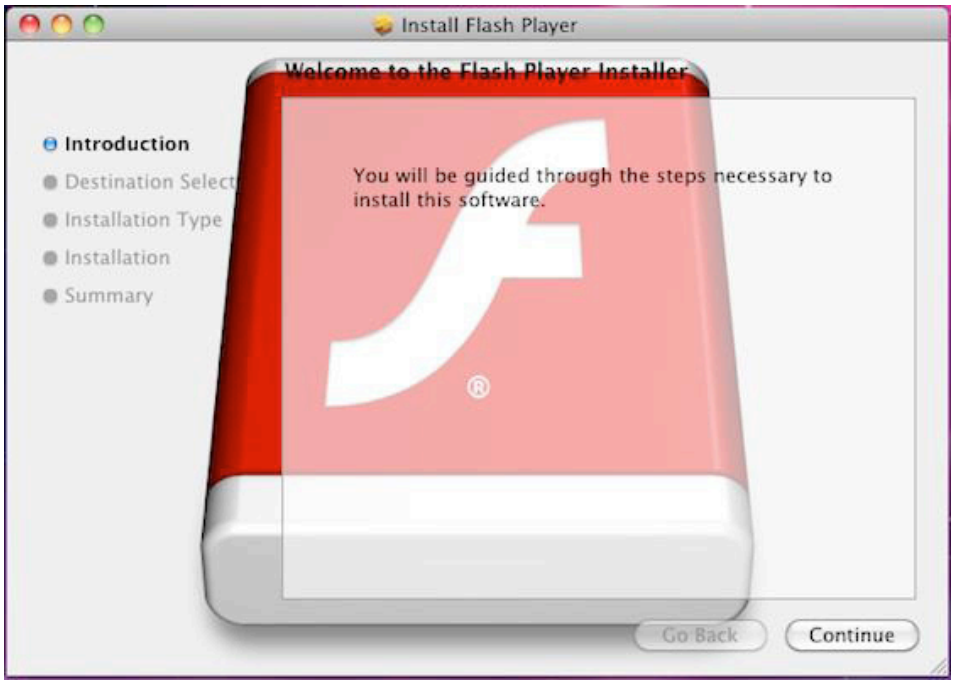
Flashback

Infection by the Flashback (or Flashfake) backdoor Trojan is accomplished by exploiting Java vulnerabilities (CVE-2011-3544, CVE-2008-5353, and CVE-2012-0507) while browsing the web, including compromised WordPress websites. Older variants used a fake Adobe Flash Player update (Figure 1) to tempt the user into installing the malware, while newer variants do not require a password to install. The Flashback malware allows adversaries to install various modules; one of the modules generates fake search results with every web search and directs your traffic to a page where they will receive ad-click revenue.

Depending on the variant, evidence of Flashback installations may reside in the following locations (analysis was provided by those in the References section):

Web Browser Download Directories - These directories may contain the fake Flash Player installation files named FlashPlayer-11-macos.pkg or AdobeFlashUpdate.pkg. These directories are often linked to the main download directory at /Users/<user>/Downloads/.

Temporary Directories or Java Directories – These directories may contain Java .jar files,



Fake Flash Player Installer (Image Source: http://www.cultofmac.com/124840/new-flashback-os-x-trojan-is-in-the-wild-and-it-can-kill-os-xs-anti-malware-scams/)

however some variants reportedly delete these files after installation. An example is rh-3.jar or cl-3.jar. A malware file named .sysenter was found in the /tmp (/private/tmp) directory while the files in /Users/<user>/Library/Caches/Java/cache/ can be deleted in an attempt to remove the malicious Java applets.

Web Browser History & Cache Files – The web history files may contain known compromised websites such as ustream.rr.nu or gangstasparadise.rr.nu (rr.nu seems to be the TLD of choice.) The browser cache files may contain fragments of downloaded compromised sites that contain JavaScript code that was inserted into them to redirect to these domains.

Root of User's Home Directory – The user's home directory can be used to store a downloader module of the malware. The filename is known to be randomly generated and hidden file as it has a dot '.' as the first character in the filename.

The User's LaunchAgents Directory – This directory (/Users/<user>/Library/LaunchAgents) is used for malware persistence; it uses a property list file referencing the file created in the user's home directory. This directory is used by a variety of applications to start services and helper programs when a user logs into the machine. One particular variant uses the property list filename com.java.update.plist with a reference to the file .jupdate in the user's home directory.

Application Bundles – Depending on whether user credentials were given when the malware was installed, there may be files in Application Bundles. If credentials are given, the Safari.app bundle may contain two hidden files with .png and .xsl extensions in the /Applications/Safari.app/Contents/Resources/ directory. References to these files can be found in the Info.plist in the /Applications/Safari.app/Contents/ directory. If the user does not provide credentials, a file named .libgmalloc.dylib is created in /Users/Shared/ and a property list named environment.plist is created or modified in the /Users/.MacOS/ directory. This property list file references the .libgmalloc.dylib file. These file installations will allow the malware to hook into the Safari.app or any launched applications.

Logs – The secure.log as shown to provide another resource to find evidence of malware installation; the malware uses /bin/sh to run an installation script. Tom Webb of irhowto.wordpress.com gives a great visual example of this.

Tibetan-Related Mac Malware

Each of these pieces of malware targets Tibetan Non-Governmental Organizations (NGOs) using various techniques.

Lamadai

Lamadai installs is a backdoor that targets Mac and Windows systems using one of the same Java vulnerabilities as Flashback (CVE-2011-3544) via an email with a link to a malicious website.

Many of the same locations previously suggested may contain evidence of these infections. Look in the temporary directories for .jar files and in the Internet history for the domain dns.assyra.com. This particular malware sample uses the user's LaunchAgents directory as before but with a different filename, com.apple.DockActions.plist and a reference to an executable in the /Library/Audio/Plug-Ins/AudioServer/ directory. The targeted email may be found in the user's favorite email program files, whether it is Apple Mail, Microsoft Outlook, Firefox Thunderbird, or a webmail client.

SabPub

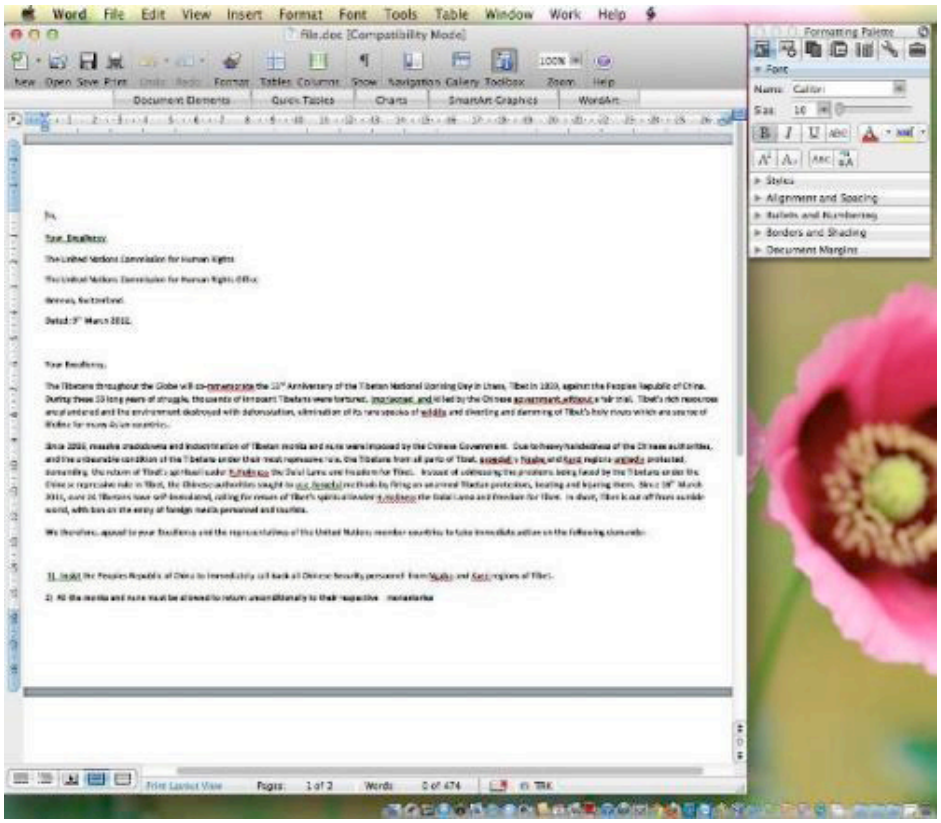
SabPab exploits a Java vulnerability (CVE-2012-0507 again

