

# eForensics

## Magazine

**COMPUTER**

**VOL.2 NO.2**

# FORENSICS ANALYSIS with FTK

**50+  
PAGES**

**DIGITAL FORENSICS 101: Case Study Using FTK Imager |**

**FORENSIC APPROACHES TO ENCRYPTED DISKS |**

**HOW TO DETECT SYSTEM INTRUSIONS |**

**INTERVIEW OF CYBER LAWYER FERNANDO M. PINGUELO |**

**COMPUTER FORENSIC CERTIFICATIONS EXAMINED |**

# AnDevCon

The Android Developer Conference

**BOSTON** • May 28-31, 2013

The Westin Boston Waterfront

Get the best real-world Android developer training anywhere!

- Choose from more than 75 classes and tutorials
- Network with speakers and other Android developers
- Check out more than 40 exhibiting companies

Register Now  
and SAVE!

"AnDevCon is one of the best networking and information hubs available to Android developers."

—Nate Vogt, Android Developer, Willow Tree Apps



Register NOW at [www.AnDevCon.com](http://www.AnDevCon.com)

A BZ Media Event

Follow us: [twitter.com/AnDevCon](https://twitter.com/AnDevCon)

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.





Get the scoop on  
SharePoint 2013!

March 3-6, 2013 → San Francisco



**Register Early and SAVE!**



# The Best SharePoint Training!



Choose from over  
**90 Classes & Workshops!**

Check out these **NEW!** classes,  
taught by the industry's best experts!



**Check out more than  
55 exhibiting companies!**

How to Install SharePoint 2013 Without  
Screwing It Up

Todd Klindt and Shane Young

What IS SharePoint Development?  
Mark Rackley

SharePoint Performance: Best Practices  
from the Field  
Jason Himmelstein

Creating a Great User Experience in  
SharePoint

Marc Anderson

Ten Best SharePoint Features You've  
Never Used

Christian Buckley

Understanding and Implementing  
Governance for SharePoint 2010  
Bill English

Building Apps for SharePoint 2013  
Andrew Connell

SharePoint Solutions with SPServices  
Marc Anderson

Lists: Used, Abused and Underappreciated  
Wes Preston

Planning and Configuring Extranets in  
SharePoint 2010  
Geoff Varosky

Creating Simple Dashboards Using  
Out-of-the-Box Web Parts

Jennifer Mason

Integrating SharePoint 2010 and Visual  
Studio Lightswitch  
Rob Windsor

Solving Enterprise Search Challenges with  
SharePoint 2010

Matthew McDermott

Getting Stuff Done! Managing Tasks with  
SharePoint Designer Workflows

Chris Beckett

SharePoint 2013 Upgrade Planning for  
the End User: What You Need to Know  
Richard Harbridge

Ten Non-SharePoint Technical Issues  
That Can Doom Your Implementation  
Robert Bogue

SharePoint MoneyBall: The Art of Winning  
the SharePoint Metrics Game  
Susan Hanley

Intro to Branding SharePoint 2010 in the  
Farm and Online

Randy Drisgill and John Ross

How to Best Develop Requirements for  
SharePoint Projects  
Dux Raymond Sy

**Lots more online!**

A BZ Media Event



Follow us: [twitter.com/SPTechCon](https://twitter.com/SPTechCon)

SPTechCon™ is a trademark of BZ Media LLC.  
SharePoint® is a registered trademark of Microsoft.

**[www.sptechcon.com](http://www.sptechcon.com)**

**Editors:** Joanna Kretowicz  
[jaonna.kretowicz@eforensicsmag.com](mailto:jaonna.kretowicz@eforensicsmag.com)

**Betatesters/Proofreaders:** Roxana Grubbs,  
Kishore P.V , Vaman Amarjeet, Mada R Perdhana,  
Olivier Caleff, Jeff Weaver, Massa Danilo, Craig Mayer,  
Andrew J Levandoski , Richard Leitz, Lee Vigue

**Senior Consultant/Publisher:** Paweł Marciniak

**CEO:** Ewa Dudzic  
[ewa.dudzic@software.com.pl](mailto:ewa.dudzic@software.com.pl)

**Art Director:** Ireneusz Pogroszewski  
[ireneusz.pogroszewski@software.com.pl](mailto:ireneusz.pogroszewski@software.com.pl)

**DTP:** Ireneusz Pogroszewski

**Production Director:** Andrzej Kuca  
[andrzej.kuca@software.com.pl](mailto:andrzej.kuca@software.com.pl)

**Marketing Director:** Joanna Kretowicz  
[jaonna.kretowicz@eforensicsmag.com](mailto:jaonna.kretowicz@eforensicsmag.com)

**Publisher:** Software Media Sp. z o.o. SK  
02-682 Warszawa, ul. Bokserka 1  
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!

We would like to present the latest issue of eForensics Computer.

As our magazine is a professional writing directed mainly to experts in digital forensics, this time we decided to give a chance to all enthusiasts interested in that field who would like to become experts. Beginning with this issue, we will provide you with basics of a particular eForensics topic. Beginners' Section opens with Dauda Sule's article, presenting Case Study with FTK Imager. He teaches you basic understanding of what digital forensics is, which applications you can use as well as the basic process of digital forensics investigation.

In the opening article Omar Al Ibrahim and Majid Malaika cover the subject of Forensics Analysis with FTK on more advanced level. They present this very delicate process that requires deep understanding of both legal and technical aspects and includes the knowledge of the right procedures and tools to conduct forensics analysis. They elaborate on these steps using a case study of a hypothetical scenario.

It's an old adage that security measures mean little if an attacker has physical access to your machine, however, things like disk encryption pose significant forensic challenges. In the following article Chris Domain explains you why and talks about Forensics Approach to Encrypted Discs.

In the next article our expert Almantas Kakareka presents insight into different techniques and tactics of detecting system intrusions. One character in the output may be the only difference between clean and compromised box. He shows how and where to look for intrusion artifacts and how to defend them.

Getting back to interview section, this time we've talked with Cyber Lawyer Fernando M. Pinguelo, who created and developed his law firm's cyber security and data protection law practice group. Fernando explains what are the most pressing data issues facing his clients and businesses in general. He presents his team too.

In the last article our expert Terrance J. Stachowski explores a range of popular certifications applicable to computer forensics. He examines various types of available certifications, certification bodies, topics covered in the certification exams, requirements for continued certification and associated costs.

Taking advantage of this publication we would like to ask you for cooperation. Our aim is to be "your" magazine, a helping hand when you need one and entertainment when you want to forget about your job and follow your passion. What are the topics you would like us to cover? Tools you would like to read about? Please share your needs and expectations towards our publications! We would like to ask you for feedback concerning our work. Please, follow us on Twitter and Facebook, where you can find the latest news about our magazine and great contests. Do you like our magazine? Like it, share it! We appreciate your every comment!

Joanna Kretowicz  
& eForensics Team



## FORENSICS ANALYSIS WITH FTK: A CASE STUDY SCENARIO

by Omar Al Ibrahim and Majid Malaika

Digital forensics is the process of recovering, preserving, and examining digital evidence in a way admissible in a court of law. This process is very delicate and requires deep understanding of both legal and technical aspects which includes knowing the right procedures and tools to conduct forensics analysis. In this expository article, we walk through the steps of the forensics process using FTK. We elaborate on these steps using a case study of a hypothetical scenario.

06

16

## DIGITAL FORENSICS 101: CASE STUDY USING FTK IMAGER

by Dauda Sule

It is quite remarkable how digital evidence can be used to solve crimes, even if not committed directly using digital devices and platforms. This article tries to give a basic introduction to digital forensics. It focuses on how to retrieve data, covering basic steps on collection digital evidence using simple digital forensics tools.

## FORENSIC APPROACHES TO ENCRYPTED DISKS

by Chris Domain

Did you know that “on the fly encryption” products keep keys in memory? Or that RAM doesn’t clear the second that it loses power? Some novel techniques take advantage of these facts to maintain access to encrypted disks. It’s an old adage that security measures mean little if an attacker has physical access to your machine, however things like disk encryption pose significant forensic challenges. The good news for forensic examiners is that great progress has been made in accessing OTFE disks.

24

30

## HOW TO DETECT SYSTEM INTRUSIONS

by Almantas Kakareka

We want to detect system intrusion once attackers passed all defensive technologies in the company, such as IDS/IPS, full packet capture devices with analysts behind them, firewalls, physical security guards, and all other preventive technologies and techniques. Many preventing technologies are using blacklisting most of the time, and thus that’s why they fail. Blacklisting is allowing everything by default, and forbidding something that is considered to be malicious. So for attacker it is a challenge to find yet another way to bypass the filter. It is so much harder to circumvent a whitelisting system.

## INTERVIEW OF CYBER LAWYER FERNANDO M. PINGUELO

by Joanna Kretowicz

Class actions are one of the hot button cyber issues of the day – or at least the one that seems to grab the headlines. For example, around the time of the Facebook IPO, a class action lawsuit involving Facebook’s improper use of users’ personal data for advertisement purposes dominated the headlines, and was a contributing factor to Facebook’s sluggish stock price.

44

48

## COMPUTER FORENSIC CERTIFICATIONS EXAMINED

by Terrance J. Stachowski, CISSP, L|PT

The computer forensics community, much like every other realm of information technology, places a high value on certifications as one way to validate competency and proficiency with best practices, knowledge of related tools, and computer forensics procedures. This article explores a range of popular certifications applicable to computer forensics. Examined are various types of certifications available, certification bodies, topics covered in the certification exams, requirements for continued certification, and associated costs.



# FORENSICS ANALYSIS WITH FTK

## A CASE STUDY SCENARIO

by Omar Al Ibrahim and Majid Malaika

Digital forensics is the process of recovering, preserving, and examining digital evidence in a way admissible in a court of law. This process is very delicate and requires deep understanding of both legal and technical aspects which includes knowing the right procedures and tools to conduct forensics analysis.

### What you will learn:

- Basics of forensic analysis process.
- Effective technical procedures to create and analyze forensic images using FTK
- Hands-on exercise using example forensics case scenario

### What you should know:

- Basic knowledge of Windows platform, its directory structure, mounting drives
- Basic knowledge of cryptographic hash algorithms.

**F**TK is a forensics toolkit used for digital investigation. Developed by AccessData, this toolkit consists of many useful modules including a standalone application, FTK Imager, a concise tool which provides hard disk imaging that can be exported using a file or a set of segments. FTK Imager also provides integrity checking by calculating hash values on data segments of an image. In this expository article, we walk through the steps of the forensics process using FTK. We elaborate on these steps using a case study of a hypothetical scenario.

Before starting the reader is advised to visit and download FTK and FTK Imager at <http://www.accessdata.com/support/product-downloads>.

The current release of FTK is v4.1 (as of the date of this article). You can download the demo version of

this tool to walk through the exercises. Alternatively, you can download FTK Imager which is available free of charge once you register to the site. Incidentally, there are two types of releases: Imager and Imager Light.

### A CASE STUDY SCENARIO

The scenario goes like this. You have been engaged by Mastagni, Holstedt, Amick, Miller, Johnsen & Uhrhammer (the Firm) to examine the laptop of a former employee of the California State University Observatory. They represent Charles Messier (let's assume that an age of 279 years is not too old to draw a salary from a California public university) in a wrongful termination action. Messier has been accused of stealing several deep sky objects. Another employee of the Observatory, Pierre Mechain, has claimed ownership of the objects.



The Observatory backs Mechain's claim and as a result fires Messier.

Upon his termination on 9/11/2002, Messier returns the laptop to the Observatory. He claims to have retained a flash drive device with his own files on it. The CSU-Observatory used an in-house IT staff to image the contents of the laptop hard disk drive. However, his report on the image is unclear and his chain of custody is missing. Assume you have personally imaged Partition 1 from the flash device Messier provided to Mastagni.

Now we start the forensic analysis using `messier.e01` image. You can download a copy of the image at <http://www.sendspace.com/file/lrqtz8>. The hash value for the download:

```
MD5: cd1d15dfbedf59f697559122829e7303
SHA1: 2d60ffdd2f5f1285fed92680b9c7013a56731aba
SHA256: c03457655a920c2823b3db0c611e80e393ccb2659
7f5b3f6a17a7122940e61d0
```

## FORENSICS PROCESS

From a big picture, the digital forensics process consists of various steps necessary to complete the examination. These basic steps include: 1. An *acquisition*



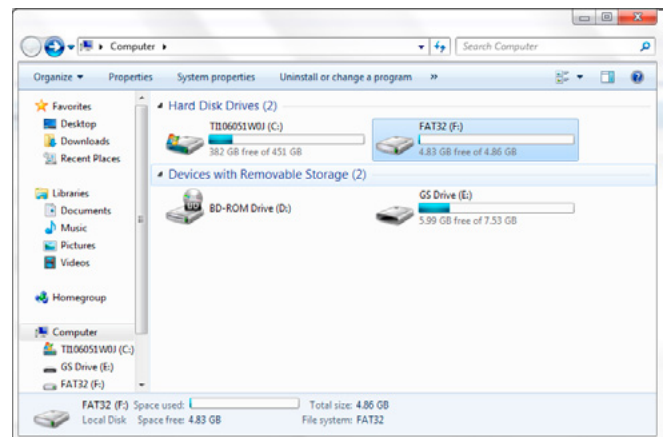
**Figure 1.** Digital Forensics Process

*quisition* step to seize the evidence from the target digital media, 2. An *imaging* step to copy the data from the evidence into a separate drive for analysis without altering the original content. 3. An *analysis* step to apply the forensics tools and techniques to gathering and investigating the information. Finally, 4. a *reporting* step where the gathered information is prepared for legal testimony (Figure 1).

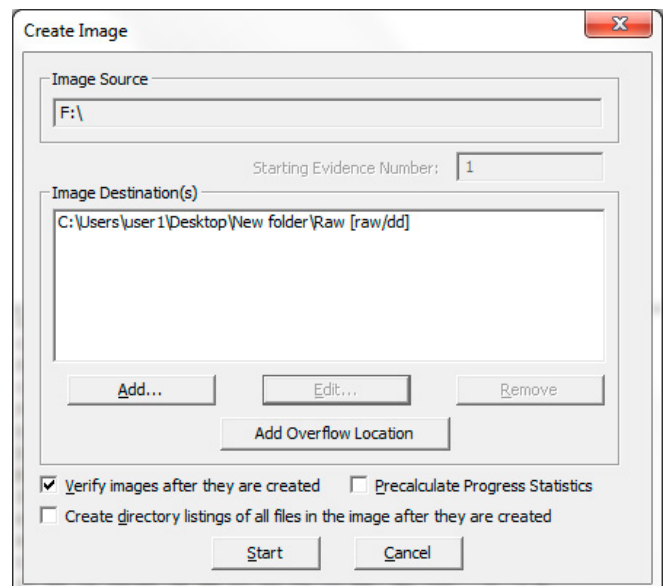
## STEP 1: ACQUISITION

For digital computer evidence to be valid it must be gathered, tracked and preserved in its original form to be admissible in a court of law. There are two ways to analyze the media without tampering with the original evidence: by creating a copy of the suspect drive using hardware devices or by using software applications. Hardware acquisition tools duplicate disk drives or allow read-only mode access to a hard drive. The preferred method to protect the evidence is to duplicate the media to a clean wiped drive, verify and analyze the duplicate instead of the original media.

To preserve the evidence in our example we created a raw (dd) image of the Messier flash drive



**Figure 2.** Mapping Flash Drive Image



**Figure 3.** Creating a Raw Duplicate Copy

(F:) shown in Figure 2. The ultimate approach is to use write blocker devices to avoid any accidental modification to the evidence in hand.

Upon opening FTK Imager go to *File* and choose *Create Disk Image*. The FTK wizard will start with “*Select Source*” page with the following options:

- *Physical Drive*: choose this option to create an image for an entire physical drive with all its partitions and unpartitioned spaces.
- *Logical Drive*: choose this option to create an image for a specific logical drive or partition.
- *Image File*: choose this option to create an image from another image type.

In this example we chose *Logical Drive* and selected drive (F:), i.e. the Messier flash drive, and followed the FTK wizard to set the destination and file name of the raw image. In addition, we had the option to encrypt the image and provide our own keys, or passphrases. As shown in Figure 3, the destination was filled and we chose to “*Verify images after they are created*”. This generated a report after creating the image comparing the hash values of the image and the original evidence.

## AUTHENTICATION OF DATA

Hashing refers to the process of generating a unique value based on a file’s content. From a

### Listing 1. FTK’s report

```
Created By AccessData® FTK® Imager 3.1.2.0

Case Information: Messier Case
Acquired using: ADI3.1.2.0
Case Number: 9961836823
Evidence Number: 1
Unique Description: Messier USB
Examiner: Omar and Majid
Notes: Raw (dd) image Acquired from the Actual Flash Drive

-----

Information for C:\Users\user1\Desktop\New folder\ImageFromRaw\Image:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 10,233,342
[Image]
Image Type: Raw (dd)
Source data size: 4996 MB
Sector count: 10233342
[Computed Hashes]
MD5 checksum: f176f40b6bccd2347d575fec496df70f
SHA1 checksum: b5c9b535abdddc75f7638f8fd12d79447e09b661

Image Information:
Acquisition started: Mon Jan 04 21:26:08 2013
Acquisition finished: Mon Jan 04 21:26:59 2013
Segment list:
C:\Users\user1\Desktop\New folder\ImageFromRaw\Image.E01

Image Verification Results:
Verification started: Mon Jan 04 21:26:59 2013
Verification finished: Mon Jan 04 21:27:31 2013
MD5 checksum: f176f40b6bccd2347d575fec496df70f : verified
SHA1 checksum: b5c9b535abdddc75f7638f8fd12d79447e09b661 : verified
```



cryptographic sense, hash values are used to verify file integrity and identify duplicate and known files. Two hash functions are available in FTK and FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1). The hashing options are selected automatically by FTK. Typically, you hash individual files to compare the results with a known database of hashes. However, you can also hash multiple files or an image to verify that the working copy is identical to the original. You can create hashes with FTK Imager or FTK.

Once FTK completes the duplication process by creating a raw (dd) image of the Messier flash drive it verifies the newly created file against the original flash drive as shown in Figure 4; the MD5 and SHA1 digest of the newly created raw image matches the original flash drive's hashes respectively.

In addition to the quick result window shown in Figure 4, FTK creates a report and saves the data as a text file within the image destination. This is the text file generated after successfully creating the raw image of the Messier flash drive (Listing 1).

## STEP 2: IMAGING

Imaging is the process of copying the data of a digital evidence to an analysis drive and providing

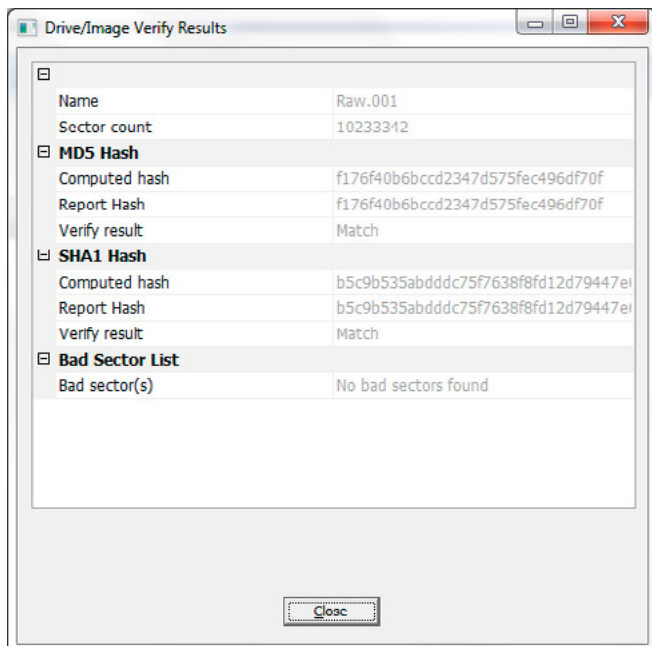


Figure 4. Verifying Data in Duplicate Copy

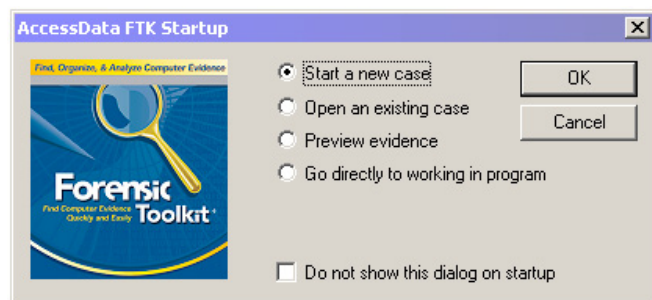


Figure 5. New Case Wizard (FTK)

checksum to verify the integrity. This process comes after the acquisition step where the actual evidence is seized by law enforcement. Below, we describe the steps to carry out the imaging step using FTK.

## STARTING A NEW CASE IN FTK

You access the New Case Wizard by selecting *File*, and then *New Case* (Figure 5). If this is your first time opening FTK or if you have chosen to always display the FTK Startup screen, select *Start a New Case* and click *OK*. To start a new case, you must complete the following steps.

- Enter basic case information.
- Check what you want to be included in the case log.
- Check the processes that you want to run on the evidence, as shown in Figure 6
- Select the criteria for adding evidence to the case.

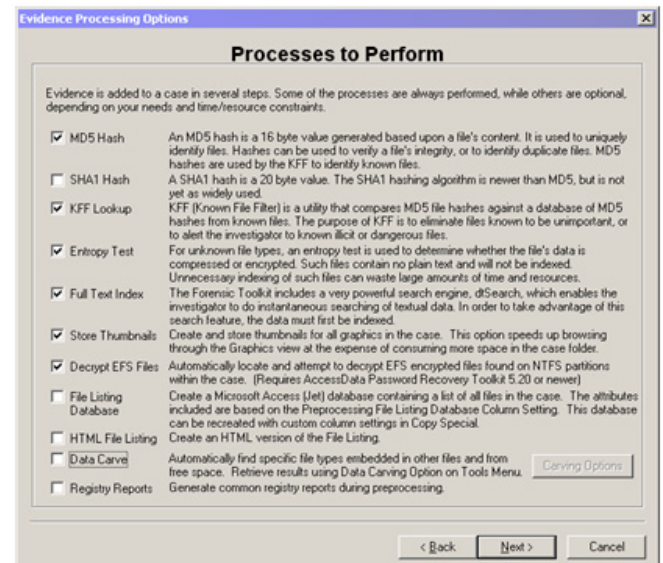


Figure 6. Process Selection Dialogue (FTK)

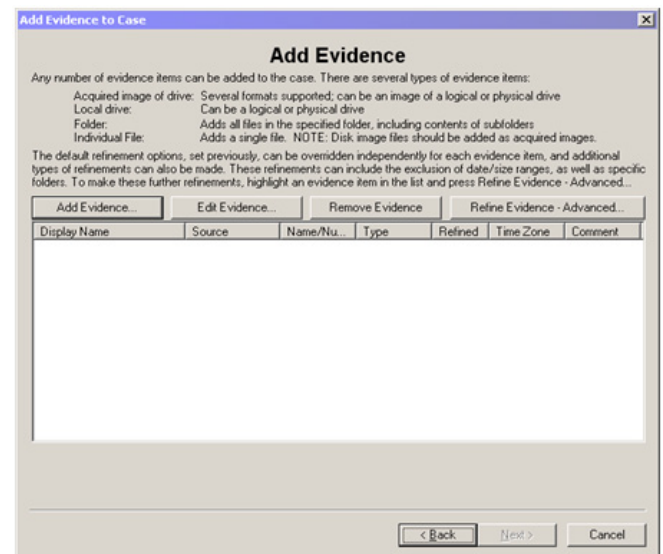


Figure 7. Add Evidence Dialogue (FTK)

- Select the criteria for creating the index.
- Add the evidence (Figures 7 and 8).
- Review your case selections.
- Complete the wizard to launch the processing of evidence.

## CREATING A NEW IMAGE WITH FTK IMAGER

To create a new image as part of the imaging process go to: *File ->* and select *Create Disk Image*. Then choose *Image File* as the source, and select the raw (dd) image created during the acquisition process. In addition, choose an image type and click *OK*. You also need to define the image destination, file name, and also verify the newly created image against the raw (dd) acquired by comparing the MD5 and/or SHA1 digests before analyzing the data.

In the Messier example, we created a new E01 image from the raw (dd) image acquired as shown in Figure 9.

At this stage we have in our possession an identical image of the object to launch an analysis in a forensics investigation. As shown in Figure 10, FTK Imager builds the tree of evidence showing all folders and subfolders.

