An Overview to Digital Forensics Tools

Waldemar Blakely Santiago
Computer Engineering
Jeffrey L. Duffany, Ph.D.
Computer Engineering Department
Polytechnic University of Puerto Rico

Abstract *— This paper is in support of seven newly created tutorials, focused on different digital forensic analysis tools. The tutorials are intended as in-class laboratory exercise for the computer forensics classes at the Polytechnic University of Puerto Rico. These tutorials are specifically designed to provide basic understanding on the functionalities and capabilities of each particular digital forensic tool. The seven tutorials will serve as a starting point for new users to explore and acquire knowledge in the computer forensics field.*

Forensic analysis tools are currently been used by law enforcement, private forensic investigators and particular individuals to recover evidence, company files or personal files from specifics electronic medias. The correct use of digital forensics tools is a key factor in the recovery, authentication and analysis phase of electronic data. The newly created tutorials provide examples of the examination phases of electronic media and digital data.

Key Terms *— Data Recovery, Electronic Data, Forensics, Storage Device, Tutorial.*

INTRODUCTION

Digital Forensics, also known as Computer Forensics, is a common name used to describe the analysis and reporting on findings from the forensic analysis of all computer or digital-related media. Digital Forensics not only includes personal computer and laptops or server hard drives, but also other storage devices such as USB flash drives, MP3 players, memory cards, SIMS, cell phones and data gathered via network analysis.

The purpose of the newly created tutorials is to provide a basic understanding to new computer forensic tools users on how digital forensics works. The tutorials will provide users with the description of the graphical user interface, examples of how to employ the tool, and practical exercises.

The tutorials are designed around seven digital forensics analysis tools which are described as follows:

- **Exif Reader:** an image file analysis tool designed to work on Microsoft (MS) Windows Operative System (OS).
- **WinHex:** a universal hexadecimal editor created for Windows file types.
- **Thumbnail Database Viewer:** a cache viewer which is used in MS Windows OS to display the contents of thumbnails files.
- **Recuva**: a data recovery tool designed to recover deleted files in Windows 98, Windows 2000, Windows 2003, Windows XP, and Windows Vista.
- **DAMN's Hash Calculator**: a simple and lightweight tool for generating checksums.
- **JPHS for Windows:** a steganography tool which allows hiding a file in a Joint Photographic Experts Group (JPEG) visual image file.
- **SAMInside:** a professional tool for recovering logon passwords in Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, and Windows 7.

DIGITAL FORENSICS

Digital Forensics is a constant evolving field that is used to conduct investigations into computer related incidents, whether is to recover data by a user or to recover evidence by investigators. Computer forensics is commonly defined as the process of collecting, recovering, analyzing and preserving computer related data.[1]

It is important to understand that most of the digital forensics analysis tools are intended to be

specialized in a particular area of the computer forensics. That is the reason why there are a variety of specialized tools available to users. Each tool has some advantages and disadvantages, and the user can find a perfect balance between them. Most of data recovery scientists will relay on various tools to ensure a complete recovery and/or analysis.

The motivation to develop tutorials on different digital forensics tools is to illustrate new users the capabilities of free software in an everyday use environment. These tutorials are intended to provide the novice user with a basic understanding on how these applications work and how they can be used for their benefit. The major advantages of these tools are the recovering of deleted files, getting information from files, the protection of passwords or recovering of passwords without having to pay an expert to do those tasks.

Exif Reader

This application is intended to analyze images in order to identify the source of the image. Within this information is the make and model of the camera, date and time that the image was taken, the size of the picture and other useful information.

Exif Reader is an image file analysis software designed to run on Windows OS. EXIF stands for Exchangeable Image File Format, and is a standard for storing interchange information in image files, especially those using JPEG compression. Most digital cameras now use the EXIF format. [2]

The Exif Reader application was specially designed to analyze and extract data from a picture taken using a digital camera. It analyzes and displays the shutter speed, flash condition, focal length, and other image information included in the Exif image format which is supported by almost all the latest digital cameras.

Figure 1 shows an example of Exift Reader tool with an image loaded.