Decoy Word Document (Image Source: http://totaldefense.com/blogs/2012/04/18/OSX/SabPub-New-Backdoor-Malware-Threat-for-Mac-OS-X.aspx)

- same as Flashback - noticing a pattern here?) A newer variant of this malware uses an old Microsoft Word vulnerability (MS09-027) in a malicious Word document to drop malware while an unassuming user is reviewing a benign Word document (Figure 2). The dropped file is named com.apple.PubSabAgent.pfile and is copied into the user's /Library/Preferences/ directory. Again, a property list file is created in the user's LaunchAgents directory, called com.apple.PubSabAgent.plist, used to start the malware once the user logs onto the system. Of note, a legitimate file on a Mac system is com.apple.PubSubAgent.plist located in the /Users/<user>/Library/Preferences/ directory. This malware is attempting to cloak itself using similarly named property list files.

MacControl

MacControl (or MacKontrol) has two known variants, each using the Microsoft Word exploit (MS09-027). One of the variants uses the com.apple.DockActions.plist file into the user's LaunchAgents directory, just like Lamadai. This file references the executable DockLight in the Automator.app software bundle, specifically in the /Applications/Automator.app/Contents/MacOS/ directory. This executable is copied from a file in the temporary directory /tmp/ called launch-hse. Also in the /tmp/directory you may find a bash script, launch-hs and a Word document, file.doc (Figure 3). The second variant uses an executable named launched in /Library/, and creates the property list file com.apple.FolderActionsxl.plist, in the user's LaunchAgents directory.



Decoy Word Document (Image Source: http://totaldefense.com/blogs/2012/04/11/MS09-027-Target-Mac-OSX-and-Tibetan-NGOs.aspx)

Mac intrusions are not all that different than Windows intrusions; Internet history, temporary directories, system logs, and download directories are similar. Malware persistence points on the file system vary, however the easiest is regularly used – The user's LaunchAgents directory is easily comparable to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key in the Windows registry. Malware on Mac systems may not be as popular or destructive as Windows-based malware, but it is giving forensic investigators one more item to consider when investigating Mac cases. The investigative methods are the same, only the details may differ.

2013 and Beyond

In just the first few months of this year we have seen more Java vulnerabilities, the same social engineering techniques and new interest in Mac malware analysis and reverse engineering. Even Apple itself has been a victim of a drive-by-download Java exploitation from a popular iPhone development website. Mac malware does not appear to be ceasing anytime soon.

Author Biography

Sarah is a Digital Forensic Analyst with Harris Corporation. Her day job consists of Windows intrusion analysis while her nightlight is all Mac related forensics research.

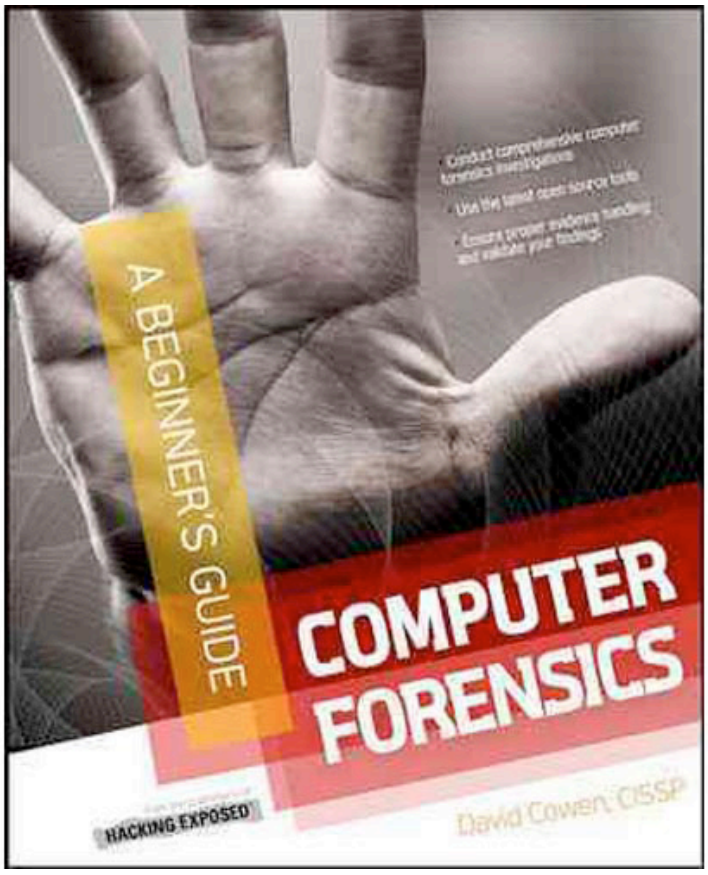
4:WIN

Each issue we're planning on holding small contests. The first person to complete the tasks and post the correct answer will win a prize.

In issue 1 the prize will be a signed copy of David Cowen's new book "Computer Forensics - Infosec Pro Guide". Dave has been working on this book for a long time and this promises to be a great read for anyone new, or planning to be in the field as well as a refresher for anyone who's been in the field for several years.

Not only will the lucky winner get the book but they will also have their name "up in lights" in the next issue of 4:mag.

Also, in the next issue we'll document how the competition panned out. This is largely based on other forensic challenges and will require some complex, and sometime obscure, thinking.



Here's what to do:

Somewhere in the digital copy of the magazine (downloaded from the 4cast website) you will find a clue. Follow this clue and complete the challenge.

That's all I'm going to tell you except that this is a relatively short challenge to complete. Once you get it, you could be done in just a few minutes, even considering the encryption portion of the challenge.

Completion of the challenge will ask you to do something. The first person to complete that task will get the signed copy of Cowen's book.

Sounds simple doesn't it? Anyone that completes this will impress me greatly.

G-C PARTNERS

Dave Cowen is the principle of G-C Partners, LLC. Find them at http://www.g-cpartners.com/

XAMN

MICRO SYSTEMATION
msab.com

IT'S NOT ABOUT THE DATA. IT'S ABOUT THE MEANING.

THE SMART ANALYST PHONE TOOL

If you think mobile forensics is just about extracting data – think again. Its not only what you get, but what you do with it that really makes the difference.