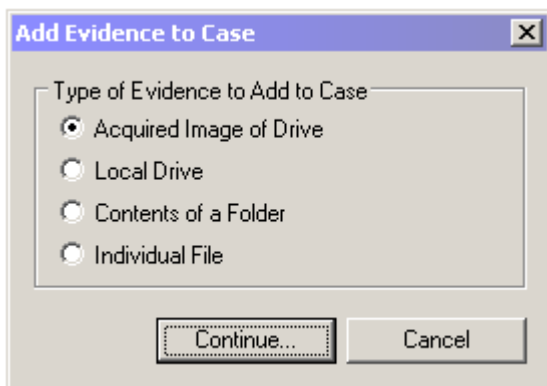


Figure 8. Add Evidence Popup (FTK)

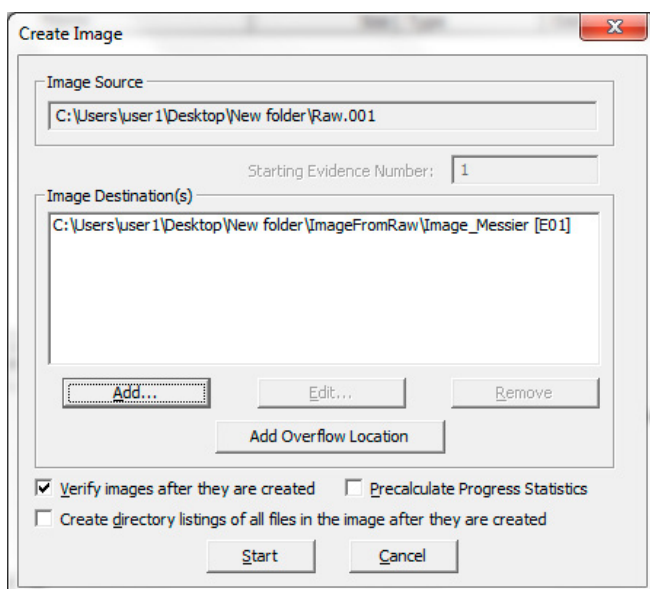


Figure 9. Imaging Process (FTK Imager)

## WIPING THE ANALYSIS DRIVE

Digital forensic examiners usually re-use drives during their investigations. Therefore, it is crucial to wipe the analysis drives before starting a new case. The standard format for wiping used in most modern operating systems is insufficient to prevent data from leaking out or being associated to a new case by mistake. Therefore, reliable wiping tools must be used to ensure data blocks are completely wiped. These tools overwrite data blocks in several rounds (DoD standard requires overwriting data blocks 3 times with zeros, ones or random bits).

In the Messier example, we used a wipe utility in Linux to ensure data contained in E01 and raw (dd) images were completely wiped.

## STEP 3: ANALYSIS

The analysis section is the core component of the forensics process. So far, we have described the forensics acquisition and imaging steps, starting from seizure of the target media to imaging the evidence into a separate drive for analysis. The techniques involved in a forensic examination can be classified into clever searching and data carving techniques. Let us take the example of the Messier case to illustrate these techniques.

In the Messier case, three partitions are available for examination namely Partition 1, Partition 2 and Partition 5 (possibly out of five partitions total). Partition 1 is the image of Messier's flash drive which we have acquired in the previous steps. Partitions 2 and 5 are part of Messier's laptop hard drive imaged by CSU- Observatory.

Let us exploit our forensics techniques to investigate this case.

## KEYWORD SEARCHES

One of the basic principles in digital forensics is to always go for the easy way. As simple as it may sound, the easy way of extracting information from digital content is to perform searches for basic keywords relevant to the investigation.

To carry out searches in FTK go to the *Search* tab. You will notice that we can carry out an in-

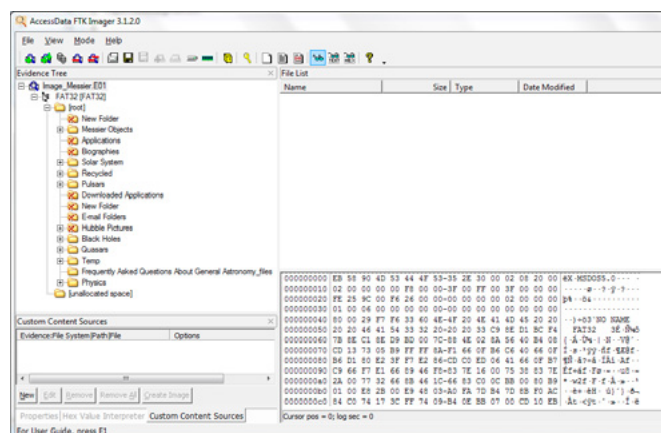

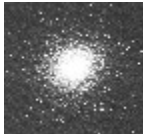





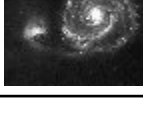


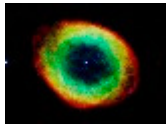

Figure 10. Evidence Tree (FTK Imager)



dexed search to give the number of recurrences for each search term and bookmark these searches. For example in our Messier investigation, we may search for the keyword “Pierre Mechain” in the evidence to see his involvement in the case. As shown in the figure below, “Mechain” is mentioned 183 times as part of documentation of discoveries with Messier. Specifically, he was mentioned 10 times in text of letter documents and web pages of Partition 1 and 3 times in hyperlinks and web pages of Partition 5. The remaining searches are in Partition 2.

To gather more information, we can also utilize more search terms such as Messier objects and Royal Society. As an example, we examined the flash drive image we created previously to find all photos of Messier objects. In the discovery production, we have found the following thumbnails on the flash drive:

| Object name | Image   |
|-------------|---|
| M1          |   |
| M2          |  |
| M8          |  |
| M20         |  |
| M27         |  |
| M31         |  |
| M45         |  |
| M51         |  |

|     |   |
|-----|---|
| M57 |  |
| M83 |  |

## UNALLOCATED FOLDERS AND FILES

In most operating systems a delete function only unlinks the pointer to a file from the physical location on the drive. Hence, the actual data blocks of the file remain on the physical drive and can be recovered partially or fully provided that the physical data blocks were not overwritten.

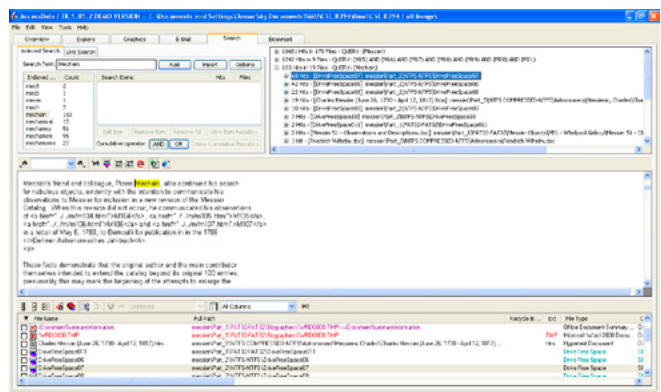
In the Messier example, FTK Imager marks the deleted files and folders with a small x as shown in Figure 11. These files/folders can be exported and recovered by right clicking on the file and choosing *Export Files...*

Similarly in FTK, these files can be bookmarked by right-clicking on the file and choosing *Add Bookmark...*

As mentioned, the delete function does not wipe out the data blocks associate with a file from the physical drive, but releases the physical blocks allocated to the pool of free disk space. In some cases, the data segments will remain intact, keeping the file uncorrupted, while in other cases a portion of the blocks may be overwritten, thus corrupting the file. Using FTK Imager an examiner can attempt to recover the remaining data of a file but will have to determine the file type.

In the Messier example, we recovered some of the files as shown in Figure 12. These files have no file type signature (magic numbers) to indicate its format. This is likely because some of the data segments were overwritten as they are associated with other files in the filesystem. In this example we were able to identify the data segment# 129042 from the signature highlighted below.

FF D8 FF E0 XX XX 4A 46 is known to be the signature for JPEG, JPG, JPE and JFIF which match-



**Figure 11.** Searching Keyword “Mechain” in the Evidence (FTK)

es the unallocated segment# 129042. It is also known that JPEG, JPG, JPE and JFIF file types should end with FF D9, but in this case the unallocated segment does not end with FF D9, which explains why FTK Imager was not able to identify a file type.

To prove this hypothesis, we exported the unallocated segment#129042 and appended .JFIF to the file name and then opened the file with an image viewer. We were able to view and recover around 85% of the image from the unallocated segment as shown in Figure 13 by examining and comparing the signatures.

## SYSTEM DIRECTORIES AND FILES

Searching for system files and directories include boot directories and files related to account management, permissions, system configuration, as well as installed programs and settings.

In this examination, we notice that Windows is used as the operating system on the Messier disk drive. We also notice that the disk drive was tampered with during the process of imaging by CSU. Specifically, the WINDOWS folder is missing from the disk partitions making the image unbootable, at least not without extensive repair. The registry

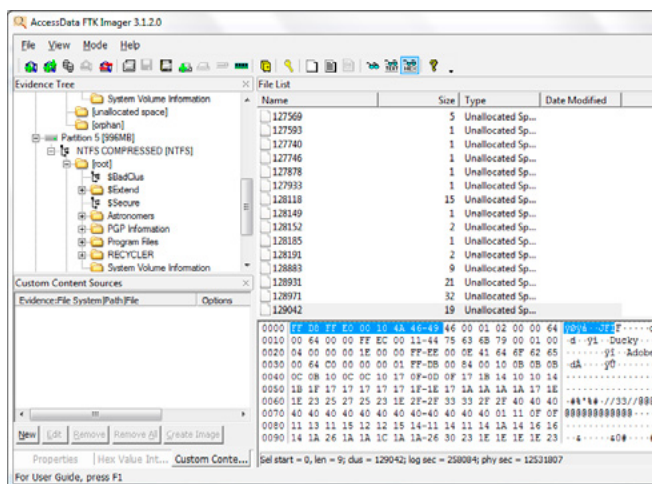


Figure 12. Unallocated Space (FTK Imager)

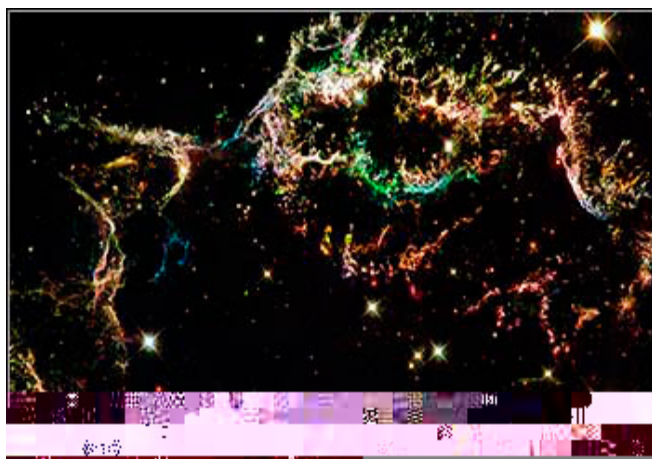


Figure 13. Recovered JFIF file

files: SAM, Software, System and Security files usually located under the file path *WINDOWS/system32/config/* are unavailable for registry view analysis. Typically, when a portion of the evidence is missing, as in this case, we need to examine the timestamps for any modifications or tampering on the file system.

Examining the contents of the Recycle folder, we find remnants of the Windows system directory tree, as shown in the figure above. Restore points were used on the laptop hard disk, one of them having a modification date of 9/12/2002, one day after Messier's termination and submission of the laptop.

## APPLICATION DATA

Another source of valuable information is to examine application data. This includes emails, browser history, calendar appointments and so forth. Let us take the example case to illustrate how useful application data can be to prove that the laptop image belongs to Messier. In Partition 2 of the image, we found an *Email* folder which consists of directories of multiple email clients: Microsoft Outlook, Outlook Express, and AOL. We observe that the laptop includes a webmail application and email clients to manage Messier's email accounts: *cmessier1730@aol.com* and *cmessier@hotmail.com*. Messier has used the laptop to read and send out emails from these accounts. His email activity provide evidence that he used the laptop and his Outlook account shows 8 appointments being scheduled using the calendar feature as shown under the *Email/Outlook/Top\_of\_Personal\_Folders/Calendar* directory. Finally, the Internet Explorer browser history (*index.dat*), found in Partition 2 under *Email/History/History.IE5*, displays the username *cmessier* as the logged in user when these web browsing activities took place.

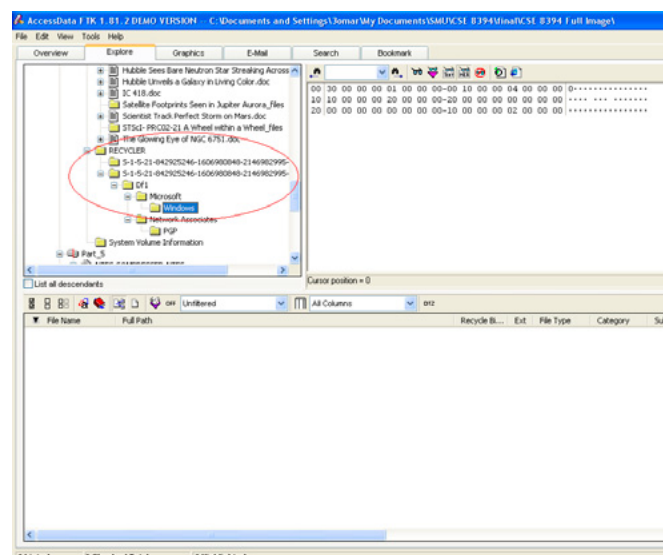


Figure 14. Windows System Directory under Recycle Bin (FTK)



## ENCRYPTION KEYS

Encryption is one of the widely used and effective methods to hide and obfuscate data in the digital world. A forensic case could take substantial amount of time analyzing encrypted data in an attempt to figure the encryption algorithm, key, and block size used. Thus, searching for encryption keys will assist greatly in figuring the encryption scheme used; giving the examiner enough clues to decrypt and investigate the data. Encryption keys can be identified by file type like .key, .skr, .pkcs12 and .pfx. Other clues can be figured from file sizes and the string's length. From the Messier example, we were able to locate what seems like PGP private and public keys (.skr and .pkr) under Partition 5 [/root]/PGP Information/PGP directory path as shown in Figure 15.

## STEP 4: REPORTING

After completing the forensic investigation, the examiner is required to produce a complete report describing the findings to the client. A complete and solid report includes detailed process notes, extracted files, timestamps of each finding, and screenshots. The report should include an overview, acquisition, preparation steps, findings and finally a conclusion.

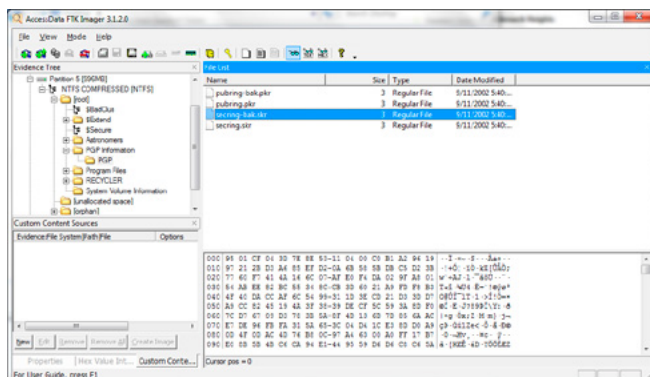


Figure 15. Locating Cryptographic Keys (FTK Imager)

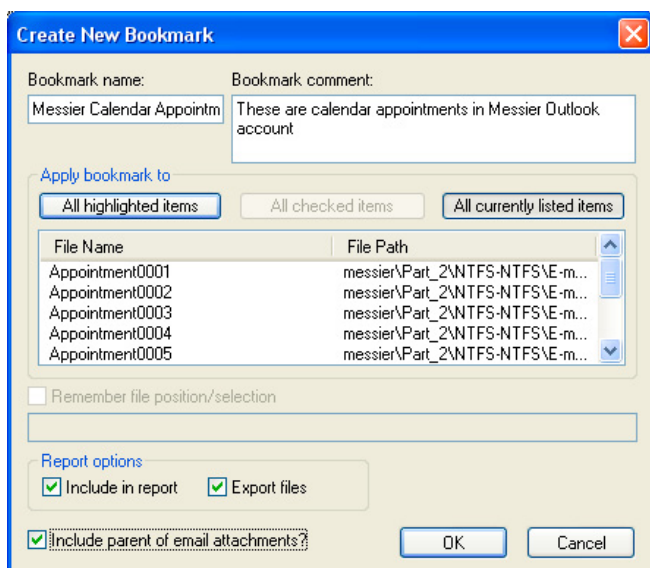


Figure 16. Including Bookmarks in Report (FTK)

The forensics report must be technically detailed at the same time simple to comprehend since it may be presented to cross-examiners, jury or a judge. Examiners may be asked to testify few weeks or even years after the investigation was carried out; therefore, a complete and detailed report always assist the examiner into increasing the value of digital evidence into the legal realm.

FTK can help with reports by cataloguing bookmarks and linking them to files and images. To include a bookmark to an FTK report, go to the **Bookmark** tab, select a bookmark and check "Include in Report" on the right pane (Figure 16).

To create a report, FTK provides the Report Wizard. You can access the Report Wizard by selecting **File**, and then **Report Wizard**. The wizard takes you through multiple steps (Figure 17-18):

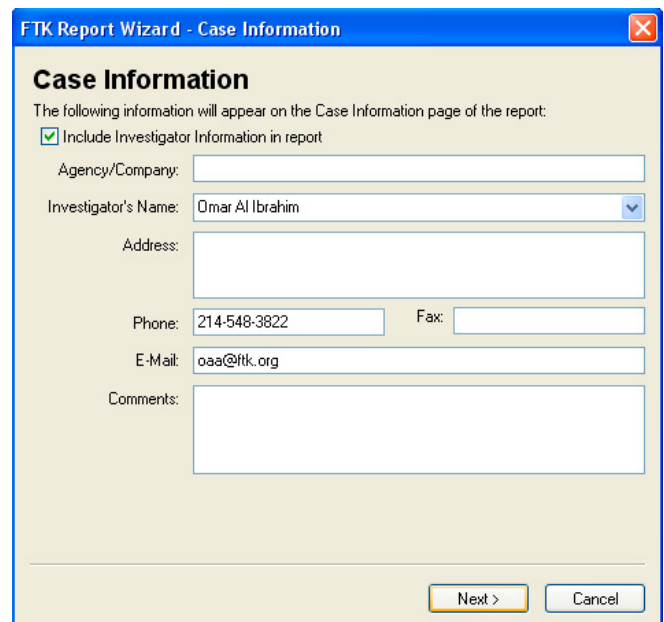


Figure 17. FTK Report Wizard – Case Information (FTK)

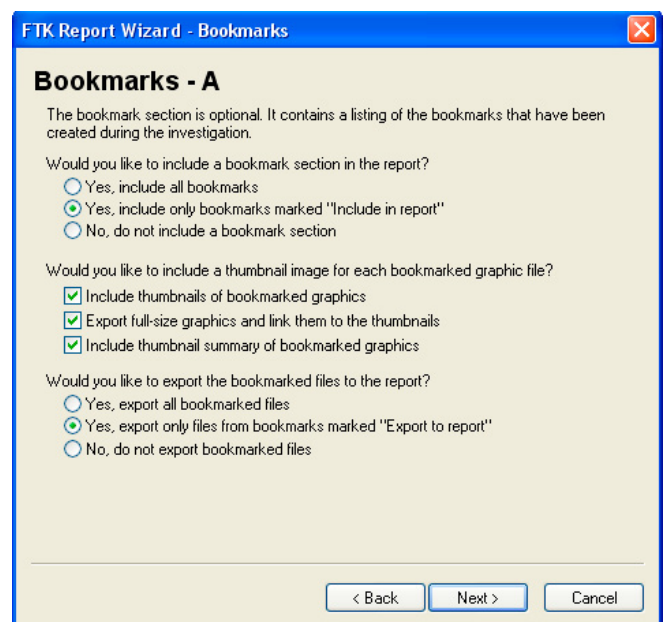


Figure 18. FTK Report Wizard – Bookmark (FTK)

- Enter basic case information.
- Decide how to handle bookmarks.
- Select the properties of bookmarks.
- Decide how to handle graphic thumbnails.
- Decide if you want a file path list.
- Decide if you want a file properties list.
- Select the properties of the file properties list.
- Add *supplementary files* and the case log.

- Add the *Registry Viewer* report or a *custom graphic* to the report and select the *report location*.

Upon completing bookmarking, FTK then generates the HTML report with the case and examiner information as shown in Figure 19. FTK also gen-

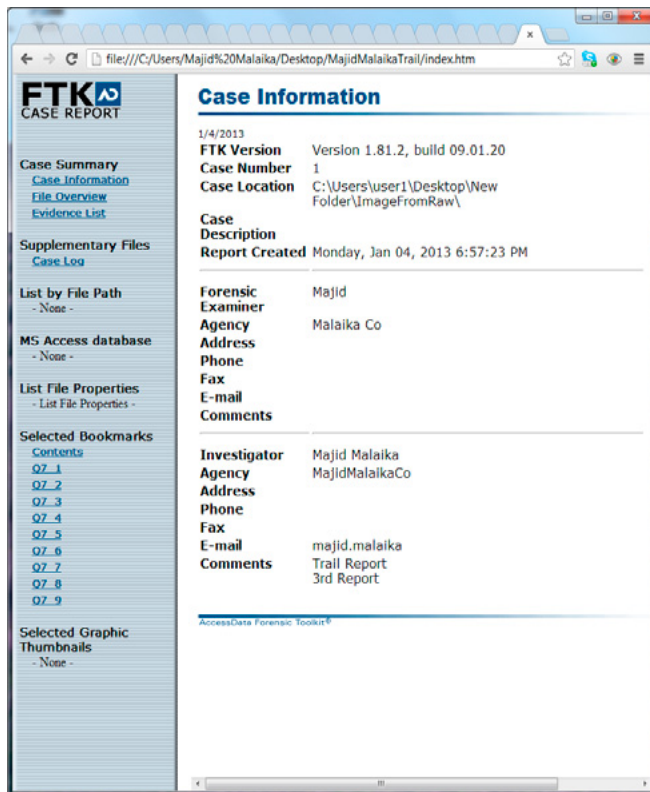


Figure 19. FTK Generated Report (FTK)

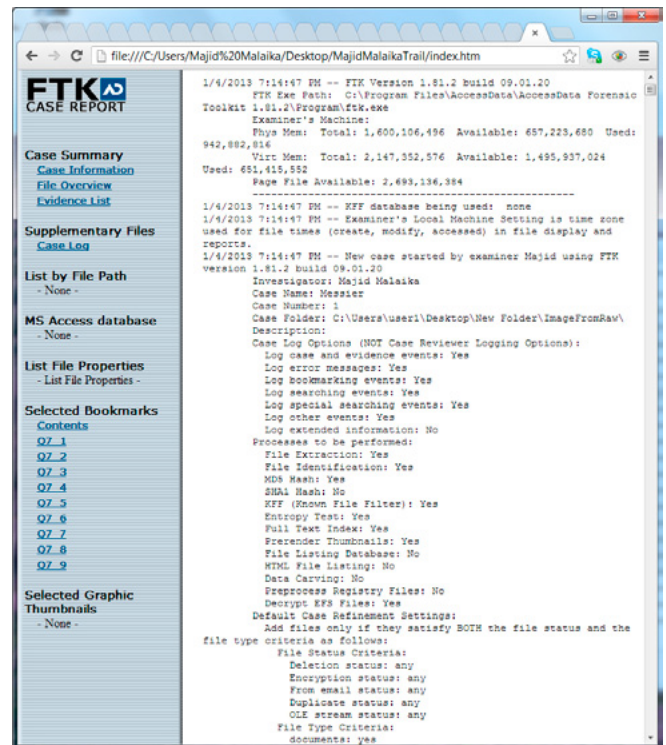


Figure 21. FTK Generated Report – Case Log (FTK)

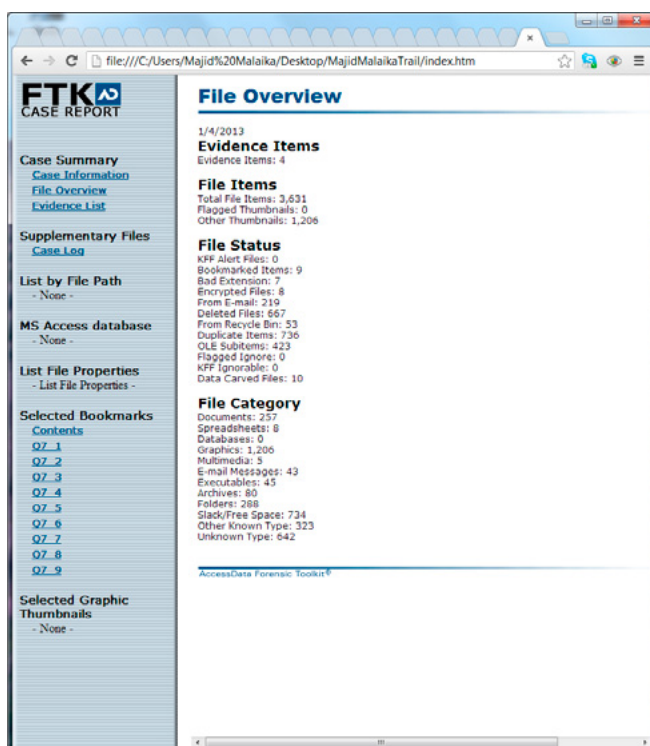


Figure 20. FTK Generated Report – File Overview (FTK)

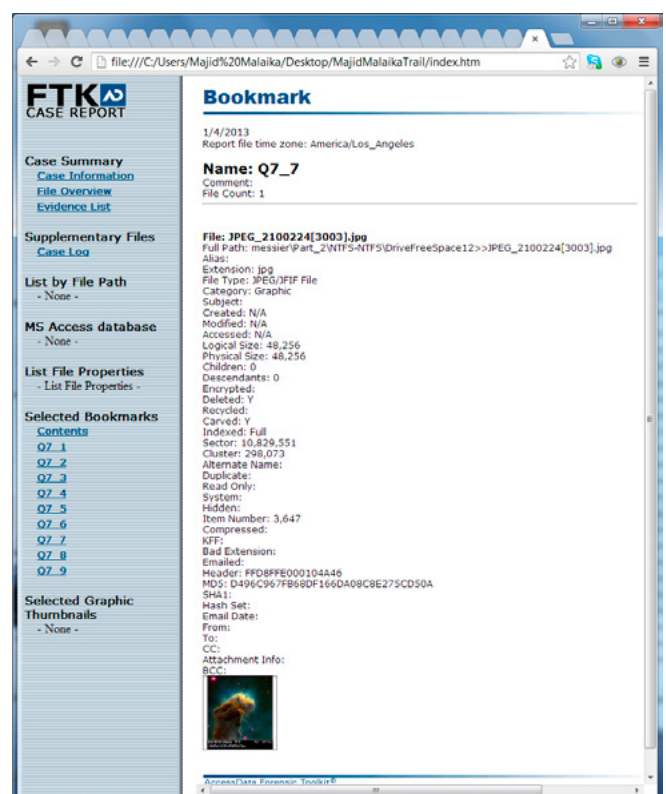


Figure 22. FTK Generated Report – Bookmark (FTK)

## References

- <http://www.accessdata.com/support/product-downloads>
- <http://thestarman.pcmindustry.com/asm/5220/index.html>
- <http://computer-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/>

erates an overview of all files discovered and categorize them based on type. In addition, it provides a summary status of all files as shown in Figure 20.