WinHex

WinHex is in its foundation a universal hexadecimal editor created for Windows OS Files. It is particularly helpful in the area of computer forensics, data recovery, low-level data processing, and IT security. Since WinHex goes directly to the hexadecimal values of the disk, this gives advantage by allowing users to access otherwise prohibited locations on a hard drive. This could be used to restore master boot records, file allocation tables and to do data carving on deleted files.

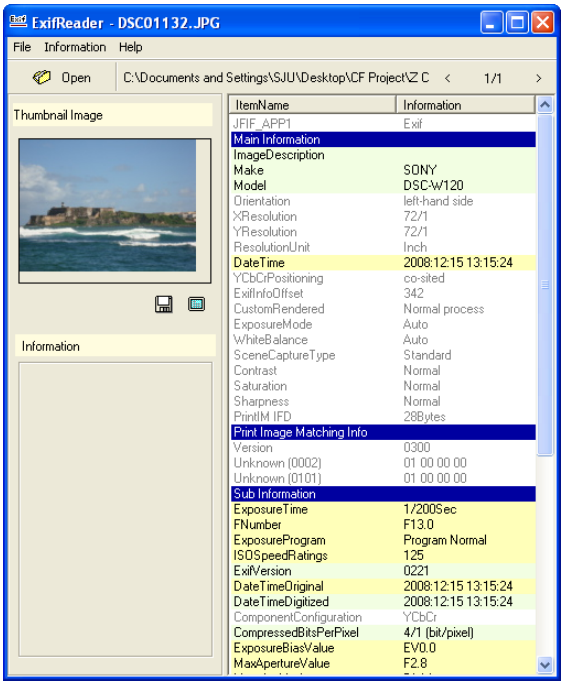

Figure 1
Exif Reader Application with an Image Loaded

WinHex is an advanced tool for everyday and emergency use. The application can be used to inspect and edit all kinds of files, recover deleted files or lost data from hard drives or from digital camera cards.[3] As an hexadecimal editor, it is a computer program that allows a user to manipulate computer files. A hex editor is capable of completely displaying the contents of each file type. Unlike a text editor, a hex editor even displays control codes and executable code, using a two-digit number based on the hexadecimal system.

WinHex will provide the user with the options to edit files using the hexadecimal window or by using the decimal or text window area. For example: A byte whose decimal value is 65 is displayed as 41 in hexadecimal notation and as the letter A in text mode. The American Standard Code for Information Interchange (ASCII) character set

defines the capital letter A to have the decimal value of 65.

When editing files of a certain type (for instance executable files), it is essential not to change the file size. Please note that changing the contents of a file generally may be the reason for the corresponding application to behave anomalously. It is quite safe to edit text passages in a file. At any rate, it is recommendable to create backup files before editing. Editing should never be done on an original file. Always edit on a copy of the original file.

Figure 2 shows WinHex application and displays the available options. Data can be edited in either the text or hexadecimal area, depending on the expertise of the user.

Thumbnail Database Viewer

This tool is intended to allow user to view images files that are or have been stored inside a specific folder, even if the images have been deleted. Thumbnail Database Viewer is a cache viewer which is used to display thumbnails files created by MS Windows. In MS Windows OS (Windows 98 and up) [4], a thumbnail cache is a file used to store thumbnail images for Windows Explorer's thumbnail view.

By creating thumbnails MS Windows can speed up the displaying of images as the smaller images do not need to be recalculated every time the user views the folder. It prevents intensive CPU processing and load times when a folder that