XAMN is the new analytical tool for XRY that allows users to view multiple files in one easy view for timeline, link analysis and geographical mapping.

Starting C

We all come into the field of digital forensics and incident response through various paths. Some of us have started learning our craft through the Government, be it the military, law enforcement, or agency training. Some of us have started our learning our craft through Academia, being self-taught or on the job training. Some of us have known from the time we sat down in front of a computer that we wanted to work with them; others took a roundabout way of deciding that. Regardless of how we have ended up here we are now part of a community that is growing and facing ever changing challenges. A community that in order to excel and stay competitive against those wishing to do harm against the systems we protect, we must work together.

This will not be an article about the threats we are facing externally, there are plenty of people out there that currently do a fine job discussing those. This will hopefully be a reoccurring article that will focus on the threats we face internally as a community and provide opportunities for discussions on what we can do to improve our capabilities as a community.

For the inaugural article I will be covering my journey into Digital Forensics and Incident Response, what steps I took and how you can give back to the community.

The first threat I want to talk about is the insecurity of new responders collaborating within the community. This is something that I have had a personal journey through and have taken steps to change that. To understand my approach to this and my thoughts on the matter, I feel it best to understand my journey into Incident Response and how it impacts my abilities as a responder.

I am a late bloomer into this field; I have been doing Infosec for the last 6 years, an Incident Responder for 2.5 years, received my BS in 2007 at the age of 30, and currently pursuing my Masters. Before being in the field I did AV for Lectures, Concerts and other venues as need. Other jobs I did included Agricultural Drainage Tiling and Terracing work, Namco Arcade Manager, and multiple dead end jobs. All in All most of my jobs have been designed by choice to stay behind the scene and to be left alone, I hated the spotlight.

I decided to go back to school after my daughter was born, because I wanted something different. Don't let me fool you doing AV for concerts rocked, except when I could go two weeks without seeing my family and seasonal layoffs killed the budget.

I went back for Software Development (VB, C, Java) and was sitting in one of my elective Linux classes when the teacher showed us the joys of network security. For the first 4 weeks of class we used Red Hat and did minor attacks and

Out... and Getting Ahead

Ken Johnson

foot printing of each other machines. The last 4 weeks of class he introduced us to Helix and showed us how those things we thought we hid or deleted could still be found. That's the day I decided I wanted to do forensics professionally. Keep in mind at this point my driving force for my degree was my infant daughter.

I was going to ITT-Tech in Nashville at the time we decided to move back to the Midwest. Moving back without a job makes you do some interesting things, we wanted Kansas City, but somehow luck dealt us Des Moines. I took my last year online and finally graduated. I felt upon graduation that I did not know enough to pursue my Masters, so I kept working and slowly moving through the ranks. I also started to realize that the Digital Forensics and Incident Response Community in Central Iowa don't exist. For all purposes the InfoSec Community here could be considered on life support. There are pockets of groups, but from the stand point of a new practitioner there is nothing here.

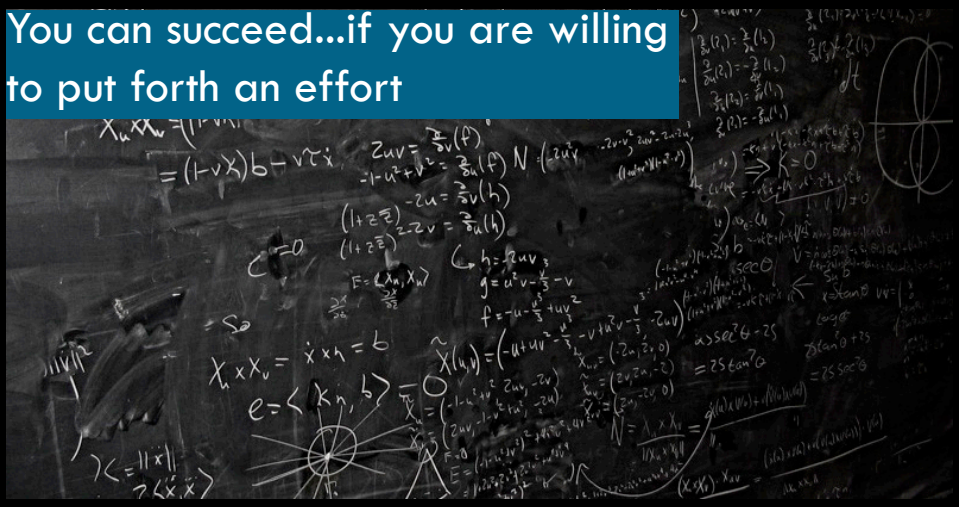
The second step came after finally attending my first InfoSec conference GFIRST which was hosted in Nashville in 2011 I realized that if I wanted to things to change it had to start with me. The first steps I took to change this was enrolling in a Master's Program, and considering organizing a security conference. Looking back at these events I realize that they were the catalyst for the change that I needed.

About the same time all of this was going through my mind I came across an old classmate from high school, which had his own business. Chad's business is The Chad Carden Group that specializes in Motivational Speaking and Sales training, knowing Chad personally I had a good feeling that he learned most of this through personal trials. Chad was always an outgoing hard worker. As a fellow classmate, I decided that I would at least purchase his book called P.E.P.P., since the day I started reading the book and taking to heart the philosophy behind it I have seen things change.

I am not going to attempt to sell you on the program, because what works for one may not work for another. The main concept behind P.E.P.P. is Preparation, Execution, Persistence and Patience. Basically you are going to set achievable long term goals and create a plan to achieve them. Execute on your plan and work towards your goals. Be persistent and do not become discouraged and quit when things go wrong. Finally that any good long term goal will take time and not happen overnight. The key to successfully achieving goals is to readdress and reevaluate the preparation and execution planned for the change.

My initial P.E.P.P. decision was to change my introvert personality and to give back to the community. In the course of 9 months, I have taken ma-

You can succeed...if you are willing to put forth an effort



jor steps in overcoming this obstacle, and within a year of setting this goal I should have made some major leaps on them. I am still not sure where this ride is going to take me, but in the meantime it has been incredible.

My next step was to work on revitalizing the local InfoSec community was to create something that would draw them out of their cubicles and meet with like-minded professionals and future practitioners in the field. This came to be as BsidesIowa, and the turnout was incredible, being that this was my first conference I was ever part of on an organizational aspect I was impressed with the turnout.

The next step was submitting a CFP for the Sans DFIR Summit, Secure360, and GFIRST. I have been accepted to speak at 2 of the 3 conference, which now is forcing me to get over the fear of my public speaking.

Now I am trying to be more active on my blog, and write for this Publication, to help get over the occasional inability to express myself in the written word. All of this is to better help build my local community and to collaborate with the greater global community of Incident Responders.

So now you are probably asking what does this have to do with me, what does he expect to have me learn from these 1200 words I just read?

I want you to learn that regardless your background, your experience, and your capabilities that you can succeed in the digital forensics and incident response community if you are willing to put forth an effort. I am not saying that this will be an easy journey but it will become a rewarding journey. By doing this you will undoubtedly learn something and you will pass your knowledge on to someone else.

While the thought of sharing information to the community might be a little scary, remember that we have all been there. As a community we do not expect perfection but we do expect that you can learn from the research of others, use search engines properly and eventually give back to the community.

It might be a new malicious IP that you have seen in your network traffic near the end of your work day, and while you want to stay and investigate it you can't so you turn to the community with the information. Within a few hours there are multiple responders who have acted on your data and found more information out, so by the time you get home it has been solved and you can take mitigation steps.