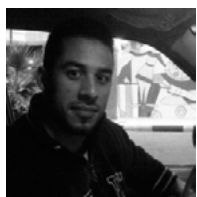
FTK also provides a case log with time and date stamps that goes in great detail on what tools and features were used and each step performed by the examiner (Figure 21).

Finally, FTK generates a list of all bookmarks added during the analysis and gives full details about each bookmark in a separate page as shown in Figure 22.

## CONCLUSION

In this article, we have described the various phases of digital forensics going through acquisition, imaging, analysis, and reporting. We accompanied our discussions with descriptions on how to carry out the various processes using FTK and FTK Imager, with step-by-step tutorial on using the tools and an illustration of a hypothetical case study. Hopefully, these discussions help explain the overall digital forensics process at the same time provide a beneficial hands-on experience.

### Author bio



*Omar Al Ibrahim received his Ph.D. in Computer Science from Southern Methodist University, Dallas, TX, USA in 2012 and his Masters degree in Computer Science from Rice University, Houston, TX, USA in 2007. During his Ph.D. Omar conducted research in embedded security where he*

*developed scalable approaches to secure low-cost RFID and sensors. Recently, Omar has joined Virtual Security Research (VSR) in Boston, MA, USA as a security consultant where he conducts penetration testing and reverse engineering.*  
[oalibrahim@vsecurity.com](mailto:oalibrahim@vsecurity.com)

### Author bio



*Majid Malaika completed his Doctor of Engineering Degree in Software Engineering from Southern Methodist University in 2011. Majid's research focus was Automating Application Security through the usage of N-Version Programming Methodology. He is currently a Security Architecture*

*Consultant at Cigital working with various development groups within financial firms in New York City to provide architecture risk analysis, risk management and security proficiency.*  
[Majid.Malaika@gmail.com](mailto:Majid.Malaika@gmail.com)



## Virtual Security Research

<http://www.vsecurity.com/>

## Services

- Application Architecture Security & Design Review
- Application Security Code Review
- Application Penetration Assessment
- Network Vulnerability & Penetration Assessments
- Digital Forensics & Incident Response
- Information Risk Management & Corporate Risk Advisors
- Application Security Quality Assurance
- Training Services

## Contact us

VSR is always looking to expand its team of experienced security consultants so that we may better serve our clients and expand our thought leadership. If you wish to apply, please send your resume (ASCII, RTF, PDF, or HTML) to: [careers@vsecurity.com](mailto:careers@vsecurity.com)

For all other inquiries, you can reach us at: [inquiry@vsecurity.com](mailto:inquiry@vsecurity.com)

Phone: (617) 993-8919 Fax: (617) 933-8920

Location: 40 Warren St. Suite 300 Boston, MA 02129, USA



# DIGITAL FORENSICS 101: CASE STUDY USING FTK IMAGER

by Dauda Sule

In the information age, virtually everything we do is done through or along with electronic devices and platforms (like PCs, mobile phones, tablets, the Internet and so on). This has greatly affected how we carry on business and live our lives, as a result, getting information and trying to know what had transpired in an event involves use of these digital devices and platforms.

## What you will learn:

- Definition of digital forensics
- Basic understanding of what digital forensics is
- Some basic practical applications of digital forensics
- How files are stored on clusters
- The basic processes for a digital forensics investigation
- Recovery of deleted files using FTK imager

## What you should know:

- Types of digital devices and platforms
- The basics of operating a Windows computer system
- Bits and bytes

When forensics is mentioned, what tends to come to mind are TV programs like the different CIS series. Historically, forensic science has been used in investigation and solving of criminal cases. Forensics is where law meets science: science is used for solving legal cases, usually by tracing trails like footprints, finger prints, DNA and so on. In the digital age, a new branch of forensics has evolved (and is still evolving) – digital forensics.

## WHAT IS DIGITAL FORENSICS?

Digital forensics can have a wide variety of definitions. Basically, it is the analysis and use of digital evidence to support or establish a case. A more refined and encompassing definition is that digital forensics is the use of computer and information systems knowledge, coupled with le-

gal knowledge to analyze in a legally acceptable manner digital evidence acquired, processed and stored in a legally acceptable manner. Emphasis is on the legal acceptability of the way the evidence is gathered and analyzed, particularly when the evidence is going to be used in a court case. The legal frameworks vary from country to country (or jurisdiction); hence what is considered legally acceptable would differ according to jurisdiction. It is also important that the digital evidence is collected in such a way as not to distort or damage the evidence being collected or give room for the possibility of that, giving whoever it is to be used against the opportunity to claim the evidence was manipulated against him/her.

A very basic example of a digital forensic examination is checking your

recycle bin to discover a porn video that had been downloaded on your desktop by your kid brother who had claimed that it was not his fault your laptop was infected with malware. In the case only you and him have access to the laptop, this can be basis for you to know he had been downloading porn on your laptop. You can also check your laptop browser's history, and when you discover a very wild risqué sounding URL that was visited at a time when the laptop was in your kid brother's possession, this further helps buttress the case against him.

In the above scenario, your kid brother could have been smart; he could have emptied the recycle bin, and cleared the browser history or could have used the browser in private browsing mode. How would you discover or prove that your kid brother downloaded porn in such a scenario? This is where more advanced digital forensics tools and techniques come in.

This article tries to give a basic introduction to digital forensics, as such is not be all encompassing. It focuses on how to retrieve data, legal requirements will not be covered in detail for example, but rather basic steps on collection digital evidence using simple digital forensics tools on a PC are shown.

## INTRODUCTION

It is quite remarkable how digital evidence can be used to solve crimes, even if not committed directly using digital devices and platforms. An example is the case of serial killer, Maury Roy Travis, who was apprehended based on a map attached to a letter he sent to a reporter. The police were able to trace the website the map was downloaded from, and got necessary warrants for the website owners to supply IP addresses of users who had checked the map within that particular period of time (yielding only one), then records of the IP address owner from the ISP which yielded Mr. Travis (Casey, E. (2004) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 2<sup>nd</sup> ed. Elsevier Academic press).

When a document is deleted on a system and the deleted from the recycle bin, it is not entirely lost. It is recorded on the system that the cluster that had been allocated for storing the document is now unallocated (vacant), meaning the cluster is available for storage of a new file (ibid). In the event no new file is stored on the cluster, the deleted document can be completely recovered. However, if a new file is stored on the cluster, the size would determine if the deleted file can be recovered. That is to say if the new file's size is smaller than the former, the former can be partially recovered from the slack space, but if the size is greater or equal to the former, recovery is not possible this way. Computers store files in sectors which hold a maximum

of 512 bytes (Sammons, J. (2012) The Basics of Digital Forensics. Elsevier, Inc.), a combination of sectors form a cluster. A file of 1000 bytes, for example, would be stored over two sectors (a cluster of 1024 bytes) as shown in Figure 1. 512 bytes are stored in one sector and the remaining 488 bytes in another. If the file is deleted and the recycle bin is emptied, the 1000 bytes remains unallocated within the 1024 byte cluster.

If a new file of say 600 bytes is saved and gets stored in the previously unallocated cluster, it will overwrite part of the previously used cluster as shown in Figure 2. 600 bytes of the original file that was deleted will be overwritten, but 400 bytes remains in the slack space, which can be recovered. Of the 600 bytes, 512 bytes are stored in the first sector, then 88 bytes overwrites part of the 488 bytes in the second sector leaving 400 bytes of the previous file in the slack space, which is recoverable.

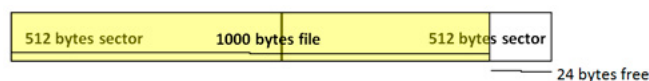
## PROCESS OF DIGITAL FORENSICS INVESTIGATION

The digital forensics investigative process basically has three steps: Acquire, Authenticate and Analyze (AAA) (University of Liverpool/Laureate Online (2011) Lecture Notes from Computer Forensics Module – Seminar 2. University of Liverpool/Laureate Online Education VLE).

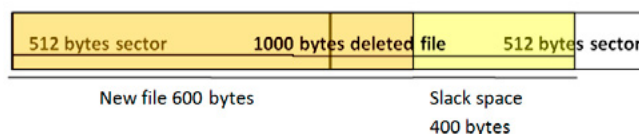
### ACQUIRE

When it has been determined that there is a digital forensics case that needs to be investigated, the first step is to acquire digital evidence. This could involve acquisition of information/data or physical evidence like PCs, laptops, hard drives, removable media, etc. care has to be taken to ensure the acquisition is authorized and carried out in line with laws of the land. Care should also be taken to ensure the evidence is not damaged or altered during this stage. Such precautions are necessary to ensure that the evidence is admissible in court; the means of acquiring the evidence is legally acceptable.

It is advisable when acquiring a computer not to boot it directly if it is off or shut it down if on. Some digital evidence can be obtained from the RAM; like date, time and other configurations which can be lost if the system is shut down or booted directly be-



**Figure 1.** Storage over two sectors (a cluster of 1024 byte)



**Figure 2.** Storage in the previously unallocated cluster

fore extracting anything from it. A system that is running can have its RAM and hard drive imaged using digital forensics tools to replicate the system's contents for analysis such that the original tampered with, which would give room for insinuation that the evidence was manipulated or damaged, affecting its authenticity. A system that is not running could be booted using an external disk (e.g. CD-ROM) and not directly from the hard disk so as not to lose or alter date-time stamps (Casey, E. (2004) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 2<sup>nd</sup> ed. Elsevier Academic press). In the case of United States v. Zacarias Moussaoui, the convicted terrorist's laptop had lost power when government officials examined its contents, creating authentication problems regarding the digital evidence (original date, time settings, boot sequence and other settings were lost); what saved the day was that an agent had initially recorded the CMOS settings earlier (ibid).

Everything that has happened to digital evidence from the point of acquisition to presentation as exhibit needs to be fully documented (Sommer, P. (2012) Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers. 3<sup>rd</sup> ed. Information Assurance Advisory Council). This documentation is known as "chain of custody" (also known as continuity of evidence in some jurisdictions). The chain of custody provides assurance that digital evidence has been properly collected and preserved such that alteration or damage does not occur. For example, hard drives should be car-

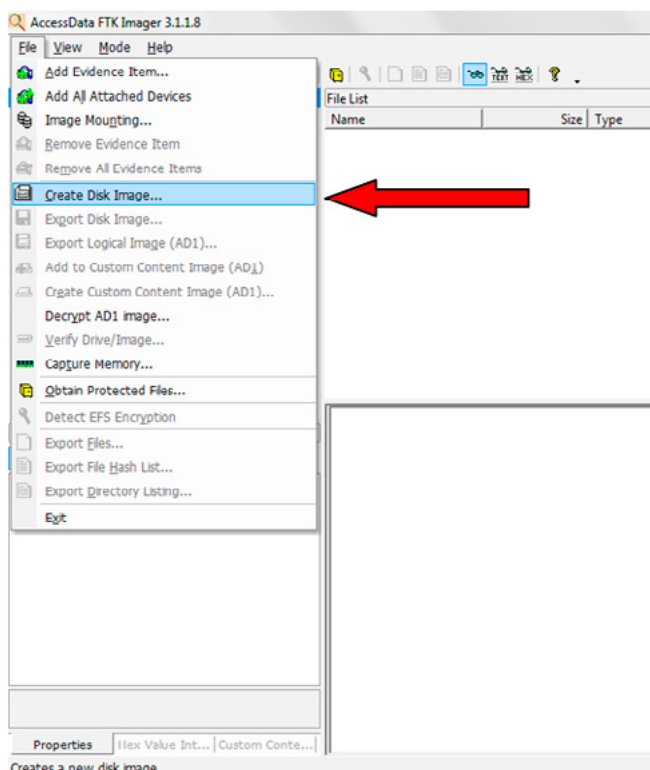
ried and stored using special anti-static bags, to prevent damage; an investigator should use his own forensic tools to carry out examinations and such tools should be legally acceptable in his jurisdiction. Such measures need to be documented to give assurance that the evidence is in good shape and was properly collected and stored. The chain of custody should show who collected the evidence; how and where it was collected; who took possession of it between point of collection and presentation as exhibit; how it was stored and protected; and who took it out of storage, for what reason (University of Liverpool/Laureate Online (2011) Lecture Notes from Computer Forensics Module – Seminar 2. University of Liverpool/Laureate Online Education VLE). Photographing the scene of evidence is also advisable. That is snapping the room containing the PC, for instance, snapping pictures of the wiring and connections, to further strengthen the chain of custody.

## AUTHENTICATE

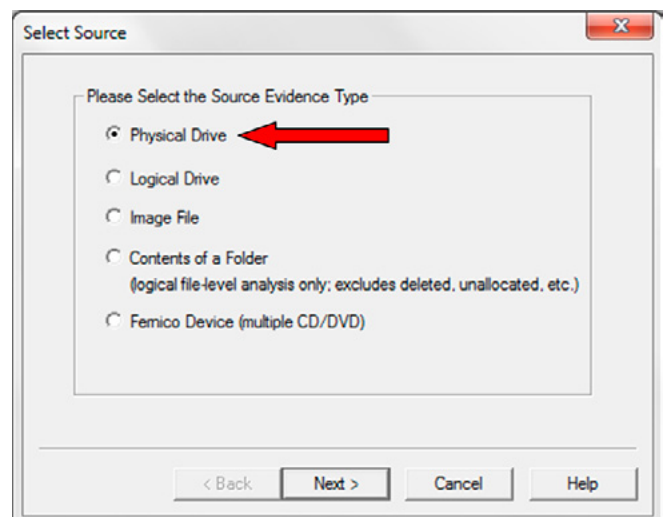
The chain of custody assists in ensuring the integrity of collected digital evidence. This has to be established to a degree of reasonability for the evidence to be deemed admissible in court; that is to authenticate the evidence. The slightest possibility of compromise to the evidence can cast reasonable doubt as to its authenticity, so there should be proof that the evidence was not manipulated or damaged in any way from point of collection to presentation in court or wherever applicable (like a board committee investigating an issue in an organization). Cryptographic hash functions and digital signatures can be used to prove integrity of digital evidence, and also time stamps (ibid).

## ANALYZE

The best way to analyze digital evidence is to work on duplicate images of hard drives and RAM, this



**Figure 3.** Click create disk image under file



**Figure 4.** Dialog box that pops-up after clicking create disk image



helps prevent damage to the original evidence. Documents and files on the duplicate can be viewed and analyzed as well as unallocated slack spaces. In our example of your kid brother, in the event he deleted the downloaded video and emptied the recycle bin, an analysis slack space on the duplicate image of the laptop hard drive would reveal details of the video (if the space had not been completely overwritten), at least partially if not completely. When analyzing digital evidence, the examiner should be familiar with techniques used to evade forensic analysis (anti-forensics) like steganography, changing file extensions (e.g. Changing a video file extension from .wmv to .doc to hide the file type), and in some cases just naming files with names that do not give away their content.

Digital evidence is usually reconstructed in the course of analysis. Reconstruction of digital evidence involves bringing together the evidence and information gathered during the course of investigation to try and recreate what may have occurred between a victim and offender in the course of the crime (Casey, E. (2004) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 2<sup>nd</sup> ed. Elsevier Academic press). Reconstruction depends on not only digital forensic tools, but also intelligence (elementary, my dear Watson). Behavioral analysis of digital evidence is also required to get an interpretation of the evi-

dence as accurate as possible. Profiles of victims of a crime are built (victimology) in order to determine why such victims were targeted; likewise offenders' profiles are also developed from available evidence in a bid to track them down.

## SAMPLE PROCESS

Still using the example of your kid brother, a forensic analysis of your disk can be done using a basic digital forensic tool. In this case, Accessdata's FTK Imager is used. Other tools that can be used include Encase, WinHex, Paraben and others. The imager is used to capture the disk image as shown in Figure 3, click on file, then click select create disk image.

Once this is done, a pop-up comes up as shown in Figure 4 requiring selection of evidence source. Select the physical drive is in this case, then click next. That will bring up the available disk drives on the system (as shown in Figure 5) where the required drive to be imaged is selected. Click finish.

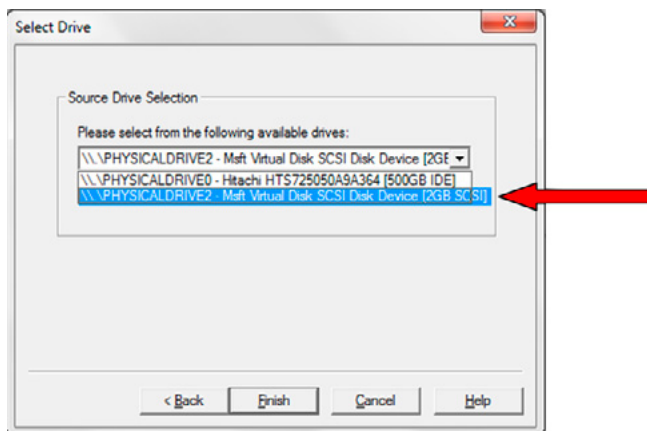


Figure 5. Selection of source drive

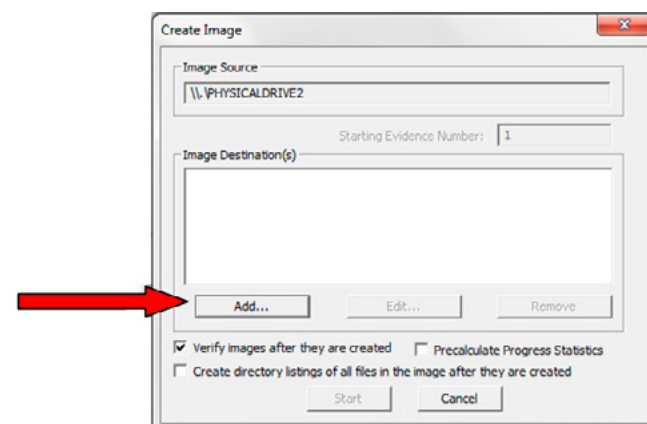


Figure 6. Dialog box for selecting image destination

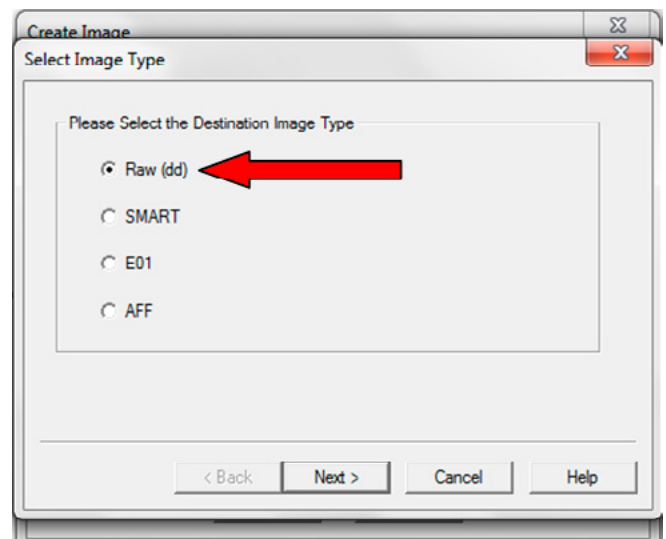


Figure 7. Pop-up to select destination image type

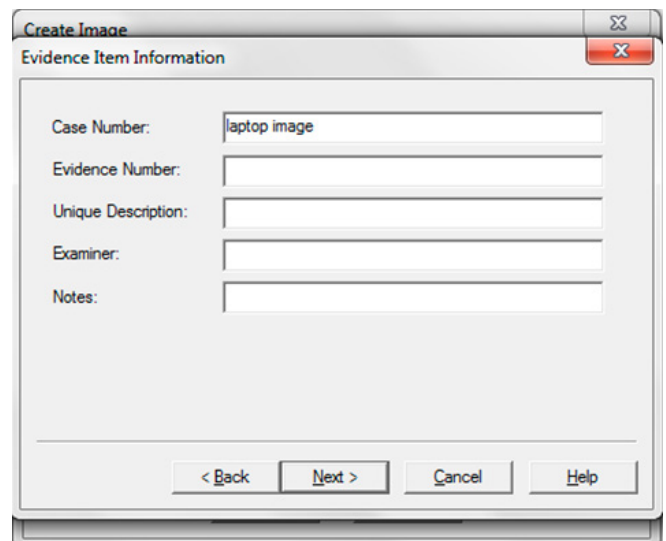
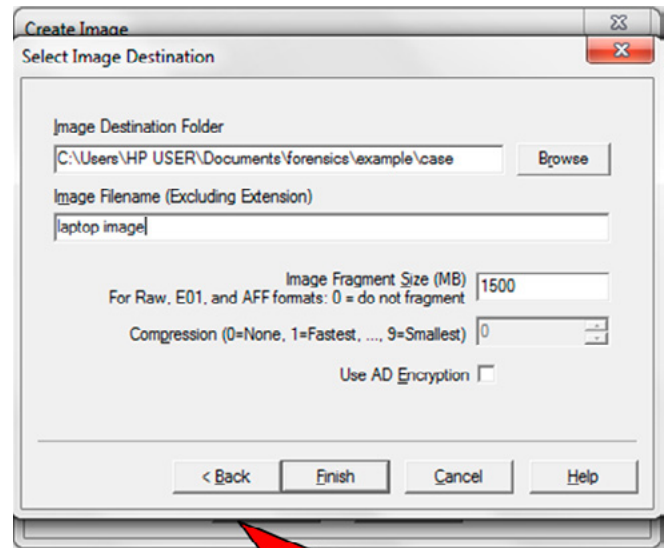


Figure 8. Dialog box for creating image details

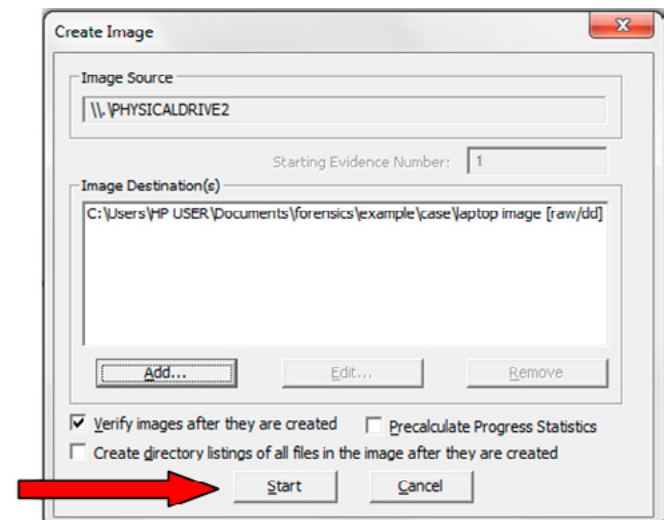
the image file to, done by clicking add (Figure 6) bringing another pop-up requiring selection of the type of data the output should be, in this case raw data was selected (as shown in Figure 7).