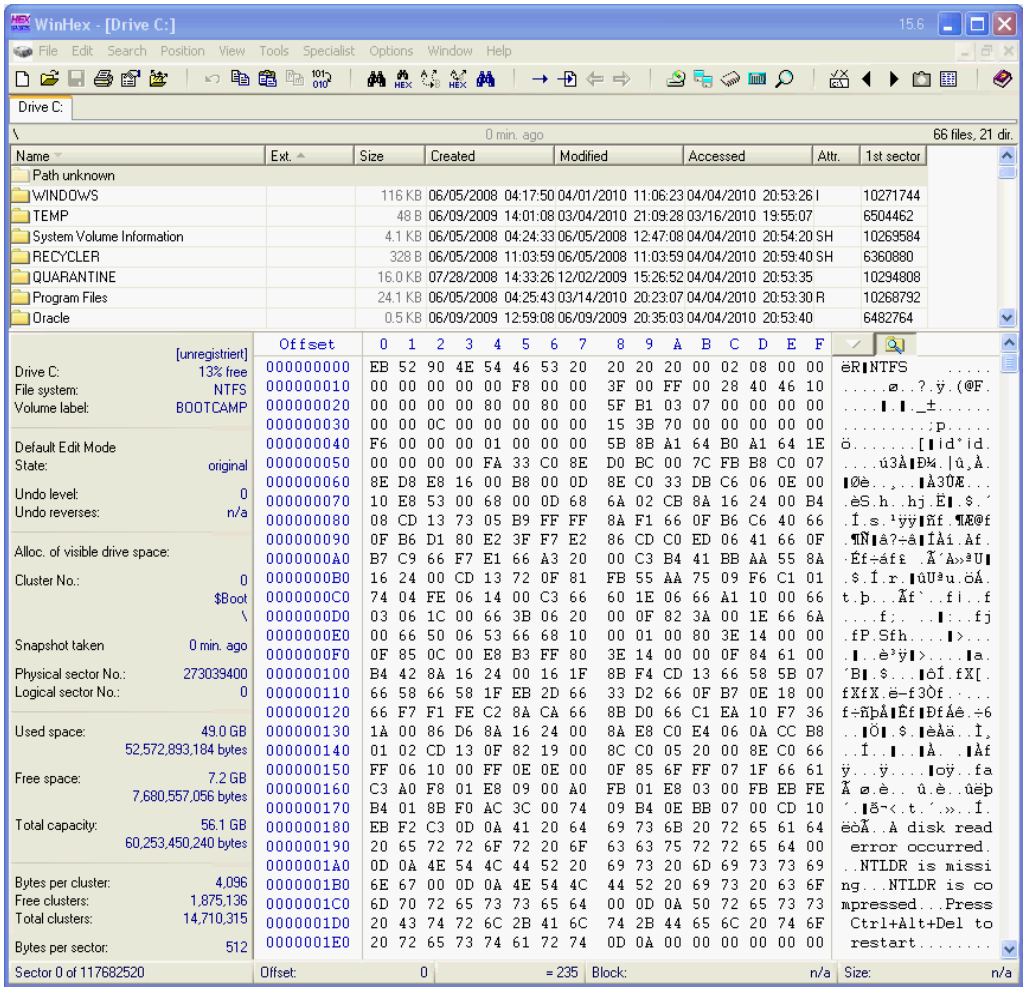

Figure 2
WinHex Main Window

contains a large number of files is set to display each file as a thumbnail.

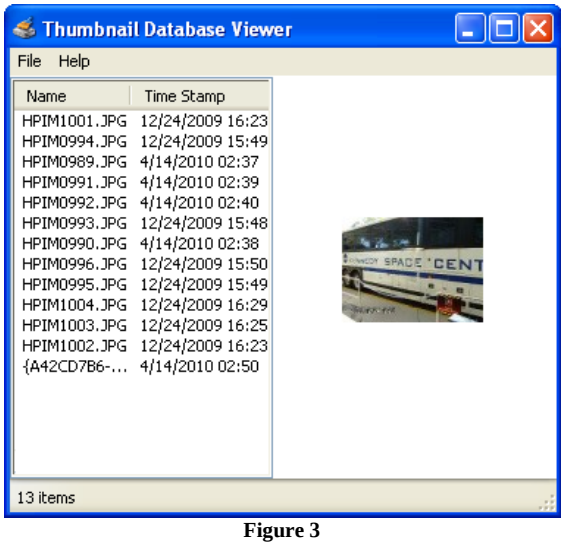

Figure 3
Thumbnail Database Viewer Main Window

Thumbnail Database Viewer is used in the forensic analysis of *thumbs.db* files providing details of the file name, when it was created and a small preview of the image file. *Thumbs.db* files are hidden files not viewed by most users and not updated when files are moved from a folder or deleted. This means that after an image has been deleted a small preview of the image will still be available inside the *thumbs.db* file of a particular folder.