It might be a new phishing email that you have received that links to a new variant black hole exploit kit that another responder has been researching and it fills in some gaps in their research.

It might be that Internet Explorer 10 (Windows 8) creates a new Windows Registry entry called TypedURLsTime which is a REG_BINARY and while you share that detail to the community you learn that the value is stored as a Filetime Object. This then turns into an initial topic of a term paper, and morphs into your first conference presentation.

It might be submitting to a conference, getting accepted and presenting in front of numerous peers. While you are filled with self doubt, but standing there you realize that you were asked to share your knowledge, your findings so at least one set of people felt that the information you had to share was worthwhile.

While the previous examples have been examples of sharing actionable intel within the community, it is not always this aspect of sharing that provides valuable information that is necessary. Sometimes the simple review or feature request of the tools we are using provides insight to the developers of these tools how they are being used.

When I learned about Triage, I submitted to Mike numerous request for code changes, as well as eventually giving him my modified code. Mike saw how I was using it, what my development plan was and worked on improving the code. I know that other developers appreciate feedback on how their tools are being used and how they are being used.

Finally the last tool that you have in your arsenal to grow and develop is networking within the community. Career movements in this field can be hard, and it boils down to knowing who you have in your corner and who can support you in your growth. I am grateful for the connections I have gained since I started this journey and the opportunities that it has opened.

As you can see from my journey of being an introverted, spot light avoiding tech theatre guru, ditch digging geek to a growing forensicator the journey is possible. You have to set measurable goals, work diligently to achieve them, and not be afraid of failure in order to succeed. When the goals are finally being achieved the rewards are incredible, and you finally start to feel as an active member of an incredible community.

So what is your story? What brought you into the community? What do you want out of it? What can you give back? What are you waiting for?

Author Biography

Ken Johnson is currently employed at a big 4 consulting firm in their Forensic Technology Service practice. Previously he was employed by Principal Financial Group based out of Des Moines IA. He is currently pursuing an MS in Computer Engineering and Information Assurance from Iowa State University. Ken's current research for his thesis is targeted on Windows 8 artifacts and the impact of the recovery options related to the retention of these artifacts.

When not studying, working or pretending that he understands the full scope of his thesis topic Ken enjoys spending time with his family. He is also an aspiring photographer, and has a range of rough coding experience with various languages. Ken is also an organizer for the BSides Iowa Security Conference.

When the goals are finally being achieved the rewards are incredible

The Newest Forensic Solutions from Guidance Software

EnCase Forensic v7.06

The latest software release offers dramatically faster evidence processing, along with improved functionality and productivity. Process evidence more than three times faster, on large evidence files, and analyze evidence even quicker, with prioritized processing. Embed hyperlinks in exported reports, and display more metadata. New options to filter, search, and view results; open multiple evidence files or view multiple e-mails and records. Review Package and Case Analyzer modules enhance productivity, and Passware integration ensures painless password recovery and decryption.

Tableau TD3 Forensic Imaging System

There's no other forensic product like the amazing TD3. Innovations like a high-resolution touch screen user interface, modular "cable-free" device connections, protective evidence drive enclosures, network connectivity, and a Linux based OS put this product in a class by itself.

EnCase Portable v4.02

EnCase Portable is a packed with innovative features all designed to address the challenge of completing forensic triage and data collection in the field, for both forensic professionals and non-technical field personnel. The new features in EnCase Portable v4.02 make it the most powerful, flexible and field-ready solution available for handling computer forensic tasks. New System Info Parser options combine with an intuitive UI to facilitate collection, preview and advanced analysis on system RAM, local drives and mounted network drives.

Tableau TD2 Forensic Duplicator

When we released the Tableau TD1 we changed the game in forensic duplicators. With the TD2 Forensic 1:2 Duplicator, we've taken it to a new level. If you need to acquire to two HDD's simultaneously - and you are looking for a reliable, powerful, fast, easy to use duplicator, at an attractive price, this is your product.

Tableau T35u USB 3 SATA/IDE Forensic Bridge

Tableau's forensic bridges offer unmatched performance, value, function, reliability, and visual appeal. Our newest product, the T35u SATA/IDE Forensic Bridge, is our first portable bridge to offer USB 3.0 host computer connectivity. Our pursuit of high performance continues.

Tableau T35689iu OEM-style Forensic Bridge

Do you need a new forensic workstation with the ultimate in high-performance write blocking? Make sure yours includes the Tableau T35689iu forensic bridge. This single half-height bay mount bridge will allow you to forensically collect from SATA, IDE, SAS, USB 3.0/2.0, and Firewire devices. We won't rest until we are finished. And we will never be finished.

For detailed product information visit:
www.encase.com and www.tableau.com

Guidance® SOFTWARE

Forensic 4cast Awards 2013

On June 25 2009 I was sitting in an awards show. I remember the date because, while at the awards, I found out that Michael Jackson had died.

I was part of a company that had been nominated in the Bolton Evening News Business Awards.

We were up for small business of the yearn and were up against some tough competition. OK you got me, we walked it as we were up against a local breadmaker and a flower shop.

We won the award and I ended up in the newspaper looking like I was a psychopath about to stab someone with the award (thanks Luby).

While sitting in my tux, my beautiful wife and my brother, Simon, brought up an interesting idea. Why don't we hold our own awards for those dedicated people working in digital forensics?

At first I thought this was a strange idea but I pondered on it over the next few days. I floated the idea with some close friends and they all felt that this was a great idea. Within a couple of months Simon and I found ourselves in the office on a Saturday afternoon doing the first ever Forensic 4cast Awards.

The experience was quite strange. We only broadcast to a handful of people and most of those were not in contention for an award. In fairness we didn't take it completely seriously either.

I felt like it had been a failure and decided to pull the plug on any future awards shows.

Then the emails started.

"Why weren't we nominated?"

"How did THEY win?"

"We want to be a part of this next year."

I received hundreds of emails from marketing people to significant names in the field. Not only that but Rob Lee wrote a forward in a great book in which he mentioned winning one of the awards.

There was no way that we were going to stop after this.

The next year I was approved to speak at the SANS Forensic Summit in DC. Rob and I decided to host the awards as part of the summit. It was fantastic doing it live and handing out physical awards.

We've been back twice more and each time the event gets bigger in significance.

Last year it was incredible to hear the cheer when Kristinn Gudjonsson won his award for log2timeline. It was obvious to me that a lot of people cared not only about Kristinn's efforts but about the awards too.