Next is clicked leading to snapshot in Figure 8 where evidence item information is entered: the case number, evidence number, unique description of the evidence, examiner's name and notes; then click next to browse destination folder to save the image in (Figure 9), create a name for the image file, "Laptop image" was used (Figure 10) and click finish. Clicking start (Figure 11) initiates the imaging process, which shows remaining time to complete (Figure 12). After the imaging is completed, the image is verified showing the file name, sector count and hash values (as captured in Figure 13).

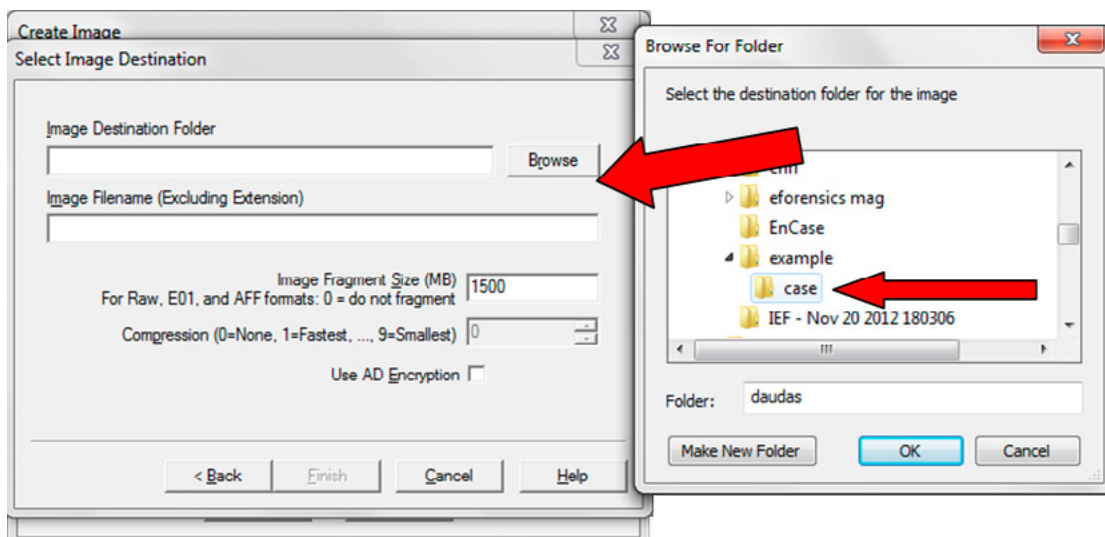
To view the image, go to file again and click select evidence item (Figure 14) which leads to the dialog box in Figure 15 where image is chosen as file type. The laptop image is loaded as in Figure 16. The FTK Imager shows hexadecimal signatures at the bottom, these signatures are used to identify file extensions and can be used to identify files disguised by change of file extension (for example, a word document having .doc extension changed to .gif can be detected by viewing the file signature in the forensic tool). The laptop image is expanded to get to the recycle bin image and contents viewed (as shown in Figure 16). In the recycle bin image, remnants of items deleted from it are visible; a look at the heaviest file, which is an MP4 video file deleted on 30<sup>th</sup> January 2013, reveals the video which can be fully viewed, revealing the type of video it was (Figure 17). A look at word document with the largest size deleted on 4<sup>th</sup> February 2013 it has a file signature of "FF D8 FF E0", which is the signature for a JPEG image (Figure 18). Some common hexadecimal signatures are available on Gary Kessler's website: [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html). In the



**Figure 10.** Name image file and click finish



**Figure 11.** After clicking finish, start image creation process



**Figure 9.** Browse to select destination folder



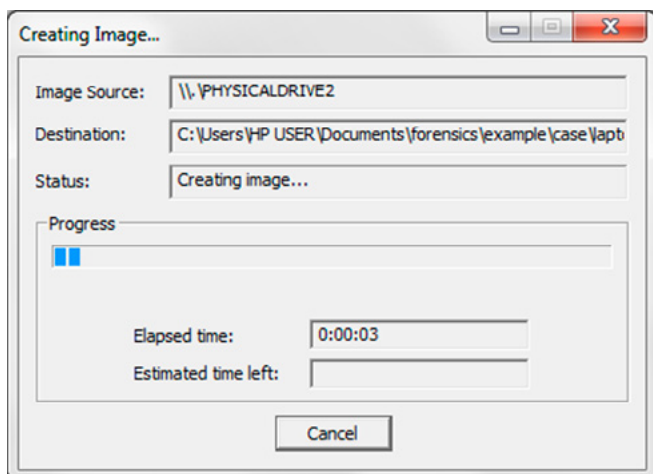


Figure 12. View of image being processed

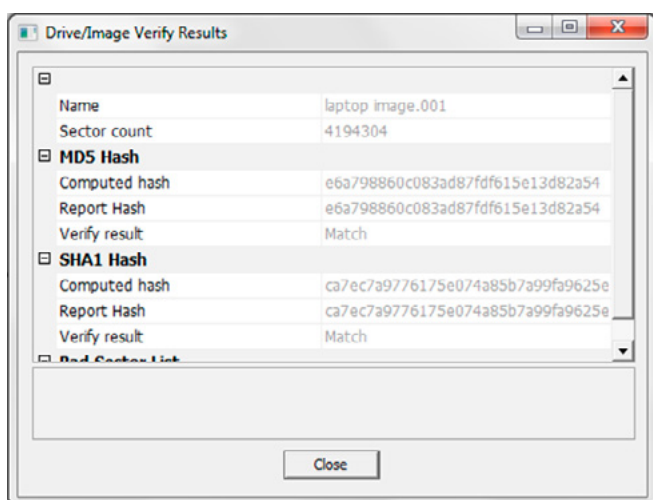


Figure 13. Image verification results

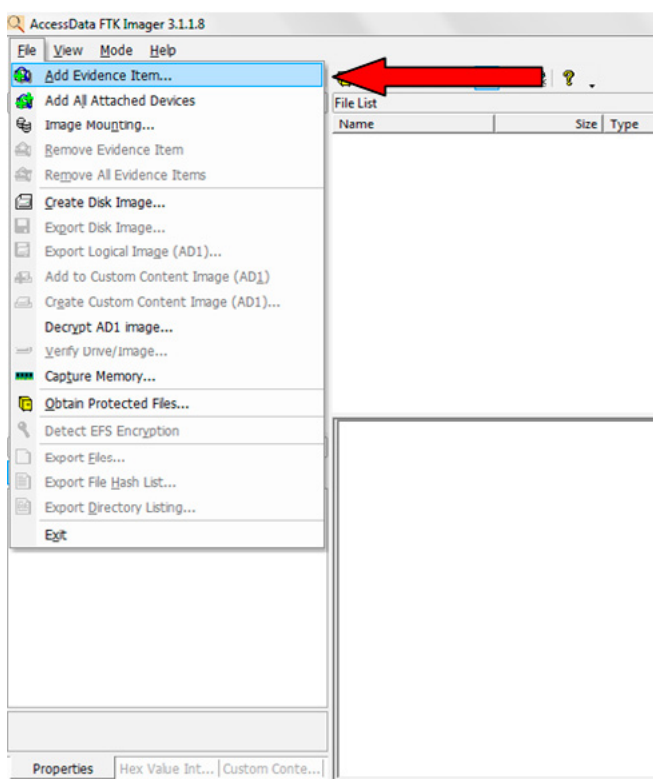


Figure 14. Click add evidence item to view image

unallocated space (Figure 19), the actual file that was deleted can be viewed.

The disk drive may be analyzed directly as well, that is without imaging it. This can be done by going to file on the FTK Imager and clicking add evidence item, as was done in Figure 14, but this time around instead of selecting image, physical drive is selected. This mounts the actual drive for analysis directly without going through image creation.

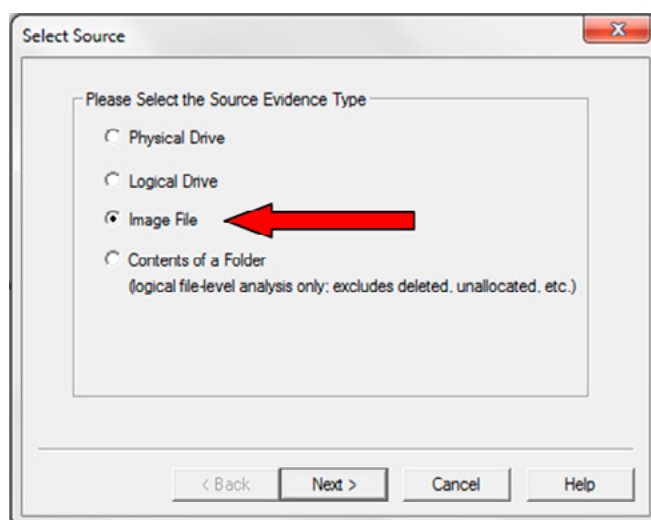


Figure 15. Select type of evidence to be viewed

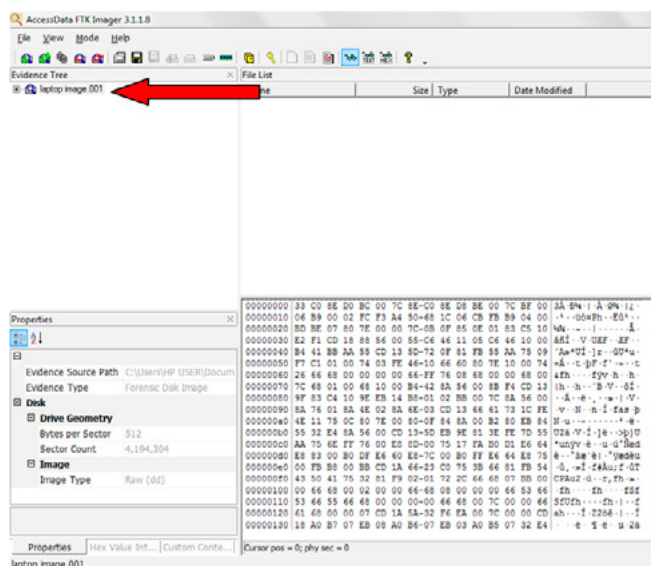


Figure 16. The laptop image with hexadecimal signatures

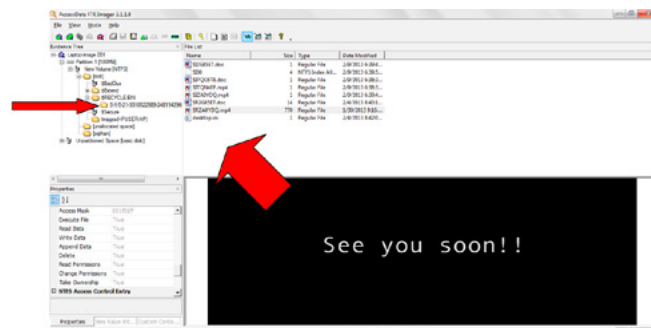
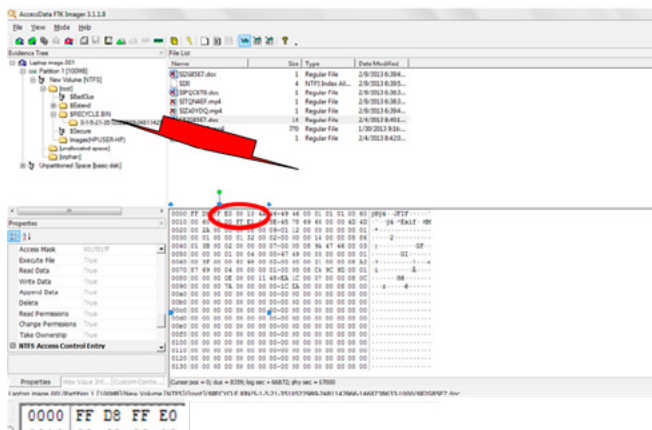
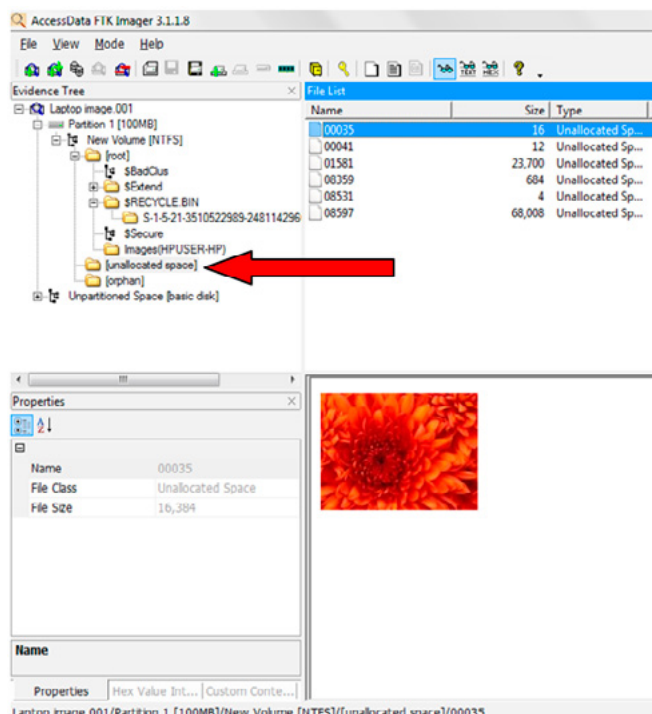


Figure 17. Image of recycle bin contents, deleted video highlighted and visible

The same steps followed for analyzing the disk image are followed to analyze the actual drive directly. This process is probably more practical when analyzing your laptop for kid brother's activity, but as previously stated, in a real life digital forensics investigation that would probably involve going to court, it is highly recommended that the disk be not analyzed directly, rather it should be imaged and the image analyzed. Another point in a real life scenario is that the disk would not be imaged using software that are installed on the laptop or installing such on the laptop, special forensic investigation tools are used for such imaging to avoid contaminating or destroying the evidence. Forensic devices are used to create duplicates of the drive which do have write protection to ensure disk is not modified in any way, then the duplicate of the disk becomes subject to analysis. Hash functions are used to verify accuracy



**Figure 18.** Hexadecimal signature of homework.doc showing the document's real file extension to be .jpg



**Figure 19.** Actual document the was renamed homework.doc visible in unallocated space

cy and integrity of the duplicate. The most common hashing algorithms are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) (Arthur, K.K. and Venter, H.S. (n.d.) An Investigation into Computer Forensic Tools [Online]. Available from: <http://www.forensicrofocus.com/computer-forensic-tools-investigation> (Accessed: February 14, 2013)).

## CONCLUSION

Digital forensics is a remarkable and interesting field which is still undergoing development. It is basically both an art and a science, and draws heavily on Law as well as technology and technological advancements. In this digital age, issues of cyber-crime, cyber-espionage, cyber-terrorism, and cyber-warfare are the buzz; digital forensic investigations come in handy for preventing and tackling such issues. Digital forensic investigations can help solve crimes as well as prevent them; they can unravel how a system was compromised or how a malware got to spread, such evidence can be used to prevent further similar attacks by strengthening digital security in addition to possible apprehension of culprits. They can also be used to determine is a business's systems or networks went down as a result of negligence or not, which could determine the extent of losses the business would incur or who to blame for it. Mistakenly deleted files can also be recovered using digital forensic tools.

By and large this article has just been a basic introduction to digital forensics and an elementary introduction to the process of data recovery using disk imaging. The most important thing in a digital forensic investigation is to preserve the chain of custody. Evidence collection and analysis needs to be documented in a bid to ensure that the evidence was handled and analyzed in a legally acceptable manner and also to prove that the evidence had not been modified or damaged.

## Author bio



*Dauda Sule, CISA is currently the Marketing Manager of Audit Associates Limited which is a consultancy firm that specializes in designing and organizing training programs pertaining to auditing, fraud detection and prevention, information security and assurance, and anti-money laundering. He is a CISA and has an M.Sc. in Computer Security from the University of*

*Liverpool. Dauda also has a first degree black belt in Tae-kwondo. He has previous experience of over five years in the Nigerian Banking industry, and also did some time in Gtech Computers (a computer and allied services company) as a systems security and assurance supervisor.*



**Make them hang on your every word...  
Put them on the edge of their seats  
when you speak...**

**Leave them wanting more...  
It can happen, but ONLY IF YOU GET THIS:**

## **THE ELECTRONIC ADVANTAGE: 101 the Basics**

**This fast-paced, 4-hour, online tutorial is for any  
Skill level and even includes 10 case examples!  
All this for just \$360**



**BONUS GIFT:**  
**The first 50 orders get our incredible  
92 Page Tech Guide, eBook, and Audiobook  
a \$100 value**

**Go here now and order:  
[www.technologicalevidence.com](http://www.technologicalevidence.com)**

# FORENSIC APPROACHES TO ENCRYPTED DISKS

by Chris Domain

Did you know that “on the fly encryption” products keep keys in memory? Or that RAM doesn’t clear the second that it loses power? Some novel techniques take advantage of these facts to maintain access to encrypted disks.

## What you will learn:

- A broad coverage of the methodologies being developed for use when encountering encrypted drives. This includes a summary of what OTFE is, memory acquisition methods, particular implementations and existing commercial tools

## What you should know:

- A basic understanding of encryption
- A basic understanding of computer architecture

It’s an old adage that security measures mean little if an attacker has physical access to your machine, however things like disk encryption pose significant forensic challenges. The good news for forensic examiners is that great progress has been made in accessing OTFE disks. In “On the fly” encryption (OTFE) data is transparently decrypted as it is read from the disk and encrypted as it is written. OTFE is growing in popularity, resulting in numerous stories of investigations being stifled by inaccessible disks.

*“In January last year Dolgov’s offices were raided, but the haul would almost certainly have been much greater had not one of the gang’s members, Estonian Aleksei Kostap, thrown a power switch which*

*blanked out the bank of computers on which the operation relied and triggered layers of encryption.”*

David Pallister, The Guardian. Friday December 1, 2006

OTFE can happen at the file level, as with Microsoft’s Encrypting File System. This article will focus primarily on full-disk and virtual volume encryption, which typically acts at the sector level, and arguably poses the greatest challenge to digital forensic practitioners. Sector level OTFE uses a cryptographic “filter” that intercepts access to the disk and uses a symmetric encryption key to access the unencrypted data.

OTFE is only meant to protect data “at rest” – once an encrypted volume is mounted it is accessible as if it was unencrypted (Figure 1).



## SHORTCOMINGS OF THE TRADITIONAL FORENSIC ACQUISITION METHODOLOGY

The traditional approach to forensic acquisition fails when encountering encryption. The investigator typically pulls the plug as soon as possible, then attaches a write blocker and creates a clone or virtual image. However if OTFE was being used on the system, the investigator has just lost the best chance of recovering the plaintext data. The decryption filter and associated key will very quickly disappear from the volatile memory.

When investigators “pull the plug” on a system they are losing all kinds of volatile information stored in RAM. This data could include running processes, network addresses, file fragments and time data. So far, this volatile data has been ignored due to fears of data corruption, as well as a lack of tools and training.

The forensic examiner is then left with less reliable methods. Occasionally keys will be stored on the hard drive in hibernation files, crash dumps and virtual memory. If they are very lucky alternative keys may be stored on backup disks for disaster recovery. There have also been cases of law enforcement using keyloggers and network forensics to steal keys, though this effort and intrusion can only be justified in the most extreme of cases.

If passphrase-based authentication is used, the investigator can attempt a slow dictionary attack on the volume. I built an open source tool (“Luks Volume Cracker”) that can brute force volumes encrypted with methods that FreeOTFE supports, at a rate of about 3 keys / second or 250 000 /day on a typical Dual Core 2 Ghz laptop. Other software is faster and supports distributed attacks, but is still infeasible for well chosen passphrases.

In the UK suspects can be compelled to give the encryption key or face jail. This has led to OTFE software products that provide “plausible deniability” – one key will decrypt a “good” volume, and another the “bad” volume. In response, techniques have been developed to detect whether or not an extra “bad” volume exists within the free space of the “good” volume.

A better solution may be to perform a “live acquisition”, where a bit-for-bit image is made of the encrypted drive while it is still mounted as an unencrypted volume. Creating an image of a running

system, however, results in a “smeared” version of the disk as data changes whilst the system operates. This same activity can damage the evidential data on the disk, and relies on a trust-worthy operating system giving correct data.

## MEMORY ACQUISITION

It is important to acquire volatile memory before any other kind of live acquisition, as live forensic tools will make significant changes to volatile memory.

Traditionally, Linux memory acquisition was as simple as the command

```
dd if=/dev/kmem of=/root/kmem
```

Kernel 2.6 introduced security restrictions around `dev/mem` and `dev/kmem`, so a tool such as the free `fmem` is now required.

There are a number of free tools available to acquire memory on Windows, such as Moonsols DumpIt. These tools require administrator access, as Windows restricts access to the Device\PhysicalMemory Object. It is possible to exploit Windows FireWire support in order to directly access memory without administrator access via exploiting how FireWire works, though some have questioned if it is a forensically sound method.

Another interesting possibility is a “cold boot attack”, which involves rebooting into another operating system to dump the memory, which will contain data from before the reboot.

Researchers at Princeton showed that liquid nitrogen could be used to keep contents in RAM for hours without power, and researchers at Cambridge have shown that lasers can be used to read RAM. However, as much fun as it may be, there is no need to get out your lasers and tanks of liquid nitrogen to perform a cold boot attack – a simple quick reboot at room temperature will do the job.

*“Contrary to popular assumption, DRAMs used in most modern computers retain their contents for seconds to minutes after power is lost, even at operating temperatures and even if removed from a motherboard.”*

<https://citp.princeton.edu/research/memory/>

MSRAMDUMP is a Linux distribution for “cold boot attacks”. The idea is you plug a USB stick containing the operating system into a computer, then restart the computer and boot off the USB stick. You can then dump the RAM to another USB device, which will likely have retained any keys in memory from before the computer was reset.

The best chance on a computer that has been in hibernation is to look for `C:\hiberfil.sys` – the memory dump that is made by Windows



**Figure 1.** Outline of an OTFE system



when going into hibernation. As it is stored in non volatile memory it may be your best bet.

## KEY IDENTIFICATION METHODS

Now that we have our acquired the memory, we need some way to search the gigabytes of data for interesting data and encryption keys. Thankfully, we have an awesome tool in the “Volatility Framework” which makes implementing methods to search the memory dump easy.

We could try simply pulling out all text with the strings utility, looking for a passphrase. While a brute force attack on the entire keyspace would be computationally infeasible, a brute force attack using all possible key-sized blocks of data and strings within a RAM image would not. However this would still be slow, and would miss fragmented or encoded keys.

To find our keys, we need to ask ourselves the question “What is different about the data we are looking for from the surrounding data?”. Answers might include

- A passphrase should look like “low entropy” human readable text, and a key like pseudo-random data
- We might expect the interesting data to be located in certain places, such as kernel space or a particular driver.

The kernel component of Windows OTFE encryption software is typically a device driver that acts as the encryption filter. Extracting this device driver is a quick way to reduce the area in which to search for the passphrase. For example, if we are looking for TrueCrypt pass phrases we can dump all device drivers with the word “true” in their name with the volatility command:

```
volatility -f windows_xp-memory-image.raw moddump
-D dump/ --regex=true
```

- Are there toolmarks? There may be certain headers and footers that we can “carve” around.

Often long term storage allocations in memory on Windows use structures called pools. These pools have headers containing a four-byte PoolTag, an identifier that specifies the driver. This isn’t always set, and pools aren’t used by default in XP, but where they are found they are very useful in narrowing down our search.

For example, the BitLocker key schedule has the PoolTag “FVEc”, which we will later use to steal BitLocker keys. Similarly, old versions of TrueCrypt used a magic value (0x7d0) to identify the location of the passphrase in memory.

- If available, are there any hints in the source code?

Source code can provide hints about how keys are stored, but the approach may need to be updated with different versions. For example, Bartosz Inglot updated the volatility plugin cryptoscan to work with later versions of True Crypt as follows:

*“As I was puzzled with the lack of magic value [in the latest version of TrueCrypt], I thought that maybe TrueCrypt’s source code could reveal anything useful. Spot on! The Password header file from the version 7.1, the latest at the time of writing this post, shows the following data structure: (Listing 1)*

*This proves to me that maybe there used to be a magic value before the password’s length in some of the previous versions, but definitely there isn’t one any more.”*

- Key Schedule Search. Most cryptosystems are implemented as a series of rounds of transformations. This is useful as:
- The key schedule provides a testable mathematical relationship between the master key and the subkeys.
- The key schedule is often pre-computed and stored with the original key for performance reasons.