Having the *thumbs.db* file available will help forensic investigators to locate files that are inside a folder or files that were previously inside a folder. Thumbnail Database Viewer will not recover the deleted files, but it can provide the forensic investigator with leads about pictures that were previously inside that particular folder even if they are long gone.

Figure 3 presents Thumbnail Database Viewer with a *thumbs.db* file opened. It can easily be observed that the file contains: names of files, time stamped, and a small image of each file.

Recuva

This forensic tool is designed to recover deleted files on a MS Windows environment. This is one of the easiest free software available to recover all types of files in a Windows system. It is intended to recover from images files, document files to unknown extension files.

Recuva is a freeware data recovery program, developed by Piriform, and designed for MS Windows 98, 2000, 2003, XP, and Vista. Recuva is able to recover files that have been "permanently" deleted and marked by the operating system as free space. [5] The program can also be used to recover files deleted from flash/USB drives, memory cards or MP3 players.

Recuva works on both FAT and NTFS file systems. It is able to recover lost directory structure and automatically renames files when trying to recover two files with the same name. As a file recovery program, Recuva works by looking for unreferenced data, but if the operating system has written new data over a deleted file then recovery will not be possible.

The software can recover missing files using either the file recovery wizard or the application's manual mode. The file recovery wizard is handy when the user is sure his data is gone but he is not quite sure where it went or how to get it back. The wizard lets the user narrow the search type to pictures, music, documents, video, or all files. The user can also set the search location to everywhere in the computer, removable media only, in My Documents, the Recycle Bin, or a specified location. In manual mode, the user get to work searching where the user knows the file should be.

Recuva uses a green/yellow/red light system to indicate how probable the recovery of the files will be, and when available, it can provide previews of image files available for recovery. Recuva also includes a tool to securely wipe files; handy if the user is attempting a file recovery just to ensure the files are actually dead and gone.

As shown in Figure 4, Recuva's easy to read information panels help the users to recognize the desired files to be recovered. The preview tab will allow users to preview files before recovering them.

DAMN's Hash Calculator

The usual intent of a hash function calculator is

that the hash can act as a signature for the original data, without revealing its contents. Providing the exact same input twice, the hash function will always produce the same output. Even a single bit changed in the input, though, should produce a different hash value. This is commonly used to verify if two files or texts are identical, such as passwords.

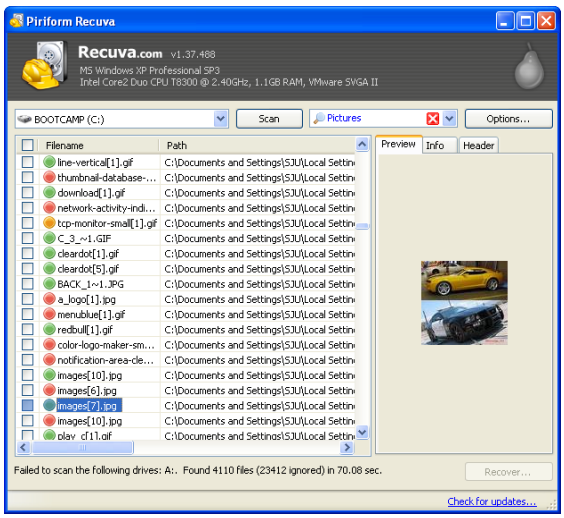

Figure 4
Recuva Main Window

DAMN's Hash Calculator is a simple and lightweight tool for generating checksums. The source can be a single file or a text entered into a text field. The tool also allows the users to select between five different hash algorithms to be calculated.

A hash function or cryptographic hash function is a procedure that takes an arbitrary block of data and returns a fixed size bit string. A hash value (or simply hash), also called a message digest, is a number generated from a string of text. [6] The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hash functions have many information security applications, notably in digital signatures used for forensics, message authentication codes, passwords and other forms of authentication. Any accidental or intentional change to the data will change the hash value.