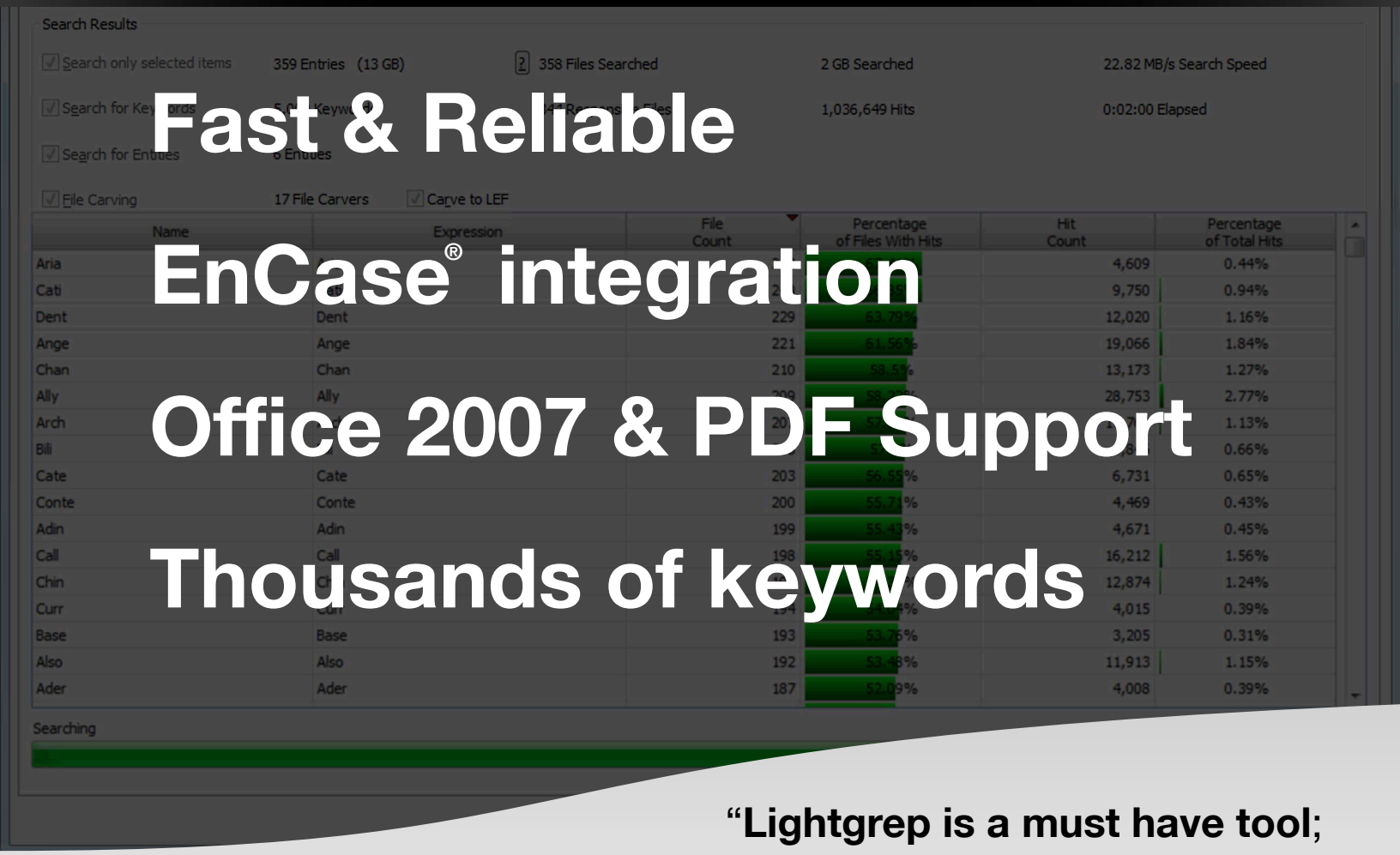
Once again, this year, we have been invited back to the summit in Austin to present the awards. Please help us to make this the best ever as we celebrate great achievements in our field.

Visit forensic4cast.com to place your votes and remember to follow the live stream on Wednesday July 10 at 8am to see if your favorites won awards.

Lightgrep™ Search

Fast Search for Forensics

View the demo – www.lightgrep.com



Fast & Reliable

EnCase® integration

Office 2007 & PDF Support

Thousands of keywords

Contact us for a free trial today:
www.lightgrep.com

$350/yr Corporate
$300/yr Public Sector

Lightbox™ technologies, inc

"**Lightgrep is a must have tool**; not only is it significantly faster, but you can perform computational searches (like Luhn) and it provides more granular options and control!"

– Colby Clark, FishNet Security

4:PRO

Each issue we will be profiling someone that works in the field. For issue #1 we have David Nides.

Where do you work? What do you do there?

I am a manager at a big 4 consulting firm in the Forensic Technology Services (FTS) practice.

My career started here by supporting our Office of General Counsel leading and assisting in internal investigations involving the identification, preservation, analysis, and presentation of Electronically Stored Information. Subject matters included government inquiries, IP theft, PII, data breaches, employee misconduct, and other sensitive subjects. After 2 years, I had the opportunity to partake on a global secondment in China. Ultimately I was in part responsible for the establishment of a FTS team and service line in Shanghai, China. Currently I play a lead business and technical role delivering Incident Response (e.g. network intrusion, data breach) services to clients.

How did you get into the field?

The short answer is I have always been passionate about technology and intrigued by the unknown.

When I was 5 years old I "magically" fixed an Apple 2E computer that a family relative had. He was so impressed he gifted the computer to me. At the age of 8 my family purchased their first computer, a Macintosh Performa 410. I recall my babysitter had told me I would never be successful in the "business world" only knowing how to use an Apple computer. Approximately 4 years later I had finally saved enough money to purchase my first Windows computer. The babysitter was right, within months I had established a web development business, and had more lunch money in my pockets than my fellow middle school classmates.

Shortly after, I was introduced to a reseller of alphanumeric paging devices. This seemed like a great product for e-commerce. At the time, e-commerce was simple; HTML, pictures of products, a few radio boxes, a PHP form to collect personal and credit card information, and a "submit" button to email orders to my AOL account in clear text. So naturally I became a reseller and created an e-commerce site for alphanumeric paging devices. Business was great, so great, I joked about dropping out of high school.

Similar to someone calling the house and disconnecting the dial up internet connection, the business came to a sudden halt. I recall credit card processors had sent me notifications stating customers had used either stolen or inaccurate billing information. I was now in a position where I owed more money than earned for some customers. Like the victim of any normal crime I visited my local Police department. However, I quickly discovered this was not a "normal" crime and there was nothing that could be done. From that point on I was obsessed with conducting investigations.

I went to college double majoring in Computer Science and Criminal Justice. I also worked through college including an Internship my senior year with Target Corporation. They created a special position for me on the Information Security & Compliance Team. That's where I was first exposed to digital forensics. From there, I went on becoming one of the youngest Encase Certified Examiners (EnCE) at the time.

What did you want to be when you

grew up?

This is exactly what I always wanted be.

What is 4n6time?

4n6time is a cross-platform freeware tool that allows users to review large sets of forensic timeline data. The latest version will also allow users to create timelines thanks to Kristinn Gudjonsson's plaso project.

What was the motivation behind the software?

I saw Rob Lee give a presentation about timeline analysis using Log2timeline and was absolutely fascinated by the tool and concept. I went on to try the tool on a case but failed because Excel could not open a 400 MB timeline. I looked, looked, and looked for an alternative solution to review timeline data but there wasn't a good one. So I took it upon myself as an opportunity to learn and contribute back to the community a solution.

What is the most interesting case you have worked on that you can talk about?

Wow, there are so many! I once had the opportunity to do forensics on a mechanical robot. The short story goes like this, an individual was updating the robot's firmware, it "panicked" and severely severed the individual. Through forensic analysis of the onboard computer I was able to show the incident, in part, resulted from the individual updating the robot with incorrect firmware. Ouch.

What was your best moment in forensics?

My first network intrusion case. After many late nights, we found our first lead in a Sqlite artifact that tied an individual to "hands on the keyboard". Observing my boss, Edward Goings, a former AF-OSI agent, use this artifact during an interview to get a hand written admission from the individual, was a moment that I'll never forget and he/she probably won't ever forget either!