### Listing 1. The password header file in C for TrueCrypt 7.1

```
typedef struct
{
    // Modifying this structure can introduce incompatibility with previous
versions
    unsigned __int32 Length;
    unsigned char Text[MAX_PASSWORD + 1];
    char Pad[3]; // keep 64-bit alignment
} Password;
```

This provides a generic approach to quickly finding keys from a variety of vendors.

#### SPECIFIC IMPLEMENTATIONS

##### TRUECRYPT

Nick Petroni and Aaron Walters observed that on Linux, TrueCrypt volumes are implemented as Device Mapper targets. Using knowledge of how the Device Mapper kernel module interfaces with and distinguishes between devices, as well as the module's exported symbols, they were able to locate TrueCrypt's Device Mapper target in memory.

According to Bartosz Inglot's interpretation of the source code, True Crypt 7.1 for Windows stores passphrases in a very particular structure:

*"Passphrases are stored in a structure containing a passphrase length (a value between 1 and 64 stored in the first of the four bytes), 65 bytes of passphrase data and then 3 bytes of padding to keep 64-bit alignment. The data must contain exactly length ASCII characters, all remaining bytes must be zeros except for the padding which has a random value."*

We can use Cryptoscan, a volatility plugin built on this information, to extract True Crypt keys. There are also commercial tools available from Elcomsoft and Passware which claim to break True Crypt volumes.

##### BITLOCKER

BitLocker is included in the Ultimate/Enterprise editions of Windows Vista, Windows 7, and with Pro/Enterprise editions of Windows 8. BitLocker employs OTFE to provide at rest encryption. It is intended to be used with a hardware Trusted Platform Module (TPM) to provide protection for data at rest. By default, BitLocker will store the key in the TPM and automatically allow access to the disk once Windows has booted.

It has a number of authentication options:

- TPM Only
- USB Key
- TPM + PIN
- TPM + USB
- TPM + PIN + USB

A 512-bit Full Volume Encryption Key (FVEK) is used to decrypt the volume, and is stored encrypted on the protected volume. The first 256 bits of the FVEK are used to decrypt data, the next 256-bits are used to generate sector keys. The FVEK is decrypted by the Volume Master Key (VMK), which is itself encrypted and stored multiple times on the protected volume. Each encrypted VMK is decrypted by a separate authentication method.

The FVEK is stored in RAM when a drive is mounted, and it is possible to perform a key schedule search to find it. Several schedules may be in the memory at any given time and it's important to note that keys are taken out of the TPM and placed into RAM where they can be found.

The following image, taken from Jesse Kornblum's excellent presentation "Practical Methods for Dealing with Full Disk Encryption", displays how the BitLocker key schedule may look in memory: Figure 2.

Jess notes the following interesting locations:

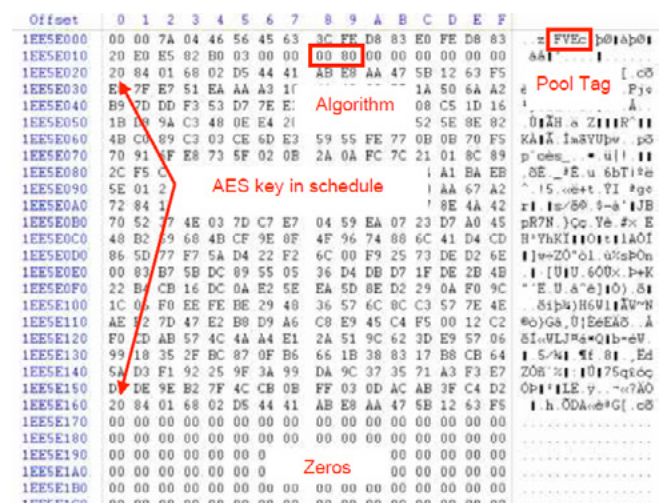
- 0x0 The FVEc pool tag
- 0x14 Algorithm ID, must be 0x8000-0x8003
- 0x1C Start of first BitLocker AES schedule – An AES key must be at start and end of schedule
- Bytes 0x1C-0x2C and 0x15C-0x16C for 128-bit – Zeros are at the end of the schedule in 128-bit mode
- 0x1EC Start of second BitLocker AES schedule

In 2008, researches from Princeton created a tool called "BitUnlocker" that could successfully steal BitLocker, FileVault, dm-crypt, and TrueCrypt keys from memory. The application was not publicly released, and the only applications I am aware of that claim to perform a fully automated retrieval of BitLocker keys are from Passware and Elcomsoft.

I, and I expect a number of others, will be releasing an open source tool to retrieve BitLocker keys as part of the DoD's DC3 Forensic Challenge once the competition ends in December 2013.

##### PGP DESKTOP

In 2007 Brian Kaplan showed how to use PGP Desktop's pool allocation tags and allocation sizes to search a small space in RAM for key like data. His tool, Disk Decrypter, then validates that the key



**Figure 2.** The BitLocker key schedule in memory, taken from the "Practical Cryptographic Key Recovery" presentation by Jesse Kornblum

is correct by seeing if it decrypts a known plaintext at a particular sector correctly. As with BitLocker, the original tool “Disk Decrypter” is not publicly available, however DC3 tools will be released later this year. The only applications I am aware of that claim to perform a fully automated retrieval of PGP keys are from Passware and Elcomsoft.

## TOOL COMPARISON

To create a quick evaluation of products currently available, I used virtual machines to set up encrypted volumes of TrueCrypt 7.1 and TrueCrypt 6.3 (the last two stable releases) on Windows Vista and Windows XP. This means there were a total of 4 separate volumes being tested against each tool.

These tests should not be considered definitive, and were only performed with demonstration copies. Please try the products yourself to see how they work for you.

## CRYPTOSCAN

Cryptoscan is a free plugin for the volatility framework, originally by Jesse Kornblum. Currently, it only claims to work for TrueCrypt. I used Bartosz Inglot's updated version which supports Vista onwards.

The commands used were:

```
volatility -f windows_xp-memory-image.raw moddump
-D dump/ --profile=WinXPSP2x86 --regex=true
```

To extract the TrueCrypt device driver, then

```
python volatility cryptoscan -f truecrypt.sys
```

To run the cryptoscan plugin to extract the keys

These commands took less than 30 seconds to complete, and all keys were recovered (4/4).



Figure 3. Passware can perform either a brute force or a key schedule search

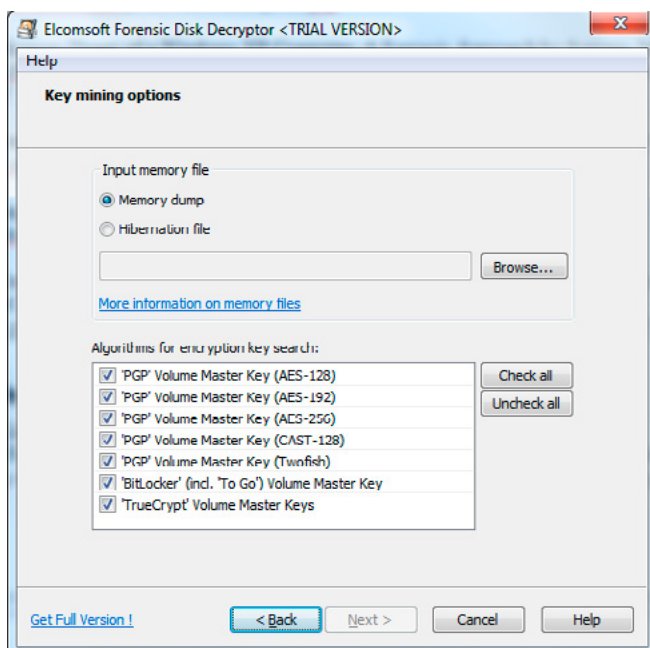


Figure 4. Selecting the keys for Elcomsoft to search for

## References & Further Reading

This article was written with frequent reference to the following articles, papers and presentations.

- RAM is Key – Extracting Disk Encryption Keys From Volatile Memory by Brian Kaplan: <http://cryptome.org/0003/RAMisKey.pdf>
- Practical Cryptographic Key Recovery by Jesse Kornblum: <http://jessekornblum.com/presentations/omfw08.pdf>
- FireWire Memory Dump of a Windows XP Computer: A Forensic Approach by Antonio Martin: <http://www.friendsglobal.com/papers/FireWire%20Memory%20Dump%20of%20Windows%20XP.pdf>
- Lest We Remember: Cold Boot Attacks on Encryption Keys by Princeton, EFF, Windriver Systems: <https://citp.princeton.edu/research/memory/>
- Implementing BitLocker Drive Encryption for Forensic Analysis by Jesse Kornblum: <http://jessekornblum.com/publications/di09.html>
- Volatools: Integrating Volatile Memory Forensics into the Digital Investigation Process by Aaron Walters and Nick Petroni: <http://www.blackhat.com/presentations/bh-dc-07/Walters/Paper/bh-dc-07-Walters-WP.pdf>



## Tools Mentioned

- Passware Kit Forensic 12.1, \$995, <http://www.lost-password.com/kit-forensic.htm>
- Elcomsoft Forensic Disk Decryptor 1.0 Build 124, \$299, <http://www.elcomsoft.com/efdd.html>
- Cryptoscan v2, Open Source, <http://passionate-about-is.blogspot.co.uk/2011/11/cryptoscan-fixed-windows-vista-support.html> or <http://www.christopherdolan.com/files/cryptoscan.zip> with Python
- MoonSold DumpIt, <http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/>

## PASSWARE PASSWORD RECOVERY KIT FORENSIC 12.1 DEMO

Passware recovers keys for BitLocker, TrueCrypt, Mac, FileVault and PGP Volumes. The interface is a very friendly point and click interface, and the tool can also recover passwords for individual file types (Figure 3). Passware managed to recover all keys (4/4), taking less than 30 seconds each time.

## ELCOMSOFT FORENSIC DISK DECRYPTOR 1.0 BUILD 124 DEMO

Elcomsoft recovers keys for BitLocker, TrueCrypt and PGP. They have done a great job in creating a tool that is easy to use, and when released it obtained a fair amount of press coverage.

Whereas Passware requires you to choose an encryption (say BitLocker or TrueCrypt) method to search for, Elcomsoft will search for all types of keys by default.

"The main and only weakness of crypto containers is human factor. Weak passwords aside, encrypted volumes must be mounted for the user to have on-the-fly access to encrypted data. No one likes typing their long, complex passwords every time they need to read or write a file," Vladimir Katalov, the ElcomSoft CEO wrote on the company's blog.

"As a result, keys used to encrypt and decrypt data that's being written or read from protected volumes are kept readily accessible in the computer's operating memory. Obviously, what's kept readily accessible can be retrieved near instantly by a third-party tool." (Figure 4)

Elcomsoft took around 6 minutes to complete, and it could only find the keys for True Crypt 7.1 with Windows Vista and XP (2/4).

Whichever tool you choose to use, it should be clear that if you are lucky enough to obtain the memory of a computer with OTFE drives mounted you have a good chance of recovery.

## Author bio



Chris Domain was the civilian winner of the 2012 DC3 Digital Forensic Challenge. You can download his open source tools at [christopherdolan.com](http://christopherdolan.com)

## Cost of CCTV



1,8m CCTV Cameras in the UK



64%  
of cases  
involve CCTV



74%  
of CCTV footage  
comes from  
private sources



£30 per hour  
**£5040**  
surveillance  
cost per week  
per camera



5  
Officers



4  
Weeks of  
viewing  
Footage



40  
hours  
work



£30  
per hour



**£24,000 cost**  
per criminal  
investigation



39m man - hours  
per year across  
all 43 UK police forces



£30 per hour  
**£1,170m**  
Cost per year

## Solution



1  
Week  
footage



5 1/2  
hours  
work



**Save 95%  
of time**

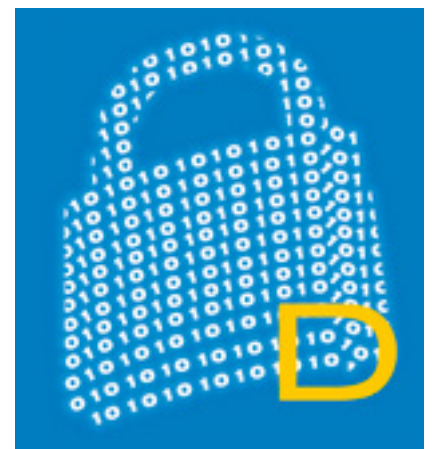
Kinesense Limited  
79 Merrion Square  
Dublin 2, Ireland

info@kinesense-vca.com  
+353 (0) 16624546  
+44 (0) 207 0961 550

# HOW TO DETECT SYSTEM INTRUSIONS

by **Almantas Kakareka**

An overlook into different techniques and tactics on detecting system intrusions. One character in the output may be the only difference between clean and compromised box.



## What you will learn:

- How and where to look for intrusion artifacts
- How typical compromises happen
- How to defend

## What you should know:

- Reader should have some experience in OS administration
- Reader should understand basic InfoSec principles

**F**irst things first, detecting system intrusion its not the same as Intrusion Detection System/ Intrusion Prevention System (IDS/IPS). We want to detect system intrusion once attackers passed all defensive technologies in the company, such as IDS/IPS mentioned above, full packet capture devices with analysts behind them, firewalls, physical security guards, and all other preventive technologies and techniques.

Many preventing technologies are using blacklisting [1] most of the time, and thus that's why they fail. Blacklisting is allowing everything by default, and forbidding something that is considered to be malicious. So for attacker it is a challenge to find yet another way to bypass the filter. It is so much harder to circumvent a whitelisting system.

## MONITORING KEY FILES IN THE SYSTEM

What are key files on the server? In Linux machine it will be `/etc/passwd`, `/etc/shadow` just to mention a few.

Lets take a look at example of `/etc/shadow` file: Listing 1.

What is wrong whit it? If you take a look at users list in this file you will notice that apache user has a hash value to it. Typically apache service never has any hash associated to it. If there is a hash for a use in this file that means this user has a password associated with it and is able to login via SSH. What happen here is hacker made a brand new account and is trying to masquerade with a valid system user/process.

One of the ways to monitor changes in the file system is to implement LoggedFS. This particular file system logs everything that happens on in-

side the files system. It is easily configurable via XML files to fit your needs [2].

Example of LoggedFS configuration file: Listing 2.

This configuration can be used to log everything except it if concerns a \*.bak file, or if the uid is 1000, or if the operation is getattr.

## FILES INTEGRITY

*File integrity monitoring* (FIM) is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and the known, good baseline. This comparison method often involves calculating a known cryptographic checksum of the file's original baseline and comparing with the calculated checksum of the current state of the file. Other file attributes can also be used to monitor integrity.

Generally, the act of performing file integrity monitoring is automated using internal controls such as an application or process. Such monitoring can be performed randomly, at a defined polling interval, or in real-time.

## SECURITY OBJECTIVES

Changes to configurations, files, and file attributes across the IT infrastructure are common, but hidden within a large volume of daily changes can be the few that impact file or configuration integrity. These changes can also reduce security posture and in some cases may be leading indicators of a breach in progress. Values monitored for unexpected changes to files or configuration items include:

- Credentials
- Privileges and Security Settings
- Content
- Core attributes and size
- Hash values
- Configuration values [3].

Many open-source and commercial software products are available that perform file integrity monitoring:

- CimTrak
- OSSEC

### Listing 1. Example of /etc/shadow file

```
# cat /etc/shadow

root:$6$0Fny79f/$LC5hcqZXNYKachPKheRh5WkeTpa/
zO3y8OX3EUHrFkrFQAdLUTKwGjLPSdZ9uhwJQ9GmChLvbhPRbPw7lDTg90:15231:0:99999:7:::
daemon:x:15204:0:99999:7:::
bin:x:15204:0:99999:7:::
sys:x:15204:0:99999:7:::
www-data:15204:0:99999:7:::
<snip>
pulse:*:15204:0:99999:7:::
rtkit:*:15204:0:99999:7:::
festival:*:15204:0:99999:7:::
postgres:!:15204:0:99999:7:::
apache:$6$LqrWlGqp$jdqlxB2GiBFgLL9kDlDkks30azWBJ1/mDU.to84mHn6nmzUzV7iHiMXK7rVm8.
pLMmaNKg9Yyu7ryw00r5VX.:15452:0:99999:7:::
```

### Listing 2. Example of LoggedFS configuration file

```
<?xml version="1.0" encoding="UTF-8"?>

<loggedFS logEnabled="true" printProcessName="true">
  <includes>
    <include extension="*" uid="*" action="*" retname="*" />
  </includes>
  <excludes>
    <exclude extension="*\.bak$" uid="*" action="*" retname="SUCCESS" />
    <exclude extension="*" uid="1000" action="*" retname="FAILURE" />
    <exclude extension="*" uid="*" action="getattr" retname="*" />
  </excludes>
</loggedFS>
```



- Samhain
- Tripwire
- Qualys
- nCircle
- Verisys
- AIDE [4].

nCircle file integrity monitor panel is in Figure 1.

## THERE IS SOMETHING VERY WRONG HERE

One bit or one symbol in the output may make the difference between war and peace, friend and foe, compromised and clean system. Lets take a look

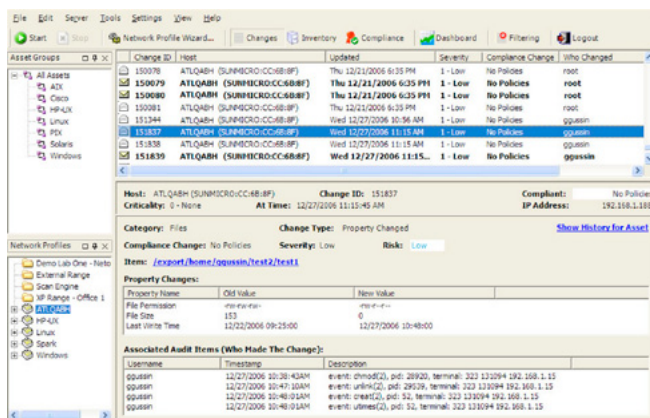


Figure 1. nCircle file integrity monitor panel

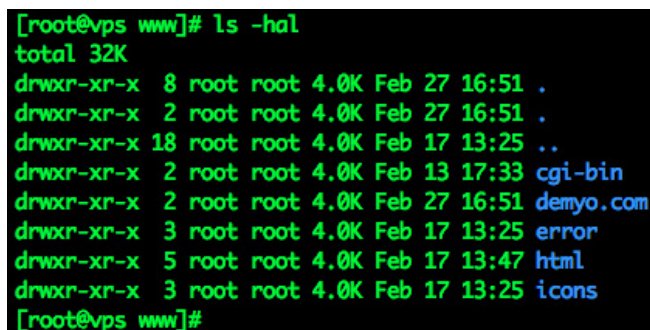


Figure 2. What is wrong in the figure?

at example below, what is very wrong in the Figure 2 screenshot? For those who don't see the wrong symbol here I will give you a hint. Is is a command to list files in directory, switch -h is for listing output in human readable format, i.e. megabytes will be megabytes and gigabytes will be gigabytes, not 1 073 741 824 bytes. Switch -l makes a list of files, once again to be easier readable by humans. Now we are coming to the main piece of information here, switch -a output will include directory entries whose names begin with a dot (.). A common hacker's technique is to hide within legit file names, or within somewhat legit names. In this case hacker has a directory on the system, which is named '.' and this is the main issue here. In usual output you should see 1 single dotted directory, in this case we see 2 single dotted directories and it should pop big red flags in your head. We change to this hidden directory by issuing command 'cd .'. Just make sure there is a space after dot.

So that's why we want to use ls -hal with switch 'a' all the time, because we want to see hidden directories and hidden files. It is pretty common to have these hidden directories in well known places, such as /root, /var/www, /home and others.

## ADDITIONAL ACCOUNTS ON THE SYSTEM

Every account on the system should be accounted for. If there are accounts that nobody knows what they belong to that may mean system is compromised. Sometimes IT admins forget to disable old accounts for people who have left company, some of these accounts may be active for months and even years. This is unnecessary risk being introduced by poor IT administrators' management. A good practice is to disable employee's account before exit interview. After compromise hackers make new account on the server and try to mimic some legit accounts that should exist. An example of additional account DBNET is in Figure 3.

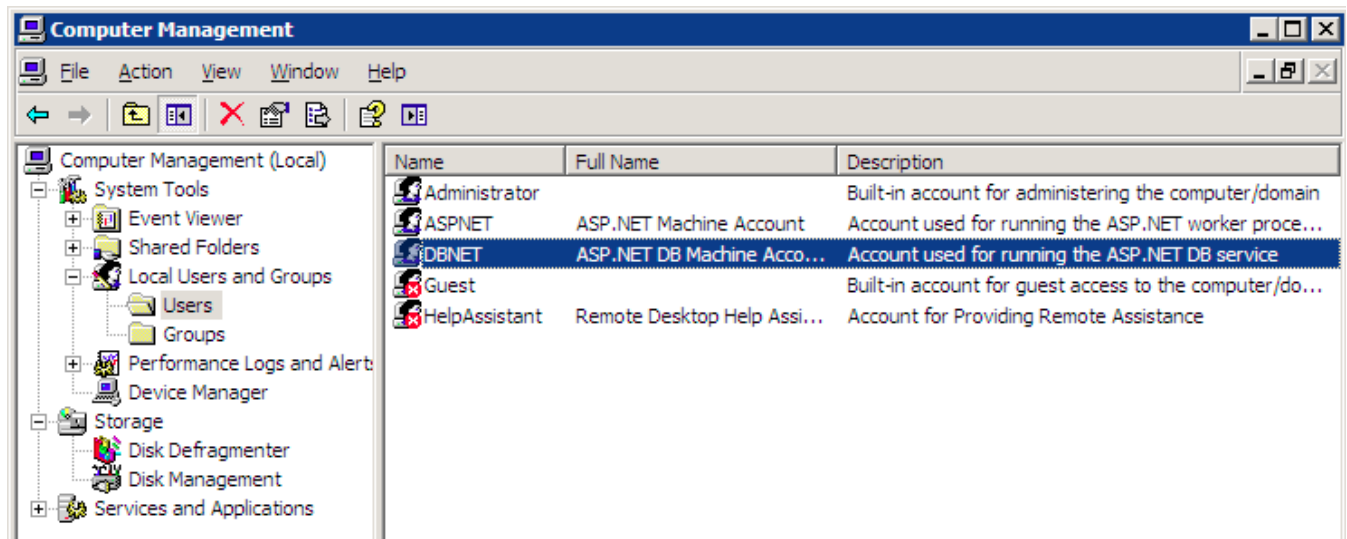


Figure 3. An example of additional account DBNET

## TIME STAMPS

A timestamp is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. The term derives from rubber stamps used in offices to stamp the current date, and sometimes time, in ink on paper documents, to record when the document was received. A common example of this type of timestamp is a postmark on a letter. However, in modern times usage of the term has expanded to refer to digital date and time information attached to digital data. For example, computer files contain timestamps that tell when the file was last modified, and digital cameras add timestamps to the pictures they take, recording the date and time the picture was taken.

A timestamp is the time at which an event is recorded by a computer, not the time of the event itself. In many cases, the difference may be inconsequential: the time at which an event is recorded by a timestamp (e.g., entered into a log file) should be close to the time of the event.

The sequential numbering of events is sometimes called time stamping.

This data is usually presented in a consistent format, allowing for easy comparison of two different records and tracking progress over time; the practice of recording timestamps in a consistent manner along with the actual data is called time stamping.

Timestamps are typically used for logging events or in a sequence of events (SOE), in which case each event in the log or SOE is marked with a time stamp. In file systems, time stamp may mean the stored date/time of creation or modification of a file [5].

Lets say you have a lot of folders and executable files in C:\Windows\System32 directory, all of them pretty much match OS installation date and time, but there is one folder which does not match OS installation time. Could there be a problem? This executable might be just some additional software

installed later on the system, or it also might be malware hiding in this directory. Windows malware just loves this folder! Folder was modified in different month than all others in Figure 4.

## HIDDEN FILES AND DIRECTORIES

A hidden file is a file that is not normally visible when examining the contents of the directory in which it resides. Likewise, a hidden directory is a directory that is normally invisible when examining the contents of the directory in which it resides.

A file is a named collection of related information that appears to the user as a single, contiguous block of data and that is retained in storage. Storage refers to computer devices or media that can retain data for relatively long periods of time (e.g., years or decades), such as hard disk drives (HDDs), CDROMs and magnetic tape; this contrasts with memory, which retains data only as long as the data is in use or the memory is connected to a power supply.

A directory (also sometimes referred to as a folder) can be conveniently viewed as a container for files and other directories. In Linux and other Unix-like operating systems, a directory is merely a special type of file that associates file names with a collection of metadata (i.e., data about the files). Likewise, a link is a special type of file that points to another file (which can be a directory). Thus, it is somewhat redundant to use phrases such as hidden files and directories; however, they are descriptive and convenient, and thus they are frequently used. More precise terms are hidden file system objects and hidden items.

Hidden items on Unix-like operating systems are easily distinguishable from regular (i.e., non-hidden) items because their names are prefixed by a period (i.e., a dot). In Unix-like operating systems, periods can appear anywhere within the name of a file, directory or link, and they can appear as many times as desired. However, usually, the only time that they have special significance is when used to indicate a hidden file or directory.

In the Microsoft Windows operating systems, whether a file system object is hidden or not is an attribute of the item, along with such things as whether the file is read-only and a system file (i.e., a file that is critical to the operation of the operating system). Changing the visibility of such items is accomplished using a multi-step procedure.

Unix-like operating systems provide a larger set of attributes for file system objects than do the Microsoft Windows operating systems, including a system of permissions, which control which user(s) have access to each such object for reading, writing and executing. However, whether objects are hidden or not is not among the attributes. Rather, it is merely a superficial property that is easily changed by adding or removing a period from the beginning of the object name.

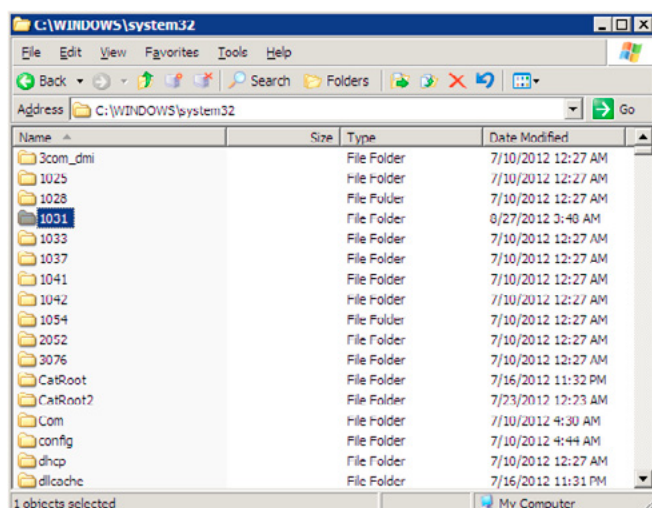


Figure 4. Modified folder

Many operating systems and application programs routinely hide objects in order to reduce the chances of users accidentally damaging or deleting critical system and configuration files. Hiding objects can also be useful for reducing visual clutter in directories, and thereby making it easier for users to locate desired files and subdirectories.

Another reason to hide file system objects is to make them invisible to casual snoopers. Although it is a very simple matter to make hidden files and directories visible, the great majority of computer users are not even aware that such files and directories exist (nor need they be) [6].

## ODAY ATTACKS

About 90 percent of all successful compromises are made via known flaws, so 0day attacks are not that common. A zero-day attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability. 0day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability.

## ATTACK VECTORS

Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors. Web browsers are a particular target because of their widespread distribution and usage. Attackers can also send e-mail attachments, which exploit vulnerabilities in the application opening the attachment. Exploits that take advantage of common file types are listed in databases like US-CERT. Malware can be engineered to take advantage of these file type exploits to compromise attacked systems or steal confidential data such as banking passwords and personal identity information.

## VULNERABILITY WINDOW

Zero-day attacks occur during the vulnerability window that exists in the time between when vulnerability is first exploited and when software developers start to develop and publish a counter to that threat. For viruses, Trojans and other zero-day attacks, the vulnerability window typically follows this time line:

- The developer creates software containing an unknown vulnerability
- The attacker finds the vulnerability before the developer does
- The attacker writes and distributes an exploit while the vulnerability is not known to the developer
- The developer becomes aware of the vulnerability and starts developing a fix.

Measuring the length of the vulnerability window can be difficult, as attackers do not announce when the vulnerability was first discovered. Developers may not want to distribute data for commercial or security reasons. Developers also may not know if the vulnerability is being exploited when they fix it, and so may not record the vulnerability as a zero-day attack. However, it can be easily shown that this window can be several years long. For example in 2008 Microsoft confirmed vulnerability in Internet Explorer, which affected some versions that were released in 2001. The date the vulnerability was first found by an attacker is not known; however, the vulnerability window in this case could have been up to 7 years.

## DISCOVERY

A special type of vulnerability management process focuses on finding and eliminating zero-day weaknesses. This unknown vulnerability management lifecycle is a security and quality assurance process that aims to ensure the security and robustness of both in-house and third party software products by finding and fixing unknown (zero-day) vulnerabilities. The unknown vulnerability management process consists of four phases: analyze, test, report and mitigate.

- Analyze: this phase focuses on attack surface analysis
- Test: this phase focuses on fuzz testing the identified attack vectors
- Report: this phase focuses on reproduction of the found issues to developers
- Mitigate: this phase looks at protective measures explained below

## PROTECTION

Zero-day protection is the ability to provide protection against zero-day exploits. Zero-day attacks can also remain undetected after they are launched.

Many techniques exist to limit the effectiveness of zero-day memory corruption vulnerabilities, such as buffer overflows. These protection mechanisms exist in contemporary operating systems such as Windows 7, Microsoft Windows Vista, Apple’s Mac OS X, recent Oracle Solaris, Linux and possibly other Unix and Unix-like environments; Microsoft Windows XP Service Pack 2 includes limited protection against generic memory corruption vulnerabilities. Desktop and server protection software also exists to mitigate zero day buffer overflow vulnerabilities.

“Multiple layers” provides service-agnostic protection and is the first line of defense should an exploit in any one layer be discovered. An example of this for a particular service is implementing access control lists in the service itself, restricting network access to it via local server firewalling (i.e., IP tables), and then protecting the entire network with



a hardware firewall. All three layers provide redundant protection in case a compromise in any one of them occurs.

The use of port knocking or single packet authorization daemons may provide effective protection against zero-day exploits in network services. However these techniques are not suitable for environments with a large number of users.

Whitelisting effectively protects against zero day threats. Whitelisting will only allow known good applications to access a system and so any new or unknown exploits are not allowed access. Although whitelisting is effective against zero-day attacks, an application “known” to be good can in fact have vulnerabilities that were missed in testing. To bolster its protection capability, it is often combined with other methods of protection such as host-based intrusion-prevention system or a blacklist of virus definitions, and it can sometimes be quite restrictive to the user.

Keeping the computer’s software up-to-date is very important as well and it does help.

Users need to be careful when clicking on links or opening email attachments with images or PDF files from unknown users. This is how many cyber criminals deceive users, by pretending they are something they are not and gaining the user’s trust.

Utilize sites with Secure Socket Layer (SSL), which secures the information being passed between the user and the visited site.

## ETHICS

Differing views surround the collection and use of zero-day vulnerability information. Many computer security vendors perform research on zero-day vulnerabilities in order to better understand the nature of vulnerabilities and their exploitation by individuals, computer worms and viruses. Alternatively, some vendors purchase vulnerabilities to augment their research capacity. While selling and buying these vulnerabilities is not technically illegal in most parts of the world, there is much controversy over the method of disclosure. A recent German decision to include Article 6 of the Convention on Cyber-crime and the EU Framework Decision on Attacks

```
root@bt:~/. # ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 2844 1604 ?        Ss   Apr15  0:01 /sbin/init
root         2  0.0  0.0      0   0 ?         S    Apr15  0:00 [kthreadd]
<snip>
root    10962  0.0  0.0 2740 476 ?        S<   09:33  0:00 udevd --daemon
root    11550  0.0  0.0      0   0 ?         S    11:13  0:00 [kworker/0:2]
root    11567  0.0  0.0      0   0 ?        S<   11:15  0:00 [hd0]
root    11619  0.0  0.0      0   0 ?         S    11:18  0:00 [kworker/0:1]
root    11654  0.0  0.0      0   0 ?         S    11:23  0:00 [kworker/0:0]
root    11664  5.3  6.1 36092 31360 pts/1    S    11:24  0:00 ./httpd
root    11665  0.0  0.2 2764 1052 pts/1    R+   11:24  0:00 ps aux
root    12015  0.0  1.7 34800 8736 ?        S    Apr16  0:00 /usr/lib/notification-daemon/notification-daemon
```

Figure 5. Monitoring running processes in the system

against Information Systems may make selling or even manufacturing vulnerabilities illegal.

Most formal efforts follow some form of disclosure guidelines or the more recent OIS Guidelines for Security Vulnerability Reporting and Response. In general these rules forbid the public disclosure of vulnerabilities without notification to the developer and adequate time to produce a patch [7].

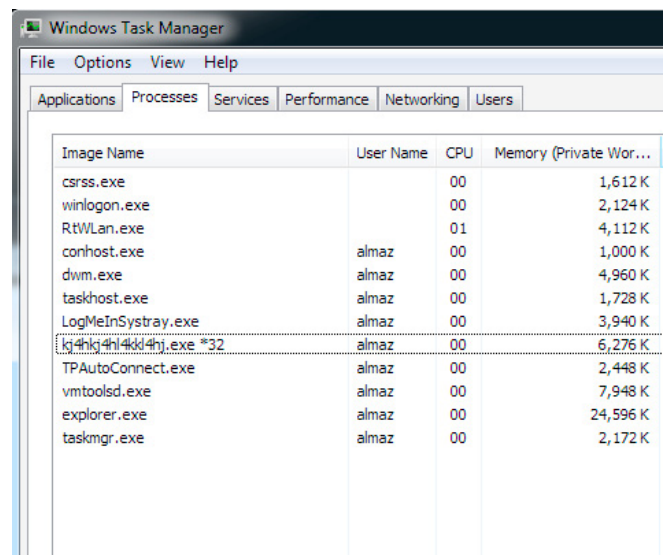
## GOOD KNOWN STATE

When attackers compromise a system, what is the very first thing they do? They install different backdoors, and as many as possible. So, if some backdoor was found on the system and it was deleted, it does not mean the system is clean. It is much safer to restore the system to a good known state; typically it is done via OS re-installation. Big companies typically have a gold image for their systems. They use gold image to quickly wipe any infected machine and reinstall OS with all its updates, and software at once. On Linux systems the software called System Imager is capable of doing many Linux installations at once.

System Imager is software that makes the installation of Linux to masses of similar machines relatively easy. It makes software distribution, configuration, and operating system updates easy, and can also be used for content distribution [8].

## MONITORING RUNNING PROCESSES IN THE SYSTEM

What is wrong on the running process list in the following Linux system in Figure 5? Process ./httpd should catch a security professional eye. Dot slash at the beginning indicates it was launched locally from the directory. Processes on the servers typically are not launched locally from their directories. Attacker has launched a process and is trying to hide by renaming his software to legit looking software typically found on the server.



| Image Name          | User Name | CPU | Memory (Private Wor... |
|---------------------|-----------|-----|------------------------|
| csrss.exe           |           | 00  | 1,612 K                |
| winlogon.exe        |           | 00  | 2,124 K                |
| RtWlan.exe          |           | 01  | 4,112 K                |
| conhost.exe         | almaz     | 00  | 1,000 K                |
| dwm.exe             | almaz     | 00  | 4,960 K                |
| taskhost.exe        | almaz     | 00  | 1,728 K                |
| LogMeInSystray.exe  | almaz     | 00  | 3,940 K                |
| lg4hg4h4k4h.exe *32 | almaz     | 00  | 6,276 K                |
| TPAutoConnect.exe   | almaz     | 00  | 2,448 K                |
| vmtoolsd.exe        | almaz     | 00  | 7,948 K                |
| explorer.exe        | almaz     | 00  | 24,596 K               |
| taskmgr.exe         | almaz     | 00  | 2,172 K                |

Figure 6. Files with weird names

## FILES WITH WEIRD NAMES

Malware frequently make files with weird looking file names, and example in Windows system is in Figure 6. We see some file `kj4hkj4hl4kkl4hj.exe` is running in the memory. This should be a first indicator something funky is going on in the system. Windows updates create random named temporary folders and should not be confused with malware.

## ROOTKITS

A rootkit is a stealthy type of malicious software designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of “root” (the traditional name of the privileged account on Unix operating systems) and the word “kit” (which refers to the software components that implement the tool). The term “rootkit” has negative connotations through its association with malware.

Rootkit installation can be automated, or an attacker can install it once they’ve obtained root or Administrator access. Obtaining this access is either a result of direct attack on a system (i.e. exploiting a known vulnerability, password (either by cracking, privilege escalation, or social engineering)). Once installed it becomes possible to hide the intrusion as well as to maintain privileged access. Like any software they can have a good purpose or a malicious purpose. The key is the root/administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment. [9]

## KERNEL LEVEL ROOTKITS

Kernel-mode rootkits run with the highest operating system privileges (Ring 0) by adding code or replacing portions of the core operating system, including both the kernel and associated device drivers. Most operating systems support kernel-mode device drivers, which execute with the same privileges as the operating system itself. As such, many kernel-mode rootkits are developed as device drivers or loadable modules, such as loadable kernel modules in Linux or device drivers in Micro-

soft Windows. This class of rootkit has unrestricted security access, but is more difficult to write. The complexity makes bugs common, and any bugs in code operating at the kernel level may seriously impact system stability, leading to discovery of the rootkit. One of the first widely known kernel rootkits was developed for Windows NT 4.0 and released in Phrack magazine in 1999 [10].

Kernel rootkits can be especially difficult to detect and remove because they operate at the same security level as the operating system itself, and are thus able to intercept or subvert the most trusted operating system operations. Any software, such as antivirus software, running on the compromised system is equally vulnerable. In this situation, no part of the system can be trusted.

A rootkit can modify data structures in the Windows kernel using a method known as direct kernel object modification (DKOM). This method can hook kernel functions in the System Service Descriptor Table (SSDT), or modify the gates between user mode and kernel mode, in order to cloak itself. Similarly for the Linux operating system, a rootkit can modify the system call table to subvert kernel functionality. It’s not uncommon for a rootkit to create a hidden, encrypted file system in which it can hide other malware or original copies of files it has infected.

Operating systems are evolving to counter the threat of kernel-mode rootkits. For example, 64-bit editions of Microsoft Windows now implement mandatory signing of all kernel-level drivers in order to make it more difficult for untrusted code to execute with the highest privileges in a system.

## USERLAND ROOTKITS

User-mode rootkits run in ring 3, along with other applications as user, rather than low-level system processes. They have a number of possible installation vectors to intercept and modify the standard behavior of application programming interfaces (APIs). Some inject a dynamically linked library (such as a .dll file on Windows, or a .dylib file on Mac OS X) into other processes, and are thereby able to execute inside any target process to spoof it; others with sufficient privileges simply overwrite the memory of a target application. Injection mechanisms include:

- Use of vendor-supplied application extensions. For example, Windows Explorer has public interfaces that allow third parties to extend its functionality
- Interception of messages
- Debuggers
- Exploitation of security vulnerabilities
- Function hooking or patching of commonly used APIs, for example, to mask a running process or file that resides on a file system.

## ROOTKIT DETECTION

There are a lot of software for rootkit searches meant to be run on live system. One of many examples would be software called “rootkit hunter” in Figure 7 [11].

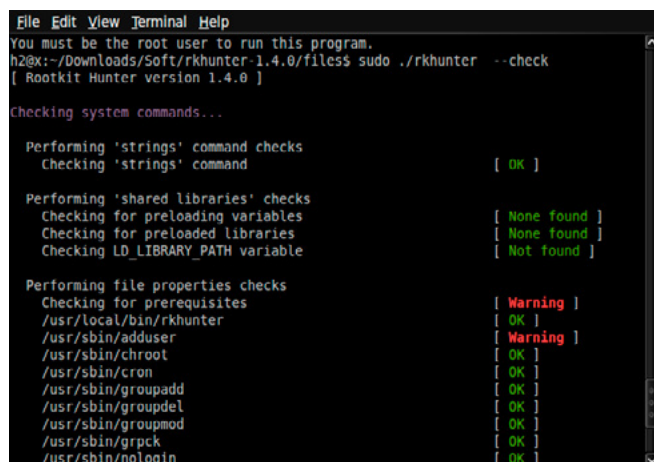
## LOW HANGING FRUIT

Do you have to run faster than bear? Not necessarily, you just have to be running faster than your friend, so he will be eaten and not you. Do your systems have to be as secure as Pentagon computers with myriad of controls? Not necessarily, your system have to be more secure than your neighbor’s and hopefully you will avoid trouble. Some other techniques to deter intrusions:

- Deterring intrusions by snow flaking (no two snowflakes are the same, so it takes more time to analyze particular system in order to gain access. Making them useless to be scanned with automatic tools). Example would be to move SSH port from default TCP/22 to TCP/31234. Some determined hacker will find it out pretty soon, but it will be an extra step for a script kiddie.
- Low hanging fruit is attacked most of the time, simply ignoring pings to the host will deter some hackers, as there are many more systems that reply to ping and it takes much less time to detect those live IPs and scan them for vulnerabilities [12].

## ANTIVIRUS SOFTWARE

The biggest fear for malware is antivirus engine on the system. Antivirus can detect attack, but it might be too late already. AV is based on signatures in the files. Hackers bypass signature detection by encrypting their executables in unique ways. Every executable is encrypted in unique way and AV engines are always losing by being late into the game of detection. If your AV engine fires – that means malware managed to slip by your IDS/IPS solution into the network and/or system.



```

File Edit View Terminal Help
You must be the root user to run this program.
h2@x:~/Downloads/Soft/rkhunter-1.4.0/files$ sudo ./rkhunter --check
[ Rootkit Hunter version 1.4.0 ]

Checking system commands...

Performing 'strings' command checks
Checking 'strings' command                [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables          [ None found ]
Checking for preloaded libraries           [ None found ]
Checking LD_LIBRARY_PATH variable          [ Not found ]

Performing file properties checks
Checking for prerequisites                  [ Warning ]
/usr/local/bin/rkhunter                    [ OK ]
/usr/sbin/adduser                           [ Warning ]
/usr/sbin/chroot                           [ OK ]
/usr/sbin/cron                             [ OK ]
/usr/sbin/groupadd                          [ OK ]
/usr/sbin/groupdel                         [ OK ]
/usr/sbin/groupmod                         [ OK ]
/usr/sbin/grpck                            [ OK ]
/usr/sbin/nologin                          [ OK ]
  
```

Figure 7. “rootkit hunter”

## HOMEGROWN INTRUSION DETECTION

In order to defeat a hacker you have to think as a hacker. Lets take a look what is a robots.txt file in web server. This file sits in the root of a web page, for example [www.mywebpage.com/robots.txt](http://www.mywebpage.com/robots.txt) and provides information to search engines what should be cached, what should be skipped, how frequently crawling has to be done, etc. Lets say you have sensitive files in directory called “reports”. This directory can be excluded from search engines crawlers and will not end up in search results. Other files and directories such as `/private/`, `/adminpanel/`, `/phpmyadmin/` should be excluded from search engine results. This technique looks great so far, but a little more experienced attacker will take a look at robots.txt file and see what you don’t want him to know!

| Incorrect robots.txt implementation   | Correct robots.txt implementation   |
|---|---|
| Disallow: /<br>adminpanel/<br>Disallow: /phpmyadmin/<br>Disallow: /backup/<br>Disallow: /uploads/ | Move all sensitive directories into one directory called for example <code>/private/</code> and disallow this directory:<br>Disallow: /private/ |

A little customized robots.txt file would look like this:

```

User-Agent: *
Disallow: /private/
Allow: /
User-Agent: hacker
Disallow: /please/go/to/an/easier/target/
  
```

It would give attacker some clue that this is probably not the easiest target, and hopefully he will move to an easier one. Needles to say it will not push away targeted attack [13]. So, if you have somebody trying to access non existing directory `/please/go/to/an/easier/target/` on the server it should give you a clue who is interested in your website.

## FULL PACKET CAPTURE DEVICES

Sometimes it is easier to detect intrusion on the wire, i.e. by monitoring ingress and egress traffic. We have to be aware of out of band communications, for example communication that come to the corporate network via GSM signals. These communications do not go through border routers of the company, and thus cannot be inspected via this technology.

Packet capture appliance is a standalone device that performs packet capture. Packet capture appliances may be deployed anywhere on a network, however, most commonly are placed at the entrances to the network (i.e. the internet connections) and in front of critical equipment, such as servers containing sensitive information.



In general, packet capture appliances capture and record all network packets in full (both header and payload), however, some appliances may be configured to capture a subset of a network's traffic based on user-definable filters. For many applications, especially network forensics and incident response, it is critical to conduct full packet capture, though filtered packet capture may be used at times for specific, limited information gathering purposes.

## DEPLOYMENT

The network data that a packet capture appliance captures depends on where and how the appliance is installed on a network. There are two options for deploying packet capture appliances on a network. One option is to connect the appliance to the SPAN port (port mirroring) on a network switch or router. A second option is to connect the appliance inline, so that network activity along a network route traverses the appliance (similar in configuration to a network tap, but the information is captured and stored by the packet capture appliance rather than passing on to another device).

When connected via a SPAN port, the packet capture appliance may receive and record all Ethernet/IP activity for all of the ports of the switch or router.

When connected inline, the packet capture appliances captures only the network traffic traveling between two points, that is, traffic that passes through the cable to which the packet capture appliance is connected. There are two general approaches to deploying packet capture appliances: centralized and decentralized.

## CENTRALIZED

With a centralized approach, one high-capacity, high-speed packet capture appliance connects to data-aggregation point. The advantage of a centralized approach is that with one appliance you gain visibility over the network's entire traffic. This approach, however, creates a single point of failure that is a very attractive target for hackers; additionally, one would have to re-engineer the network to bring traffic to appliance and this approach typically involves high costs.

## DECENTRALIZED

With a decentralized approach you place multiple appliances around the network, starting at the point(s) of entry and proceeding downstream to deeper network segments, such as workgroups. The advantages include: no network re-configuration required; ease of deployment; multiple vantage points for incident response investigations; scalability; no single point of failure – if one fails, you have the others; if combined with electronic invisibility, this approach practically eliminates the danger of unauthorized access by hackers; low cost. Cons: potential increased maintenance of multiple appliances.

In the past, packet capture appliances were sparingly deployed, oftentimes only at the point of entry into a network. Packet capture appliances can now be deployed more effectively at various points around the network. When conducting incident response, the ability to see the network data flow from various vantage points is indispensable in reducing time to resolution and narrowing down which parts of the network ultimately were affected. By placing packet capture appliances at the entry point and in front of each work group, following the path of a particular transmission deeper into the network would be simplified and much quicker. Additionally, the appliances placed in front of the workgroups would show intranet transmissions that the appliance located at the entry point would not be able to capture.

## CAPACITY

Packet capture appliances come with capacities ranging from 500 GB to 32 TB and more. Only a few organizations with extremely high network usage would have use for the upper ranges of capacities. Most organizations would be well served with capacities from 1 TB to 4 TB.

A good rule of thumb when choosing capacity is to allow 1 GB per day for heavy users down to 1 GB per month for regular users. For a typical office of 20 people with average usage, 1 TB would be sufficient for about 1 to 4 years.

## FEATURES

### FILTERED VS. FULL PACKET CAPTURE

Full packet capture appliances capture and record all Ethernet/IP activity, while filtered packet capture appliances captured only a subset of traffic, based on a set of user-definable filters, such as IP address, MAC address or protocol. Unless using the packet capture appliance for a very specific, narrow purpose covered by the filter parameters, it is generally best to use full packet capture appliances or otherwise risk missing vital data. Particularly when using a packet capture for network forensics or cyber security purposes, it is paramount to capture everything because any packet not captured on the spot is a packet that is gone forever. It is impossible to know ahead of time the specific characteristics of the packets or transmissions needed, especially in the case of an advanced persistent threat (APT). APTs and other hacking techniques rely for success on network administrators not knowing how they work and thus not having solutions in place to counteract them. Most APT attacks originate from Russian and China.

### ENCRYPTED VS. UNENCRYPTED STORAGE

Some packet capture appliances encrypt the captured data before saving it to disk, while others

do not. Considering the breadth of information that travels on a network or Internet connection and that at least a portion of it could be considered sensitive, encryption is a good idea for most situations as a measure to keep the captured data secure. Encryption is also a critical element of authentication of data for the purposes of data/network forensics.

### **SUSTAINED CAPTURE SPEED VS. PEAK CAPTURE SPEED**

The sustained captured speed is the rate at which a packet capture appliance can capture and record packets without interruption or error over a long period of time. This is different from the peak capture rate, which is the highest speed at which a packet capture appliance can capture and record packets. The peak capture speed can only be maintained for short period of time, until the appliance's buffers fill up and it starts losing packets. Many packet capture appliances share the same peak capture speed of 1 Gbps, but actual sustained speeds vary significantly from model to model.