What do you enjoy doing away from work?

More work. I love my job and can't believe they pay me to do this. Oh, wait I hope no one from work reads this! I spend hours outside of work preparing for the next day of work. This consists of research, development, and learning new skills. It's just something you need to do and enjoy in order to be successful in a field that is constantly changing. I also have a 66 mustang that I like doing burnouts in.

What is your ultimate goal in life?

I always joke that it's to "save the world one megabyte at a time". However, in some realistic way I think that does align with my long term goals. After having an accomplished career in consulting, I hope to find myself in an Advisor position to the President of the United States on cyber security issues and emerging threats.

What advice would you give to someone starting out in the field?

Invest in your career. Indulge in the fundamentals of hardware, operating systems, and software. Surround yourself with mentors. Challenge yourself constantly. Think outside of the box. Always work smarter not harder. Test, test and retest.

You can follow David on twitter: @DAVNADS

Visit his website at:
http://davnads.blogspot.com/

Do you want to be featured in 4:mag? Just email lee@forensic4cast.com with the subject line "4: Pro" and tell me a little about yourself. I'll then write some questions for you to answer then you, too, can be featured in the magazine.

Find evidence quickly. Turnaround cases faster.

Our Internet Evidence Finder (IEF) software recovers more data, faster—in 3 easy steps. It searches computer hard drives and live memory captures for existing and deleted data from 200+ Internet-related artifacts.

IEF is used by:

Law Enforcement | Government | Corporate Security | Military

Learn more at www.magnetforensics.com
Follow us on Twitter @MagnetForensics

For more information, call us at 519-342-0195
or email sales@magnetforensics.com

MAGNET FORENSICS

Hard Drive Secrets Revealed

Gareth Davies

The most common form of storage media used in both the commercial and domestic environment is the HDD. It is therefore unsurprising that this digital storage device forms a significant part of digital investigations. There are vast resources discussing best practice in the collection and preservation of evidence from these devices. Most large and national police forces maintain an in-house digital forensics capacity to address evidence of this nature e.g. The London Metropolitan Police Service in Great Britain, The Institut de recherche criminelle de la gendarmerie nationale (IRCGN) in France and the Federal Bureau of Investigation (FBI) in the USA. There are also a number of best practice procedures for law enforcement, an example from the UK is the Association of Chief Police Officers Guidelines. These guidelines define best practice processes and procedures for the collection and general analysis of digital evidence and are relevant to the processing and analysis of Hard Disk media.

However, in specific cases where a technically competent suspect has access to specific, commercially available hardware and software, there is the potential for the various HDD firmware implementations to be manipulated. This may enable the user to conceal vast quantities of data on the drive and place this data beyond forensic recovery using standard tools and techniques. It may also enable the drive to be sabotaged by these tools and by possible future forms of malware, prohibiting forensic analysis. More today than ever an investigator requires some knowledge of the low-level functioning of a HDD, and the tools that are available to manipulate the firmware of a HDD.

This article reviews the key aspects of HDD architecture and design. It discusses the firmware and the functionality that support the normal operation of the drive, including the defect management processes focussed on maintaining drive reliability.

The Hard Disk

A HDD is a complex device providing high volume non-volatile storage. A disk is composed of a number of elements including a voice coil, read / write heads, casing, mountings, a motor and a controller board. There are two commonly used form factors; the 3.5 inch used in desktop systems and 2.5 inch used in laptop computers although other form factors have been developed, one example is the 1 inch drives used in the older Apple iPods. Despite the variation in the form factor, the internal arrangement of the devices is similar; the data area consists of a stack of platters coated with a magnetic thin film oxide. The current maximum storage capacity for user data on a disk drive is in the region of 4TB although 14TB versions are likely to be produced with new heat-assisted magnetic recording technologies. Once a drive has been low-level formatted and a high-level file system written to the drive, the typical amount of storage is slightly less than advertised.

Data Storage

Considering a single platter surface, a track can be defined as a rotation of the disk at a particular radius. For sets of surfaces, a set of tracks at the same radius is known as a cylinder. A separate head assembly is located on the armature for each disk surface. During use the position of the read / write heads is determined by location data embedded within the user data area. This location information is written to the drive at the point of manufacture. The sector is the smallest addressable unit on a drive - a specific sector can be located at one level of abstraction using a Logical Block Address (LBA). This method

assigns a sequential address to each sector. To locate a sectors physical position on the hard drive this is converted to a physical location by referencing a specific Cylinder (C), Head (H) and Sector (S).

There are some areas of the drive that are not available for user data storage, but are known to some investigators and receive limited forensic tool support. The Host Protected Area (HPA) provides storage for diagnostics and other utilities required by the system manufacturer. A Device Configuration Overlay (DCO) is used by HDD manufacturers to configure drive sizes and may exist in addition to a Host Protected Area.

Hard Drive Firmware Functionality

In addition to those areas of a drive not addressable by a user there are also areas of the drive that are not addressable by the host computer's operating system and contain

"This may enable the user to conceal vast quantities of data on the drive and place this data beyond forensic recovery using standard tools and techniques"

firmware used to control the effective operation of the disk. HDD manufacturers implement the firmware operations in different ways, however typically

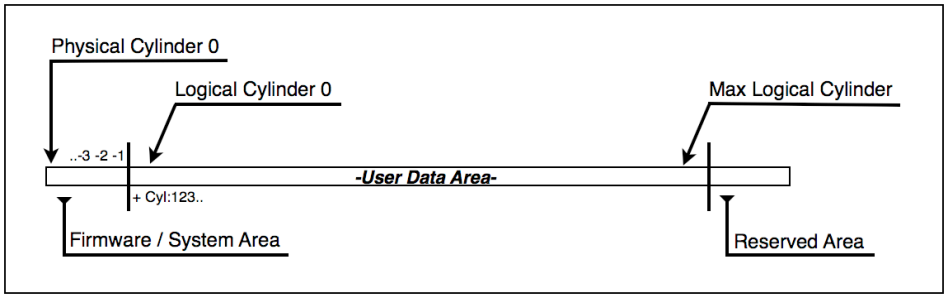


Figure 1: Data Storage Locations (single platter)

this firmware is located on both the Printed circuit board (PCB) and on the platters of the disk. The initial portion of code located on disk controller PCB, is used to load firmware resident on the drive platters. (above). It should be noted that in some cases in multi-platter drives the firmware may be duplicated across the platters.

The firmware controls the correct internal operation of the HDD, allowing it to interact with the host computer (i.e. the operating system). The initial startup loads the firmware from the disk platters into the controller board. The firmware then performs a number of checks to ensure correct operation of the drive, the disk then presents itself in a ready state enabling the host computer to load any operating / storage system on the disk. When the HDD is powered down after use, it is the firmware that executes a shutdown sequence to ensure the device powers down correctly to a safe state.

During normal firmware provides number of functions: SMART Monitoring (Self-Monitoring, Analysis, and Reporting Technology), which monitor a number of manufacturer dependent criteria to ensure the drive is operating within certain parameters. Attributes include, amongst others; read error, seek error, uptime and device temperature - this system can provide useful information in some complex investigations. The firmware is also responsible for monitoring defect control: The error management system in the device firmware contains a catalogue of physical defects present at the point of manufacture. These flaws are recorded in the disk firmware; further physical flaws are recorded as the drive wears due to use.

Monitoring defect control is an important firmware function. This process is transparently handled by the HDD and occurs 'beneath' the host operating system level. The flaws identified on the drive during production are recorded in the disk firmware as the 'P' (primary, production or permanent) list. As the disk ages and as a result of wear & tear other sectors fail and this is recorded within the firmware area in the 'G' (growth) list. Reads and write operations are automatically redirected (remapped) to spare sectors within the Reserved Area of a HDD, when a current physical location has been identified as failing (next page). The sector locations recorded in the P-list and G-list

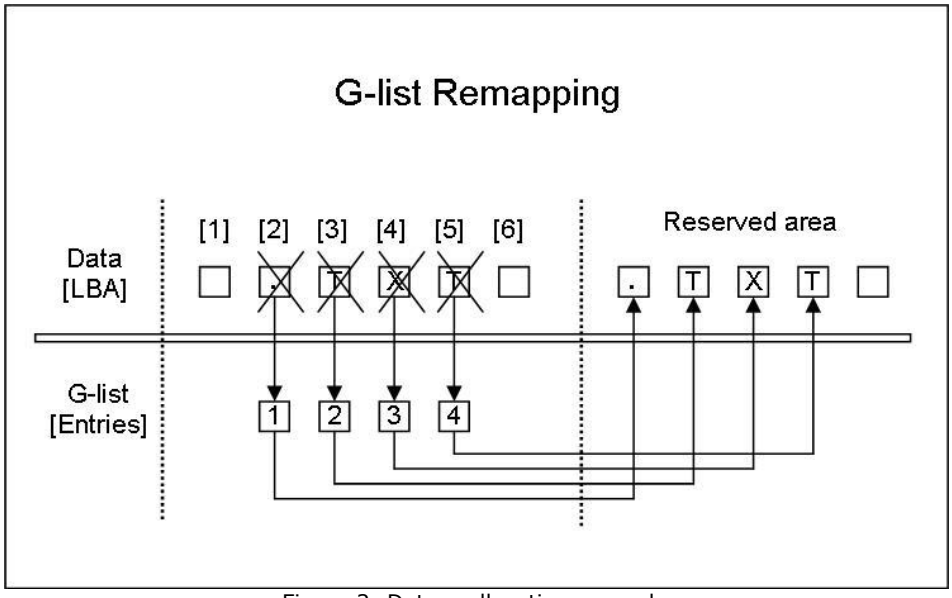


Figure 2: Data reallocation example

are automatically bypassed by the drive's logical translator and device electronics.

Steganography using Firmware

One aspect of this research is the possibility of the defect control system being manipulated to enable data to be concealed on the hard disk drive. This possibility was tested as part of the following experiment: A 3.5" Fujitsu Hard Disk Drive was populated with a Windows XP OS (NTFS File System) and a variety of mixed data files commonly located on a hard disk drive. The proposed method of steganography operates

"The data was not accessible"

'beneath' the file system and can be applied to any almost data in a physical sector on the drive. A randomly selected text file was chosen and edited to include a distinctive keyword. This was to enable the file to be searched for using standard commercial forensic tools. In the case of an investigation, the investigator would have a reasonable expectation to locate this keyword either on the original drive or in a forensically sound copy.

The particular model of the Fujitsu disk selected for this experiment supports two error lists in the firmware; one firmware list relating to production defects and another list relating to failing logical data tracks on the HDD. Typically all modern hard disk drives support this particular error handling function in some form. A specialist firmware analysis and repair tool was used to access and view the drive contents in order to locate the physical location (sector) for the text file. The selected tool can modify drive firmware, including error lists to effect repairs on malfunctioning drives. The firmware error list on the Fujitsu HDD relating to defective tracks (T-list) was modified using the data recovery tool to include an additional entry in the error list relating to the physical location of the modified text file.

The disk was rebooted and mounted. The Windows Operating System could no longer access the physical location (hidden data area) nor the text data once residing at that location. The drive firmware system would not permit access to this location and as the remapping process normally associated with a failing sector had not occurred; the data was not accessible. This was also confirmed via forensic copies of the HDD & hex editors (Winhex). What is more, after taking a forensic image of the drive, the specific keyword added to the file was not present in any searches performed on the drive using forensic search tools. The data was inaccessible by the forensic software, the computer operating system and the HDD itself. Therefore, data can be concealed beyond the reach of most commercial digital forensics tools.

The firmware recovery tool was again used to edit the track error list, returning it to its original state removing the previously added entry. The data area and text file containing the keyword was accessible on the drive. It should be noted that due to the error handling functionality being present on the vast majority of modern drives this behaviour would be repeatable on most drives to varying degrees in terms of the volume of data that could be contained in these sectors.

In addition to this highlighted area, further research has shown it is potentially possible to hide up to gigabytes of data on newer modern drives in different firmware systems.

Malicious modificaton of Firmware

The use of firmware tools for steganography purposes is fairly straightforward as outlined in the section above. A malicious user with a higher level of technical competency may be able to modify firmware to embed malware on the drive to prevent the correct operation of the drive.

Disk firmware provides low-level control of the drive. During a forensic investigation or when configuring a secure system, it is trusted and assumed to be operating correctly when supplied from the manufacturer. Malware engineered to target HDD firmware could prevent access to the data contained on the drive even with sophisticated data recovery tools and donor parts for physical rebuilds. This could be due to the malware targeting disk specific critical subsystems contained in the firmware, damaging the drive system logically, in certain cases beyond repair. There may also be a number of possible ways to damage the drive by either preventing firmware from operating normally or by modifying it to compromise the drives operation. Possible methods include disabling SMART systems, corrupting physical to logical translation tables, altering the AC current to the read/write heads to damage the circuitry or more difficult, but more destructive, would be to reduce the motor speed abruptly to destroy the air bearing causing a head-crash and damage to the disk platter. This kind of exploit would be developed and targeted at particular disks and systems and would act as a sophisticated method of sabotage that could render system inoperable and the data irrecoverable.

"Data can be concealed beyond the reach of most commercial digital forensics tools"

Forensic Impact

Currently there are a limited number of tools available to perform repair or modifications on HDD firmware. The available free / shareware tools that are capable of talking to the device at a lower level, in the case of HDD technology, are not currently powerful enough to perform such complex modifications. The high-end commercially available tools provide a finer degree of control, and access to a broader set of disk query / repair features. There are currently two main systems available for data recovery; firmware modification and repair. A complete suit for UDMA is supplied from Russia and costs approximately $10,000 for the UDMA toolset, although a more comprehensive tool suite is available with the ability to extract data from failing devices, work with SCSI & SAS drives, and USB / Solid-state devices is available. An alternative device is offered from China and can be obtained via resellers in Europe and America for approximately $450 per disk manufacturer. Either of these tools (also purchased by major PC manufactures for diagnostic & repair purposes) would enable a competent user to manipulate firmware to conceal data or code.

Firmware manipulation can have a significant impact on the forensic process. Data that has been hidden using firmware steganography techniques will not appear for analysis in a traditional forensic image created by on-the-market-software today. In the event of malware targeting and corrupting the firmware, this can potentially prevent the acquisition of a forensic image from the HDD. In the case of determining if the disk firmware has been tampered with or modified, the investigator would need to establish the provenance of the firmware. This is a challenging process, as the firmware implementation not only varies between manufacturers but also between the various models of the HDD. There are also portions of code unique to individual devices.