### **PERMANENT VS. OVERWRITABLE STORAGE**

A packet capture appliance with permanent storage is ideal for network forensics and permanent record-keeping purposes because the data captured cannot be overwritten, altered or deleted. The only drawback of permanent storage is that eventually the appliance becomes full and requires replacement. Packet capture appliances with overwritable storage are easier to manage because once they reach capacity they will start overwriting the oldest captured data with the new, however, network administrators run the risk of losing important capture data when it gets overwritten. In general, packet capture appliances with overwrite capabilities are useful for simple monitoring or testing purposes, for which a permanent record is not necessary. Permanent recording is a must for network forensics information gathering.

### **DATA SECURITY**

Since packet capture appliances capture and store a large amount of data on network activity, including files, emails and other communications, they could, in themselves, become attractive targets for hacking. A packet capture appliance deployed for any length of time should incorporate security features, to protect the recorded network data from access by unauthorized parties. If deploying a packet capture appliance introduces too many additional concerns about security, the cost of securing it may outweigh the benefits. The best approach would be for the packet capture appliance to have built-in security features. These security features may include encryption, or methods to "hide" the appliance's pres-

ence on the network. For example, some packet capture appliances feature "electronic invisibility", that is, have a stealthy network profile by not requiring or using IP nor MAC addresses.

Though on the face of it connecting a packet capture appliance via a SPAN port appears to make it more secure, the packet capture appliance would ultimately still have to be connected to the network in order to allow management and data retrieval. Though not accessible via the SPAN link, the appliance would be accessible via the management link.

Despite the benefits, a packet capture appliance's remote access feature presents a security issue that could make the appliance vulnerable. Packet capture appliances that allow remote access should have a robust system in place to protect it against unauthorized access. One way to accomplish this is to incorporate a manual disable, such as a switch or toggle that allows the user to physically disable remote access. This simple solution is very effective, as it is doubtful that a hacker would have an easy time gaining physical access to the appliance in order to flip a switch.

A final consideration is physical security. All the network security features in the world are moot if someone is simply able to steal the packet capture appliance or make a copy of it and have ready access to the data stored on it. Encryption is one of the best ways to address this concern, though some packet capture appliances also feature tamperproof enclosures [14].

### **OUT OF BAND ATTACK VECTORS**

What is the weakest link in any corporation? The answer is people. People fall into social engineering attacks; people bring "forgotten" USB sticks and CDs from bathrooms/parking lots and plug them into their computers just out of curiosity. People bring their own devices from home and connect to corporate networks. BYOD or Bring Your Own Device is a big pain for IT administrators to manage. It also introduces additional risk, because employee's own devices might already be backdoored or infected and by connecting these devices to corporate network employees are introducing a new risk. Social engineering attack with lost CD – Figure 8.

Demyo power strip is a full-blown Linux based OS with many penetration testing tools preinstalled, it looks like innocent power surge/strip, but has Wi-Fi, Ethernet and Bluetooth installed inside. Once connected to the power outlet it immediately calls back home via GSM 3g modem and establishes connection. Once connected penetration testers can use it as a jump box to do further penetration testing inside the LAN of the corporation [15]. Demyo power strip is shown in Figure 9.

How to prevent employees bringing "lost CDs" and "lost USB sticks" from parking lots and plug-

ging them into their machines? A strong policy should be in place disallowing connecting non-approved hardware to workstations. It is not enough just to write a policy and consider the job to be done. Policy has to be enforced and most importantly policy has to be understood by employees. There is no way rules can be followed if they are not understood. Another way to minimize risk is to provide security awareness training to employees explaining typical social engineering attacks and how not to fall for them.

## SECURITY AWARENESS TRAINING

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical and, especially, information assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually. Topics covered in security awareness training include:

The nature of sensitive material and physical assets they may come in contact with, such as trade secrets, privacy concerns and government classified information.

Employee and contractor responsibilities in handling sensitive information, including review of employee nondisclosure agreements.

Requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction



**Figure 8.** Social engineering attack with lost CD



**Figure 9.** Demyo power strip

Proper methods for protecting sensitive information on computer systems, including password policy and use of two-factor authentication

Other computer security concerns, including malware, phishing, social engineering, etc.

Workplace security, including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.

Consequences of failure to properly protect information, including potential loss of employment, economic consequences to the firm, damage to individuals whose private records are divulged, and possible civil and criminal penalties

Being security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization. Therefore, it would be prudent to support the assets of the institution (information, physical, and personal) by trying to stop that from happening.

According to the European Network and Information Security Agency, 'Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks.'

'The focus of Security Awareness consultancy should be to achieve a long-term shift in the attitude of employees towards security, whilst promoting a cultural and behavioral change within an organization. Security policies should be viewed as key enablers for the organization, not as a series of rules restricting the efficient working of your business. '[16]

## DATA CORRELATION

Data correlation is a technique used in information security to put all pieces together and come up with some meaningful information. For example if you see in Linux system SSH connections coming in all day long, and after 200 tries to login in there is a successful login after all. What does it tell you? It should be a good starting point to suggest a brute force attack is going on with a success at the end. All technologies help to find out intrusions, however technologies do not find intrusions, people do. Appliances and sensors are typically good about finding bad events, but good events can combine into bad one as well. How is it possible you would ask? Lets outline a simple scenario where human makes determination about compromise.

Lets say there is a company with many employees which travel a lot around the globe. Company is doing a good job by implementing various control systems, various logging systems, this company also uses RFID enabled cards for its employees in order to track who is coming and leaving its offices. All data is collected and pushed to SIEM [17] engine to do correlation between events and logs. One morning 2 seemingly good events come into SIEM. First event is user john VPN connection is

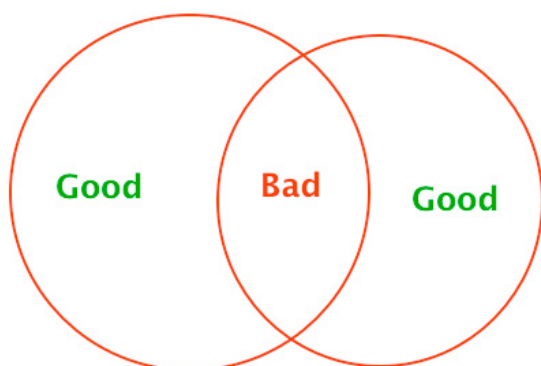


established from overseas to corporate office. Second event is user john RFID badge being scanned at the entrance to the corporate office. Well both events are pretty standard and are harmless when taken separately, but then combined together they reveal something weird. How can user john VPN in from overseas and get a physical entrance to the office at the same time? The answer is one of two: either VPN credentials are compromised, or his employee card is used by somebody else to enter the office. Figure 10 shows how 2 good things can create 1 bad thing when combined.

## SIEM

Security Information and Event Management (SIEM) solutions are a combination of the formerly disparate product categories of SIM (security information management) and SEM (security event manager). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes. The acronyms SEM, SIM and SIEM have been used interchangeably, though there are differences in meaning and product capabilities. The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as Security Event Management (SEM). The second area provides long-term storage, analysis and reporting of log data and is known as Security Information Management (SIM).

The term Security Information Event Management (SIEM), describes the product capabilities of gathering, analyzing and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database and application logs; and external threat data. A key focus is to monitor and help manage user and service privileges, directory services and other system configuration changes; as well as providing log auditing and review and incident response.



**Figure 10.** How 2 good things can create 1 bad thing when combined

## SIEM CAPABILITIES

- **Data Aggregation:** SIEM/LM (log management) solutions aggregate data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- **Correlation:** looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information.
- **Alerting:** the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues.
- **Dashboards:** SIEM/LM tools take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.
- **Compliance:** SIEM applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.
- **Retention:** SIEM/SIM solutions employ long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements.

## OTHER WEIRD STUFF ON THE SYSTEM

What are other symptoms of possible system compromise? Some examples below:

- **Log files are missing completely.** Why there are no log files?  
Script kiddies delete logs whereas hackers modify them by taking out only their IP addresses, their commands and manipulations with system.
- **Network interface is in promiscuous mode**

In computer networking, promiscuous mode is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN. The mode is also required for bridged networking for hardware virtualization.

In IEEE 802 networks such as Ethernet, token ring, and IEEE 802.11, and in FDDI, each frame includes a destination Media Access Control address (MAC address). In non-promiscuous mode, when a NIC receives a frame, it normally drops it unless the frame is addressed to that NIC's MAC address or

is a broadcast or multicast frame. In promiscuous mode, however, the card allows all frames through, thus allowing the computer to read frames intended for other machines or network devices.

Many operating systems require super user privileges to enable promiscuous mode. A non-routing node in promiscuous mode can generally only monitor traffic to and from other nodes within the same broadcast domain (for Ethernet and IEEE 802.11) or ring (for token ring or FDDI). Computers attached to the same network hub satisfy this requirement, which is why network switches are used to combat malicious use of promiscuous mode. A router may monitor all traffic that it routes.

Promiscuous mode is often used to diagnose network connectivity issues. There are programs that make use of this feature to show the user all the data being transferred over the network. Some protocols like FTP and Telnet transfer data and passwords in clear text, without encryption, and network scanners can see this data. Therefore, computer users are encouraged to stay away from insecure protocols like telnet and use more secure ones such as SSH.

## DETECTION

As promiscuous mode can be used in a malicious way to sniff on a network, one might be interested in detecting network devices that are in promiscuous mode. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this (e.g., using carefully designed firewall settings).

An example is sending a ping (ICMP echo request) with the wrong MAC address but the right IP address. If an adapter is operating in normal mode, it will drop this frame, and the IP stack never sees or responds to it. If the adapter is in promiscuous mode, the frame will be passed on, and the IP stack on the machine (to which a MAC address has no meaning) will respond as it would to any other ping. The sniffer can prevent this by configuring his firewall to block ICMP traffic [18].

- Immutable files on the system that cannot be deleted, find those with `lsattr` command  
`lsattr` is a command-line program for listing the attributes on a Linux second extended file system. It is also a command to display attributes of devices on an AIX operating system. Some malware puts +i flag on its own executable, so you cannot delete it, even if you are root.
- Mysterious open ports and services  
All open ports and running services should be accounted for. For example if there is a service running, but its not clear what it does, or why is it running – an investigation should be launched [19].

## ON THE WEB

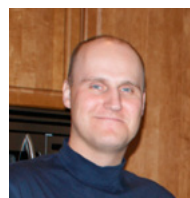
1. Whitelisting vs blacklisting – <http://bit.ly/RNxEHO>
2. LoggedFS – <http://loggedfs.sourceforge.net/>
3. File Integrity Monitoring – [https://en.wikipedia.org/wiki/File\\_integrity\\_monitoring](https://en.wikipedia.org/wiki/File_integrity_monitoring)
4. AIDE – <http://aide.sourceforge.net/>
5. Timestamps – <https://en.wikipedia.org/wiki/Timestamp>
6. Hidden files – [http://www.linfo.org/hidden\\_file.html](http://www.linfo.org/hidden_file.html)
7. Oday attacks – [https://en.wikipedia.org/wiki/Zero-day\\_attack](https://en.wikipedia.org/wiki/Zero-day_attack)
8. SystemImager – <http://sourceforge.net/projects/systemimager/>
9. Rootkit – <https://en.wikipedia.org/wiki/Rootkit>
10. Phrack – <http://phrack.org/>
11. Rootkit hunter – <http://rkhunter.sourceforge.net/>
12. What is vulnerability – <http://bit.ly/PFCWCh>
13. Targeted attack – <http://bit.ly/MTjLVv>
14. Full Packet Capture – [https://en.wikipedia.org/wiki/Packet\\_Capture\\_Appliance](https://en.wikipedia.org/wiki/Packet_Capture_Appliance)
15. Demyo power strip – <http://www.demyo.com>
16. Security Awareness – [https://en.wikipedia.org/wiki/Security\\_awareness](https://en.wikipedia.org/wiki/Security_awareness)
17. SIEM – <https://en.wikipedia.org/wiki/Siem>
18. Promiscuous mode – [https://en.wikipedia.org/wiki/Promiscuous\\_mode](https://en.wikipedia.org/wiki/Promiscuous_mode)
19. Intrusion Detection – <http://bit.ly/OCB7UU>

## SUMMARY

As we outlined above there are so many ways to detect system intrusions and so many ways to hide them. What is the proper way to analyze suspect system then? The proper sequence is:

1. Memory dump and analysis. Hackers are getting smart these days; they stay in memory as long as possible. Why? Because they know forensics will be done on the HDD itself, but if they stay in memory it requires better skill to do memory analysis. Some companies just pull the plug from the power and network and do HDD forensics analysis. This is wrong, because as soon as you pull the power plug – half of the goodies are gone...
2. Selective HDD files analysis (we make HDD image first, and work from the copy). Depending on the machine role on the network it might be an overkill to do full blown forensic analysis. In some situations partial forensic examination is enough.
3. Full HDD analysis if needed (we make HDD image first, and work from the copy).

## Author bio



*Almantas Kakareka is a founder and CTO of Demyo, Inc. and has over 15 years of IT security related experience. His expertise is vulnerability assessments, and penetration testing. Almantas has a Master of Science degree in Computer Science from Florida International University and certifications such as CISSP, GSNA, GSEC, CEH, MCDST, MCP, Net+ and Sec+. Website: [www.demyo.com](http://www.demyo.com).*

**Technology is a double sided sword.  
Internet makes you naked online!  
Get Secured & Get Certified!**

Welcome to the world of Certified Ethical Cracker  
with Hands-on practical sessions.



**CERTIFIED  
ETHICAL  
CRACKER**

An Advance **Information Security** Course

For more details, visit:

<http://www.infysec.com/training/courses/certified-ethical-cracker>

**infySEC UK :**

145-157, St.John Street,  
London, EC1V 4PW  
England, UK

Phone: +44-7405190001

**infySEC India :**

#37/45, P.H Road,  
Arumbakkam,  
Chennai- 600106  
TamilNadu, INDIA

Phone: +91-44-42611142,43



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

[enquiry@infysec.com](mailto:enquiry@infysec.com)



# INTERVIEW OF CYBER LAWYER

FERNANDO M. PINGUELO

by Joanna Kretowicz

Class actions are one of the hot button cyber issues of the day – or at least the one that seems to grab the headlines. For example, around the time of the Facebook IPO, a class action lawsuit involving Facebook’s improper use of users’ personal data for advertisement purposes dominated the headlines, and was a contributing factor to Facebook’s sluggish stock price.

## Why did you create and develop your law firm’s cyber security and data protection law practice group?

While in private practice, I’ve had a passion for technology’s impact on the law for as long as I can remember. And, finding creative ways to apply antiquated laws to present day tech realities has been a skill I’ve developed as a litigator since about 2006.

Because technology has little regard for jurisdictional and substantive boundaries, I launched Norris McLaughlin & Marcus’ Cyber Security & Data Protection group as a way to streamline and formalize what I had been doing earlier – drawing upon an interdisciplinary team of professionals across diverse disciplines and navigating the client through the myriad of federal, local, and international laws that cover – and in many cases contradict – U.S. laws that purport to govern the predicaments in which a client may find itself.

## Who’s on your team?

Four lawyers comprise the core Cyber Security & Data Protection group in our New Jersey and New

York offices, and we draw upon the subject matter expertise of our nearly 140 lawyers who practice in more than three dozen legal disciplines. Our capabilities are global, and we are often called upon to lead efforts in jurisdictions throughout the U.S. and the world— we do that by using our network of local counsel who practice in more than 70 countries.

## Any other members who play a critical role on your team?

Absolutely – my team draws upon paralegals as well as practice support and IT professionals from each of our three offices in New Jersey, New York, and Pennsylvania. Aside from possessing superior tech skills, I find that our staff’s foreign language skills – particularly Portuguese due in significant part to the many matters that originate from Brazil – and their experiences with diverse cultures offer us a better understanding of those matters with an international component. In fact, we recently added a paralegal with that background to our team.



Fernando M. Pinguelo is the new breed of lawyer – The CYBER LAWYER, who is knowledgeable of both the legal and technical side of the cyber world. Fernando works closely with business executives and IT managers to develop strategies for managing business and legal issues relating to electronic data. He focuses client attention on preventing claims and pursues strategies that enhance a client's ability to manage data- essential precautions because of the financial and public relations fallout that often results from high-profile data breaches. Fernando Pinguelo is a lawyer who knows how to apply 'ancient' (or non existent) laws to the fast-paced tech sector to help resolve disputes or address (and mitigate) an emergency. To learn more visit [www.CyberJurist.com](http://www.CyberJurist.com) or email [fernando@CyberJurist.com](mailto:fernando@CyberJurist.com)

### Career highlights

- Partner/Chair-Cyber Security & Data Protection Group – Norris, McLaughlin & Marcus (140 lawyers who practice in NY, NJ, and PA; with global affiliates in more than 70 countries and in each of the 50 U.S. States)
- Trial lawyer with 15 years experience practicing in federal and state courts – e.g., business disputes, cyber security, media and employment matters in federal and state courts.
- Appointed by Chief Justice to serve on New Jersey Supreme Court Committee on Rules of Evidence
- Tried first case in New Jersey interpreting state eDiscovery rules
- Designated by the U.S. Fulbright program as a Fulbright Specialist in eDiscovery
- Adjunct Law Professor, Seton Hall Law School
- AWARDS:
  - Martindale-Hubbell's AV Preeminent rating since 2011, its highest lawyer rating which serves as an objective indicator of a lawyer's high ethical standards and legal knowledge.
  - The New York Enterprise Report awarded him its Technology Lawyer of the Year award which recognizes the New York tri-state area's top business advisors.
  - Book Author: Chapter 13 (eDiscovery), New Jersey Federal Civil Practice (NJLJ–2013 Edition)
  - Book Author: Chapter 4 (The Cloud, Server Consolidation, Ephemeral Data, and Information Security), eDiscovery Special Edition, PenTest (September 2012)
  - Author of more than 100 articles addressing several topics including law, technology, and the practice of law.
  - Lecture nationally and internationally about law and technology, including presentations in New York, Los Angeles, New Orleans, Boston, Albuquerque, São Paulo, Guadalajara, and Paris.
  - Creator, ABA Journal award-winning blog eLessons Learned – Where Law Technology & Human Error Collide ([www.eLLblog.com](http://www.eLLblog.com)); and cyber security blog eWhite House Watch – Where Law Technology and Politics Collide ([www.eWHWblog.com](http://www.eWHWblog.com))
  - Represents a wide variety of clients from individuals, to Fortune 100 companies, to small and mid-cap private companies.
  - Law Clerk, Hon. Edwin H. Stern, P.J.A.D. (ret.)
  - J.D., Boston College Law School (1997); B.A., Boston College, magna cum laude (1994)
  - NJ Bar 1997, NY Bar 1998, D.C. Bar 1999

### What are the most pressing data issues facing your clients and businesses in general?

Class actions are one of the hot button cyber issues of the day – or at least the one that seems to grab the headlines. For example, around the time of the Facebook IPO, a class action lawsuit involving Facebook's improper use of users' personal data for advertisement purposes dominated the headlines, and was a contributing factor to Facebook's sluggish stock price. These types of suits are not going to go away anytime soon because the profit incentive related to aggregating and selling user data is too great for websites to ignore. But, the challenges potential plaintiffs face, such as lack of uniformity in the class and inability to prove concrete damages, are very real and may temper this current trend.

However, an area that receives less public outcry but a significant amount of press, and that can threaten the very core of a business' survival, is corporate espionage. Daily, numerous companies fall victim to surreptitious attacks in which valuable customer information and intellectual property are stolen. In corporate America, where trade secrets are a precious commodity, hackers engaged in economic espionage are using military-style techniques to steal information from company computer systems. This information may be sought by foreign governments, industry competitors or "hacktivists" (individuals or organizations who steal data to advance ideological agendas). Healthcare is particularly vulnerable to cyber-attacks and security breaches, as hospital staffs wrestle with the transition from paper to electronic records in compliance with a plethora of federal and state regulations. Hospitals in Georgia and California have experienced virus attacks that have shut down vital hospital systems and, in one case, the entire hospital. Recently, a physician's group received an email that its data had been stolen and encrypted by *the thieves*, and the thieves demanded ransom for the password. Across all industries malicious insiders – disgruntled employees – can be an especially harmful brand of cybercriminal. While determined cyber spies may be difficult for even the most well-funded corporations to stop, increased investment in firewalls, anti-virus software, and company cybersecurity awareness campaigns can help reduce at least some of the risk.

### Describe the critical legal issues raised by these types of disputes.

Typically, these class action suits involve some invasion of user privacy through the aggregation and sale of "personal" data – the user's likeness, web patterns, etc. Cases that span national borders are usually focused on discovery issues, whether U.S. court orders may be followed in countries where local laws proscribe transmission of personal data, including email, beyond the country's borders without the consent of the data subjects (senders and re-

cipients identified in the email). This can place litigants in the position of deciding whether to go to jail in their home country, for sending such data to the U.S. in response to a court order, or in the U.S. for violating the order. The ABA, in February of this year, passed a resolution urging U.S. judges to consider and show appropriate respect for foreign data privacy and data protection laws that affect litigants before them. Maybe that will provide U.S. judges with a more global perspective on the effects of court orders in cases involving multinational corporations.

As far as corporate espionage is concerned, email extraction programs, spam, social media scraping applications, and phishing continue to be used in order to infiltrate a business' system. The techniques and applications are becoming more and more sophisticated and effective. But a company can take proactive steps in this regard, and one of them is to create a culture of cyber-awareness through preparation of information management and security policies and procedures, prepared by interdisciplinary teams comprised of IT professionals, records management staff, legal (outside counsel and in-house attorneys), and business owners, and training on those protocols.

### What are some of the most recent matters you've worked on that implicate this area of the law?

Last year, an international company retained me to assist it in identifying a user of a popular, cloud-based file sharing website who posted for public view parts of a highly confidential report without authorization. I led U.S. efforts to compel the website to turn over information about its user. As one can imagine, timing was critical to the client. In fact, the situation couldn't have gotten any worse in that we had no choice but to file the emergency application the week of Christmas – not the best time of year to ask a U.S. court to decide an emergency application seeking a temporary injunctive relief. And yes, the website gave us the information we sought on behalf of my client. At the small business level, routine breach of contract lawsuits can have much more significant elements than may first meet the eye. For example, earlier this year I was called into court on two days' notice to address a temporary restraining order (TRO) and writ of attachment application that threatened to destroy the very existence of the client's business that had been built over the course of fifteen years. Over a holiday weekend, I mobilized my legal and tech teams and worked closely with the client in preparing our opposition when we uncovered evidence that a former employee had been siphoning sensitive business information to the very company who sued the client (and who hired the former employee). We used this information to successfully oppose the motion, and are now aggressively pursuing counterclaims seeking three times the damages being sought by the



plaintiff. I can go on, but suffice it to say that technology impacts *everyone*. Consequently, I can find myself representing a renowned international doctor who's fallen victim to an Internet defamation initiative one day, and a *Fortune* 100 company who's data security has been breached the next. These matters come in all shapes and sizes and my team is prepared to address them – *immediately*.

### **Why is it that data security breaches seem to be happening with greater frequency?**

Data and security breaches have permeated a broad cross-section of businesses – big and small – and industries for more than ten years. The “suddenness” you reference more relates, I think, to the publicity that high-profile breaches (Epsilon, Sony, LinkedIn, come to mind) have garnered the past few years, the continued, exponential growth of computer and Internet use (especially on mobile and tablet devices), the development of and access to powerful, inexpensive computers, and governments’ attempts to regulate the unexpected impact that this rapidly moving juggernaut known as technology has on global commerce. Throw negligence and ignorance into the mix and you get ... well, you know where I’m going with that. So, needless to say, this area will continue to grow – undoubtedly.

### **How do you see your team developing in the future?**

I think my team will be forced to grow to keep up with market demand as explained in my previous answer. I could see our team doubling over the next two years. And, contrary to conventional wisdom, *my* focus is on new or recent law school graduates. As popular, student-run legal/tech blogs such as *eLessons Learned* ([www.eLLblog.com](http://www.eLLblog.com)) demonstrate, young lawyers “get it” and are increasingly committed to advancing their own experiences and education.

### **How does your team fit the greater structure of your full service law firm?**

The lawyers at my firm come from diverse backgrounds, hold degrees from top U.S. law schools, and regularly serve as leaders in legal bar associations and various trade groups. We possess large-firm talent in a smaller firm setting that allows our attorneys to provide service and value to our clients on a personal level. It is the firm’s goal to accommodate the needs of every client through our experience, responsiveness, strategic planning, and through the use of technology. First and foremost, I am a trial lawyer and I know when and how to turn to the courts for relief under any given circumstances. However, that alternative may not be the best way to proceed and I often consider other, less confrontational means of achieving the same objectives. To the extent a matter requires specialized, substantive expertise beyond mine, I work closely with my partners and as-

sociates with specialties in other legal disciplines and lead those efforts accordingly. For pre-litigation data security matters, I coordinate efforts in a similar fashion and rely more heavily on the expertise of technologists and investigators to assist in the efforts.