Detecting this form of misuse is potentially very difficult. The investigator would need to evaluate the drive against a comparable disk and perhaps use key firmware modules, from a donor drive to verify the firmware is valid or to use donor hardware components to

repair the original drive. This would however leave the problem of the error lists, which are unique to the drive although it is possible to clear all of the error lists present on the drive whilst still retaining some user data. The major problem lies in the ability to obtain and verify the error lists. The error lists and certain portions of the data contained in the firmware / system area are unique and disk model specific and therefore cannot be compared to another version of the disk.

Forensic Best Practice

These types of malicious techniques have the potential to impact upon forensic best practice and information security. The possibility of firmware modification emphasises the importance of retaining the original hard disk drive. It can be argued that the analysis of firmware for evidence of tampering is not appropriate in most investigations. This is due to the fact it is difficult and timing consuming (and therefore expensive) it would be unwarranted in most cases. Rather the investigator would need to consider the possibility of firmware tampering if there is evidence to suggest this may have occurred. This may be indicated by a combination of the suspect's technical expertise, the presence of certain hardware and software tools at the scene, digital footprints of tools, and suspected incomplete or missing evidential material. Where there are grounds for suspecting that a suspect may have modified drive firmware, then there are a number of actions proposed as best practice in this type of case that have been suggested by the author in previous research publications.

Conclusions

Highlighted is the concern that there is a potential for data to be concealed on a drive by manipulating the drive firmware. There is also the possibility for firmware to be modified for malicious purposes. There are a number of potential problems relating to the forensic analysis of malicious hard disk firmware modifications. Even with the correct tools it can be very difficult to find or reverse this type of modification. Hardware and software costs supporting this type of analysis are significant. The correct training is not widely available and is expensive to obtain. While this remains unlikely to impact the vast majority of forensic cases, the every present DIY Hacker mentality, organised crime and the increasing availability of the data recovery tools used to carry out this work makes it a real area for future concern.

This research ethic has also recently been focused of the malicious modification of NAND Memory devices such as USB & Solid-state storage devices, and their data recovery opportunities after device failure. The results have demonstrated that this new form of digital steganography is possible on these devices, and in some cases, have no potential cost-issue due to freely available resources. Other more alarming NAND firmware modifications will be published in the future.

Acknowledgement

The author would like to thank the members of the Information Security Research Group (IRSG) at the University of Glamorgan, UK.

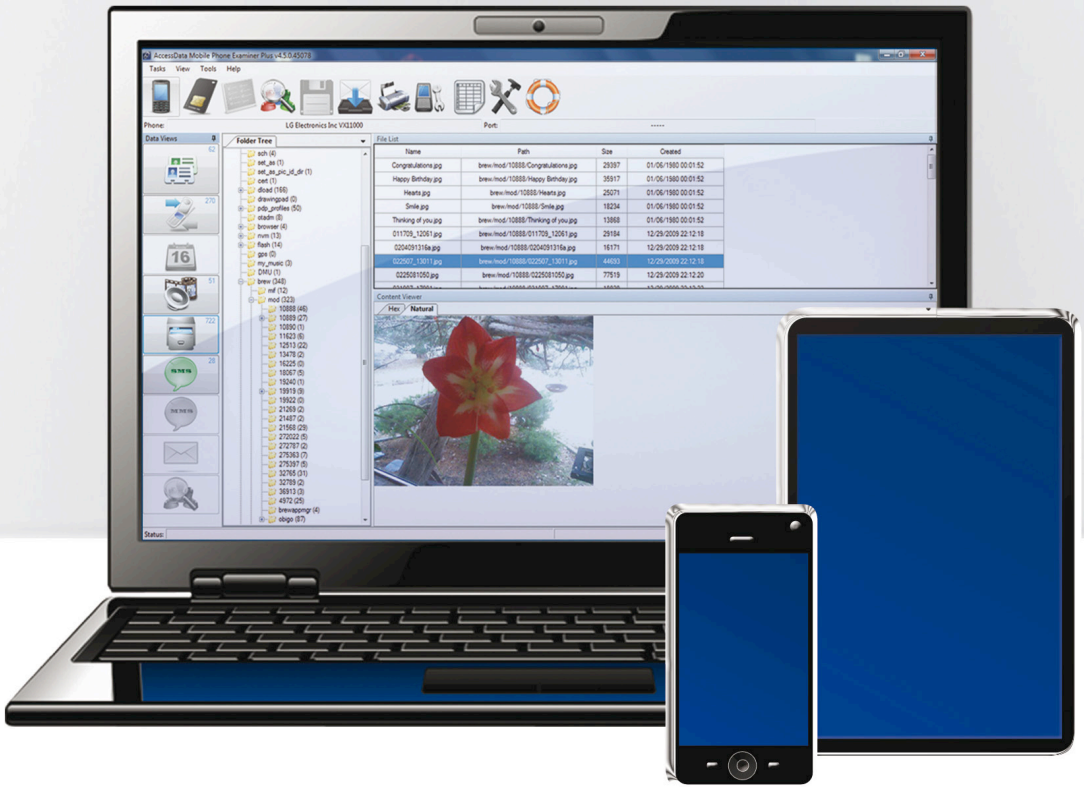
Author Biography

Mr. Gareth D. O. Davies is a Lecturer & Researcher in the Information Security Research Group (ISRG) at the Faculty of Advanced Technology, University of Glamorgan, UK. Mr. Davies also holds an Adjust Lecturer position at the SecAU Centre at Edith Cowan University, Australia. The main focus of his research is the security and forensic analysis of HDD & NAND technology. Mr. Davies lecturer's on the Computer Forensics undergraduate & postgraduate degrees at Glamorgan University and has been involved in a variety of other research projects in the area of Computer Forensics and Information Security. Mr. Davies is an active Consultant and Investigator on forensic and disk recovery technology cases at both of his respective Universities. Mr. Davies is a member of professional computer forensic bodies such as the UK First Forensic Forum & the International Association of Digital Forensics, Security and Law.

UPGRADE TO ACCESSDATA

GET FTK® OR MOBILE PHONE EXAMINER *PLUS*® FOR JUST $840

Replace your common computer forensics and mobile forensics tools with FTK and MPE+ to achieve an uncommon digital investigations experience.



Make the switch now...

http://UpgradeToAccessData.com

AccessData®

4:WARD

So, that's it for this issue. It was a long time in the making and we've learned a lot from doing this but we're just getting started.

We want to make this the de facto publication for digital forensics and I believe that, with your help, it is possible.

In order to make this venture a success we need input, not just comments and suggestions about the magazine itself (which are more than welcome) but we need contribution.

Now that you've seen what we have to offer maybe you feel that you have something to contribute. It doesn't matter whether you are a forensicator, a student, incident responder, or eDiscoverer (I guessed at that last one). If you think something is important or you have an idea for a section that you'd like to "own" in each issue please get in touch.

Here's the kind of thing we have in mind:

Product Reviews, Guides, Tips and Tricks, Technical Articles, News Items, Interviews, Case Studies, etc.

Whether you are interested in contributing only once or you want to be a regular part of the magazine we'd love to see what you have to offer.

Please send your ideas to:

lee@forensic4cast.com

FORENSIC COMPUTERS

http://www.forensiccomputers.com
Phone: (540) 726-9530
Email: info@forensiccomputers.com

Serving the Digital Forensic Community Worldwide

4:mag

a production of 4:sight