### **Is there a particular technology that you rely on in handling your matters?**

Personally, I stick to the basics – PC, laptop, and smartphone; and the Internet, email, and texting – and all their permutations (name brands omitted, intentionally). But I never forget the importance of the human element which must never be underestimated. Sitting down, *face-to-face* with an employee to assess what happened is an invaluable exercise because you learn so much more about the facts than you normally would by phone or email – or worse, from a supervisor. As far as scenario-specific software and tools are concerned, it really depends on the type of incident and the situation – there is no getting around that general response. There are a number of commercial off the shelf, open source tools that can be effective in handling cybersecurity incidents. What I can say is that it comes down to how well prepared the organization is to handle an emergency in crisis situations where hacking is involved. Most of that preparation involves having access to an all-star team ready to dive into action when called.

From a preventative perspective, organizations need to understand their risk profile and address it reasonably; and that’s where our interdisciplinary team comes in – we help the client sort through the many elements of such an assessment and offer customized solutions. For example, an ice cream shop will not have the same risk profile as a multinational bank. Organizations may consider encrypting sensitive data with AES (advanced encryption standard) encryption. Network segmentation – a concept alluded to by the court in the recent, headline-grabbing *Apple v. Samsung* case, albeit in a different context – may also be a practical, effective method to secure the part of a network or systems that stores the most sensitive data.

### **Tell me more about this team of yours.**

Sure. In addition to our core legal team, we draw upon other individuals from diverse professional backgrounds who offer expertise in each of the elements necessary to address an evolving crisis, including computer and software technologists experienced in IT security, infrastructure breaches, and hacking techniques; retired federal and state prosecutors and investigators including professionals from the U.S. Attorneys Office, FBI, and Secret Service; and public relations and media professionals knowledgeable and experienced in the issues concerning information dissemination, who are particularly useful in addressing public disclosure obligations that many federal and state laws mandate.

# COMPUTER FORENSIC CERTIFICATIONS EXAMINED

by Terrance J. Stachowski, CISSP, L|PT

This article explores a range of popular certifications applicable to computer forensics. Examined are various types of certifications available, certification bodies, topics covered in the certification exams, requirements for continued certification, and associated costs.

## What you will learn:

- Which digital forensic certifications are in demand in the field.
- The prerequisites for taking digital forensic certification tests.
- The costs associated with various certifications.

## What you should know:

- A basic understanding of information technology certification process.
- How certifications relate to digital forensics world.

Computer forensics, also known as cyber forensics, or digital forensics, is a focused wing of information technology which revolves around digital evidence which is used in the court of law. “Computer Forensics is the specialized practice of investigating computer media for the purpose of discovering and analyzing available, deleted, or “hidden” information that may serve as useful evidence in a legal matter (Hassell & Steen, 2004).”

The computer forensics community, much like every other realm of information technology, places a high value on certifications as one way to validate competency and proficiency with best practices, knowledge of related tools, and computer forensics procedures. An additional similarity which computer forensic careers share with other specialized informa-

tion technology positions is that many require previous experience – but computer forensic roles may not only require previous information technology experience, legal and forensic experience might be required as well. Without a law enforcement or legal system background, landing a computer forensics job may be a difficult undertaking; therefore pursuing training, certification or a formal education may help a candidate move towards a career in computer forensics.

## LIST OF POPULAR COMPUTER FORENSICS CERTIFICATIONS

### ENCASE CERTIFIED EXAMINER (ENCE) – OFFERED BY GUIDANCE SOFTWARE

EnCase is arguably the best known computer forensic software in the market. The EnCE certification which is offered by Guidance Software, cer-

tifies professionals from both the public and private sector in the use of EnCase software. The EnCE certification validates that professionals holding this certification have mastered computer investigation methodologies and the use of EnCase during complex computer examinations. This certification is recognized by both the corporate world and law enforcement as a sign of in-depth computer forensics knowledge. Holders of this certification are typically considered to be experts in utilizing EnCase.

Prerequisites for taking the EnCE exam are attending 64 hours of authorized computer forensic training (which may be accomplished online or in a classroom environment), -or- by having 12 months of verifiable computer forensics experience. A candidate must also complete and submit an EnCE application.

The EnCE exam is broken into two phases: a written exam, and a practical exam. The written exam consists of 180 true/false questions (174 for international students – no legal questions), and two hours are provided to complete the test, a passing score of 80% must be achieved to pass the test.

The practical exam is delivered to the candidate via a thumb drive which contains: a “certification” version of EnCase Forensic, evidence files, and objectives that the candidate must address. The candidate must “work” the case, compile a report, and then submit the report to Guidance Software for review and grading within 60 days. Candidates who failing the written exam are required to wait 2 months before retesting; failing the practical test requires a 2 month wait as well, but failing the practical portion a second time will require the written test be retaken.

The EnCE certification is valid for 3 years; renewal requires paying a fee, as well as accomplishing one of the following:

- Attend a minimum of thirty-two (32) credit hours of documented, continuing education in computer forensics or incident response within the renewal period.
- Achieve a computer forensics or incident-response related certification within the renewal period.
- Attend one CEIC conference within the renewal period.

Costs associated with this certification:

EnCE certification – \$200 (USD) or \$225 (USD) for international testers

Renewal fees (every 3 years) – \$75 (USD)

Additional information and resources on the EnCE certification can be found on the Guidance Software web site: <http://www.guidancesoftware.com/default.aspx>

### **CERTIFIED COMPUTER EXAMINER (CCE) – OFFERED BY THE INTERNATIONAL SOCIETY OF FORENSIC COMPUTER EXAMINERS (ISFCE)**

The CCE certification, offered by The *International Society of Forensic Computer Examiners* (ISFCE),

is rapidly growing in recognition. Many companies and government agencies are requiring their computer forensic examiners to hold the CCE certification in order to obtain or maintain their positions.

The CCE certification testing process is designed to test an applicant’s proficiency in several areas pertaining to digital forensics. The test measures knowledge via an online, multiple choice exam – proficiency is measured by way of an ISFCE-approved training course. Additional requirements for this certification include completing a verifiable self-study program, having a minimum of 18 months of verifiable experience in computer forensics, agreeing to the ISFCE code of ethics, and passing a criminal background check.

Costs associated with this certification:

- ISFCE Membership – CCE holder: No Fee
- CCE process: \$395.00 (USD)
- CCE recertification (every 2 years): \$75.00 (USD)
- Retake the CCE examination after waiting period: \$175.00 (USD)
- Additional information on the CCE certification can be found on the ISFCE web site: <http://www.isfce.com/index.html>

### **COMPUTER HACKING FORENSIC INVESTIGATOR (C|HFI) – OFFERED BY EC-COUNCIL**

The C|HFI, offered by the EC-Council, validates a candidate’s skills to identify an intruder’s footprints, and to properly gather the necessary evidence to prosecute in the court of law. The C|HFI provides proof of successfully passing a training course and an exam which covers many areas of computer forensic investigation.

The C|HFI certification is awarded after successfully passing exam EC0 312-49v8, which is available at Prometric, VUE and Prometric Prime centers around the world. The test is 150 questions, with a maximum duration of 4 hours allowed for testing, and a minimal passing score of 70%. The C|HFI requires renewal every three years, or the collection of 120 CPEs over the same time. There is no cost associated with CHFI renewal.

The C|HFI certification is often acquired by candidates first attending an official C|HFI training course, which is then followed by the single exam, but it is possible to waive the training requirements (with permission from EC-Council), but to do so, the candidate must have at least two years of information security related experience, must remit a non-refundable eligibility application fee of \$100 (USD), and submit a completed Exam Eligibility Application Form. Once EC-Council has given approval to take the test without training, the applicant will be required to purchase a voucher from EC-Council directly. EC-Council will then provide the candidate an eligibility code and voucher code which can be used at aforementioned test centers.



Costs associated with this certification:

- CJHFI Certification Test: \$500 (USD)
- Eligibility Application Fee: \$100 (USD)
- Approved, Official Training Course: Costs Vary
- Additional information and resources on the CJHFI certification can be found on the EC-Council web site: <https://cert.eccouncil.org>

## **CERTIFIED COMPUTER FORENSICS EXAMINER (CCFE) – OFFERED BY INFORMATION ASSURANCE CERTIFICATION REVIEW BOARD (IACRB)**

The CCFE tests a candidate's knowledge of the computer forensic evidence recovery and analysis process. A candidate's knowledge is evaluated in two parts, the first part of the test is a traditional multiple choice, true/false and multiple answer exam, the second part is a take-home practical exam. The multiple choice exam is made up of 50 questions, and the candidate has 2 hours to complete the exam. Candidates who pass the multiple choice exam are given access to the practical examination files, which are case files, and a scenario from a mock computer forensic case. The candidate must perform a computer forensics examination on the files, compile a report which could be used as evidence in a court of law, and return the report for grading within 90 days. There is no information on IACRB site pertaining to continuous education requirements, or renewal/membership fees.

Costs associated with this certification:

- Flat fee per exam: \$499 (USD)
- On-site proctored exams, per voucher: \$399 (USD)

Additional information and resources on the CCFE certification can be found on the IACRB web site: [http://www.iacertification.org/ccfe\\_certified\\_computer\\_forensics\\_examiner.html](http://www.iacertification.org/ccfe_certified_computer_forensics_examiner.html).

## **GIAC CERTIFIED FORENSIC ANALYST (GCFA) – OFFERED BY THE SANS INSTITUTE**

The GCFA certification is geared towards professionals working in the information security, computer forensics, and incident response field. The certification focuses on the skills required to collect and analyze data from Linux and Windows systems, the ability to conduct formal incident investigations, incident handling procedures, and various forensic techniques.

SANS training is an option to prepare for the certification exam, but is not required to take the exam.

The test is a proctored exam, comprising of 115 questions, with a 3 hour time limit, and a minimum passing score of 69%. The GCFA is valid for four years. A candidate may begin efforts towards the recertification process two years before the certification expires. A candidate is required to earn

36 Certification Maintenance Unit (CMU) points to demonstrate ongoing competency. There are various ways to earn CMU points, such as: retaking the exam, training/teaching, publishing work, as well as various supplemental options.

Costs associated with this certification:

- Exam fee: \$999 (USD)  
Retake failed exam (must purchase within 30 days): \$549 (USD)
- First renewal fee: \$399 (USD)
- Subsequent renewal fees: \$199 (USD)

Additional information and resources on the GCFA certification can be found on the GIAC web site: <http://www.giac.org/certification/certified-forensic-analyst-gcfa>.

## **GIAC CERTIFIED FORENSICS EXAMINER (GCFE) – OFFERED BY THE SANS INSTITUTE**

The GCFE is aimed at professionals working or interested in the information security, legal and law enforcement industries, with a need to understand computer forensics. The certification focuses on the skills required to collect and analyze data from Windows systems. The GCFE certifies that a candidate has the knowledge, skills, and ability to conduct incident investigations, forensic analysis and reporting, and evidence acquisition.

SANS training is an option to prepare for the certification exam, but is not required to take the exam.

The test is a proctored exam, comprising of 115 questions, with a 3 hour time limit, and a minimum passing score of 71%. The GCFE is valid for four years. A candidate may begin efforts towards the recertification process two years before the certification expires. A candidate is required to earn 36 Certification Maintenance Unit (CMU) points to demonstrate ongoing competency. There are various ways to earn CMU points, such as: retaking the exam, training/teaching, publishing work, as well as various supplemental options.

Costs associated with this certification:

- Exam fee: \$999 (USD)
- Retake failed exam (must purchase within 30 days): \$549 (USD)
- First renewal fee: \$399 (USD)
- Subsequent renewal fees: \$199 (USD)

Additional information and resources on the GCFE certification can be found on the GIAC web site: <http://www.giac.org/certification/certified-forensic-examiner-gcfe>.

## **CYBERSECURITY FORENSIC ANALYST (CSFA) – OFFERED BY CYBERSECURITY INSTITUTE**

The CSFA certification test is an advanced test designed for professionals who already possess

practical experience in the field. The candidate has 3 days to complete the test. There is a written component which consists of 50 multiple choice questions, and equates to 30% of the total score, and a practical portion which makes up 70% of the score. The practical portion consists of a scenario which includes processing a hard drive and may include additional media such as a CD, DVD, or USB drive. Some scenarios include a cellular phone, or a handheld device. An overall score of 85% is required to earn the CSFA certification.

The CyberSecurity Institute suggests that test candidates have at least two years of computer forensic experience, and should have already obtained one of the following certifications: ACE, CFCE, CCE, CJHFI, EnCE, or the GCFA.

When applying to take the exam, candidate must also submit an FBI background check, and fingerprint cards. To maintain certification, a candidate must attend a minimum of 120 class hours of digital forensics / information technology training every two years. Costs associated with this certification: Exam fee: \$400 (USD).

Additional information and resources on the CFSA certification can be found on the CyberSecurity Institute web site: <http://www.cybersecurityforensicanalyst.com>.

### **IACIS CERTIFIED FORENSIC COMPUTER EXAMINER (CFCE) – OFFERED BY THE INTERNATIONAL ASSOCIATION OF COMPUTER INVESTIGATIVE SPECIALISTS (IACIS)**

The CFCE certification is offered by IACIS, who was recently was approved by the Forensics Specialties Accreditation Board (FSAB) as an accredited certifying body in the field of computer/digital forensics. The CFCE certification measures a candidate's knowledge of computer forensic acquisitions, authentication, reconstruction, examination, and analysis of data stored on electronic media. Candidates must have had formal training in the field of computer/digital forensics to qualify for enrollment in the CFCE program.

The certification process is broken down into two stages, the first is a peer review phase where candidates perform practical exercises, and once successfully completing that portion they can attempt the second phase, the written test. The written test is comprised of 100 questions. Both parts require 80% proficiency to receive a passing score.

Candidates may be required to undergo a background check as part of the registration.

Costs associated with this certification:

- Registration fee: \$750 (USD)
- Additional information and resources on the CFCE certification can be found on the IACIS web site: [https://www.iacis.com/certification/external\\_overview](https://www.iacis.com/certification/external_overview).

### **ACCESSDATA CERTIFIED EXAMINER (ACE) – OFFERED BY ACCESSDATA GROUP, LLC**

The ACE certification demonstrates a candidate's proficiency with the latest versions of AccessData's Forensic Toolkit (FTK), Password Recovery Toolkit (PRTK), FTK Imager, Registry Viewer. Candidates are allowed 90 minutes to complete the test, which is made up of practical and written assignments. AccessData supplies free studied guides on their site and there are no prerequisites for taking the exam. The best part is that the test is absolutely free! Recertification is required every two years. Costs associated with this certification: Enrollment: FREE.

Additional information and resources on the ACE certification can be found on the AccessData web site: <http://www.accessdata.com/training/certifications>.

### **CERTIFIED DIGITAL FORENSIC EXAMINER (CDFE) – OFFERED BY MILE2**

The CDFE certification exam tests candidates knowledge of forensic examination, tools of the trade, seizure concepts, incident investigation, electronic discovery and digital evidence, and the fundamentals of conducting a computer forensics examination.

Mile2 offer traditional classroom based training and live online, instructor-led training for \$3000 (USD), they also offer a courseware kit for \$450 (USD). It should be noted that neither training nor courseware need be purchased to attempt the exam.

The exam itself is a 100 question test – questions are randomly selected from a large pool of questions. The candidate has 90 minutes to finish the test and must score a 70% to pass.

Costs associated with this certification:

- Exam fee: \$250 (USD)
- Instructor-led training: \$3000 (USD) – optional
- Courseware kit – \$450 (USD) – optional

Additional information and resources on the CDFE certification can be found on the Mile2 web site: <http://mile2.com/digital-forensics-courses/certified-digital-forensics-examiner.html>.

### **MY RECOMMENDATIONS**

The first thing I would recommend to anyone interested in pursuing a career in computer forensics, is to spend some time researching job listings on sites such as: LinkedIn, Careerbuilder, Monster, Dice, and USAJobs for insight into which certifications are common across the board, which are in demand for particular area of focus, which certifications are desired – but not required, and which certifications aren't even mentioned. Some key terms which may help narrow the search process: computer forensics, forensics investigator, forensics examiner, forensic analysis, digital forensics, and cyber forensics.

Although results will vary greatly, a review of approximately fifty job listings in the beginning of De-

cember, 2012, revealed a demand for those with the following certifications:

- EnCE was listed in approximately 80% of the job postings as either required or desired.
- CCE was listed in approximately 40% of the job postings as either required or desired.
- CFCE was listed in approximately 36% of the job postings as either required or desired.
- Quality Security Assessors (QSA), by PCI Security Standards Council (not discussed in certifications above because it is a company-wide certification rather than individual) was listed in approximately 30% of the job postings as either required or desired. For more information on QSA, visit: <https://www.pcisecuritystandards.org/index.php>
- Listed in more than 2%, but less than 10% of job listings were the following certifications: IA-CIS, DCITP, ACE, CISA, GSE, SCNA, GCIH, CSIH, CEH, GFCA, and DCITA.
- Also, although not computer forensic certifications, 10% of listings also required or desired the CompTIA A+ and 20% required or desired the ISC(2) CISSP certification.

Based on results gathered from the same search used for the figures listed above, experience with the following tools was listed as desired or required:

- EnCase was listed in 80% of job postings.
- Forensic Toolkit (FTK) was listed in 60% of job postings.
- dtSearch was listed in 20% of job postings.
- Safeback was listed in 20% of job postings.
- Listed in more than 2%, but less than 10% of listings were the following tools: BlackLight, Data Breach, Data Lifter, DCFLDD, Enscript, Helix, Ilook, Incident Response, Knoppix, Mac-ForensicsLab, Paraben, RCMP Utilities, SIFT, Slax, Sleuthkit, SMART, Ximager, Xways forensics, and open source (Linux) forensic tools.

It should however be noted that the above list of certifications is not fully encompassing, there exists many additional vendor neutral and vendor-specific forensic certifications, the above list is simply a collection of some of the more popular certifications.

Additionally, having the skills and certifications provided in the listing above should not be viewed as a guarantee into the world of computer forensics; many positions express that a certain amount of experience, and/or the minimum of a Bachelor's degree in a computer science field is required for placement. Those positions which adhere to the DoD 8570 series of regulations may require a certification such as Security+ or CISSP. Additional skills/certifications outside the scope of forensics may be required or at very least may help a resume stand out. Some

## References

- AccessData (n.d.). Retrieved from: <http://www.accessdata.com/training/certifications>
- EC-Council (n.d.). Retrieved from: <https://cert.ec-council.org>
- CyberSecurity Institute (n.d.). Retrieved from: <http://www.cybersecurityforensicanalyst.com/>
- GIAC, GCFA (n.d.). Retrieved from: <http://www.giac.org/certification/certified-forensic-analyst-gcfa>
- GIAC, GCCE (n.d.). Retrieved from: <http://www.giac.org/certification/certified-forensic-examiner-gcfe>
- Guidance Software (n.d.). Retrieved from: <http://www.guidancesoftware.com/computer-forensics-training-ence-certification.htm>
- Hassel, J., Steen, S. (2004). Computer forensics 101. Retrieved from: [http://www.expertlaw.com/library/forensic\\_evidence/computer\\_forensics\\_101.html](http://www.expertlaw.com/library/forensic_evidence/computer_forensics_101.html)
- Information Assurance Certification Review Board (n.d.). Retrieved from: [http://www.iacertification.org/ccfe\\_certified\\_computer\\_forensics\\_examiner.html](http://www.iacertification.org/ccfe_certified_computer_forensics_examiner.html)
- International Association of Computer Investigative Specialists (n.d.). Retrieved from: [https://www.iacis.com/certification/external\\_overview](https://www.iacis.com/certification/external_overview)
- International Society of Forensic Computer Examiners (n.d.). Retrieved from: <http://www.isfce.com/index.html>
- Mile2 (n.d.). Retrieved from: <http://mile2.com/digital-forensics-courses/certified-digital-forensics-examiner.html>
- PCI Security Standards Council (n.d.). Retrieved from: <https://www.pcisecuritystandards.org>

certifications which would likely compliment a forensic investigator resume are: A+, Linux+, MSCE, MCITP, CCNA, C|EH, and the CISSP. Experience with various hardware platforms, operating systems, networking components, smart phones and mobile devices would be a plus. I would also recommend talking to people already in the computer forensics field to get further guidance; certification and forensics forums, and career sites such as LinkedIn would be a good place to make new contacts and get insider information on how to successfully break into the field, or progress in one's career.

This article examined a range of popular certifications applicable to computer forensics. With any luck, this article helps to shed some light on the various types of certifications available, what certification bodies exist, and gives potential candidates some insight on what to expect going into the certification process.

## Author bio



*Terrance Stachowski is a defense contractor supporting the United States Air Force. He has worked in Information Technology for the past fifteen years, currently holds nineteen IT certifications, including the CISSP and L|PT, and will finish his M.S. in Cybersecurity from Bellevue University in*

*March of 2013. He specializes in IT Security, Penetration Testing, and Solaris Systems Engineering. He can be reached at [terrance.ski@skeletonkeyss.com](mailto:terrance.ski@skeletonkeyss.com).*





## IT Security Courses and Trainings

**IMF Academy is specialised in providing business information by means of distance learning courses and trainings. Below you find an overview of our IT security courses and trainings.**

### **Certified ISO27005 Risk Manager**

Learn the Best Practices in Information Security Risk Management with ISO 27005 and become Certified ISO 27005 Risk Manager with this 3-day training!

### **CompTIA Cloud Essentials Professional**

This 2-day Cloud Computing in-company training will qualify you for the vendor-neutral international CompTIA Cloud Essentials Professional (CEP) certificate.

### **Cloud Security (CCSK)**

2-day training preparing you for the Certificate of Cloud Security Knowledge (CCSK), the industry's first vendor-independent cloud security certification from the Cloud Security Alliance (CSA).

### **e-Security**

Learn in 9 lessons how to create and implement a best-practice e-security policy!



### **Information Security Management**

Improve every aspect of your information security!

### **SABSA Foundation**

The 5-day SABSA Foundation training provides a thorough coverage of the knowledge required for the SABSA Foundation level certificate.

### **SABSA Advanced**

The SABSA Advanced trainings will qualify you for the SABSA Practitioner certificate in Risk Assurance & Governance, Service Excellence and/or Architectural Design. You will be awarded with the title SABSA Chartered Practitioner (SCP).

### **TOGAF 9 and ArchiMate Foundation**

After completing this absolutely unique distance learning course and passing the necessary exams, you will receive the TOGAF 9 Foundation (Level 1) and ArchiMate Foundation certificate.



**For more information or to request the brochure please visit our website:**

<http://www.imfacademy.com/partner/hakin9>



IMF Academy

[info@imfacademy.com](mailto:info@imfacademy.com)

Tel: +31 (0)40 246 02 20

Fax: +31 (0)40 246 00 17



**Allow  
us to  
guide  
your  
CAREER**



SENIOR  
PRACTITIONER



### 2013 PUBLIC COURSE SCHEDULE

#### CISMP

Mar 18-22, Apr 22-26, May 13-17, Jun 10-14,  
Jul 8-12, Sep 30 - Oct 4, Oct 14-18, Nov 18-22

#### PCiBCM

Mar 18-22, Apr 8-12, Apr 22-26, Jun 10-14, Jul 8-12,  
Aug 5-9, Sep 16 -20, Oct 14-18, Nov 11-15, Dec 9-13

#### PCiIRM

Apr 22-26, May 6-10, May 20-24, Jun 3-7, Jun 17-21,  
Jul 8-12, Jul 22-26, Aug 5-9, Oct 7-11, Oct 21-25, Nov 4-8,  
Nov 18-22, Dec 2-6, Dec 16-20

If you are interested in learning more, get in touch:  
[contact@infosecskills.com](mailto:contact@infosecskills.com).



PRACTITIONER





# FORENSICS EUROPE EXPO

24 – 25 April 2013

Olympia, London

[ForensicsEuropeExpo.com](http://ForensicsEuropeExpo.com)



The Premier International Forensics Event for Police, Military, Intelligence Agencies, Lawyers, Corporate Forensic Analysts, Laboratories, Government Bodies and Agencies together with leading suppliers, services, equipment and practitioners from across the world.

Conferences – Workshops – Training – Networking – Exhibition

**REGISTER FOR FREE ENTRY TODAY**

[www.ForensicsEuropeExpo.com/digital](http://www.ForensicsEuropeExpo.com/digital)

Co-located with

  
**COUNTER  
TERROR EXPO**

Sponsored by



In Collaboration with



Organised in  
Partnership with