The main advantage that DAMN's Hash Calculator has is that it does not have to be installed. Therefore it can be operated from any storage media. This feature gives DAMN's Hash Calculator the advantage against all other free hash calculators in the internet. Figure 5 has a demonstration on how DAMN's Hash Calculator works.

JPHS for Windows

Steganography is the science and art of writing hidden messages in such a way that no one, other than the sender and intended recipient, suspects the existence of the message. These types of applications that can actually hide files or text inside other data, such as inside an image file, can keep important information secured from been read or edited. Steganography application can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

JPHS is a program that allows a user to hide a file or a text in a jpeg image file. The idea of this steganography tool is not simply to hide a file but rather to do this in such a way that it is impossible to detect that the host file contains a hidden file.

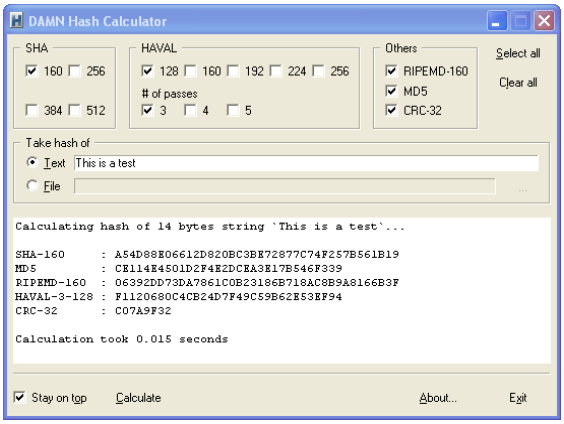

Figure 5
DAMN's Hash Calculator Main Window

In a typical image file, the absence of the original file will make impossible to conclude with any worthwhile certainty that the host file contains inserted data. Some images are much better than others when used as host files, especially if contain plenty of fine details. A cloudless blue sky over a

snow covered ski paradise is not recommended. A waterfall in a forest is probably ideal.[7]

Figure 6 contains the main window of JPHS. This tool is simple to use and does not require installation. All the user has to do is enter the name of the file they want to hide and the name of the jpeg file they want to hide it in.

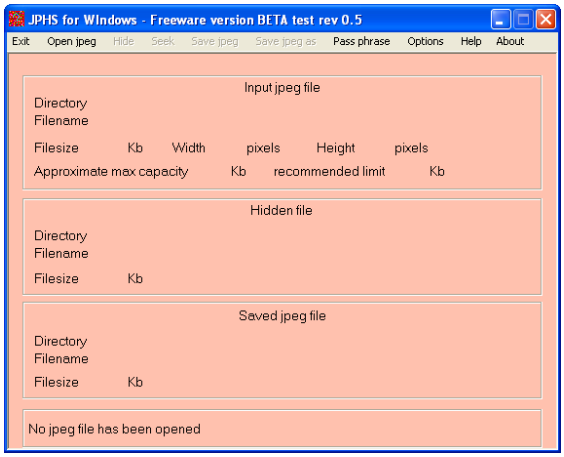

Figure 6
JPHS for Windows Main Window

JPHS for Windows uses a cryptographic algorithm as the basis of pseudorandom number generator. The key is derived from a pass phrase. This routine produces the same random numbers in the same sequence only when the key is the same. The random numbers are used to decide where the hidden data is stored within picture information. The result is that random noise is added to the visual information.[7]

SAMInside

This tool is a professional application for recovering logon passwords in Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, and Windows 7. This application, which does not require to be installed, demonstrates one of the highest password forcing speeds currently available. It can test and recover passwords at a speed of 10 millions per second in a modern computer. This is the result of core parts written in assembly language. It supports over ten types of data import, several types of attacks, and includes additional tools for extracting and processing encoded passwords.[8] It also has multi-language support and it is translated into five languages.

SAMInside uses a range of processes to attack the file including brute force, distributed, mask, dictionary, hybrid, and pre-calculated tables in order to obtain the password. SAMInside makes use of a comprehensive attack approach that relies more on the attack engines than a flashy interface. The demo has some listed limitations, but nothing that should stop expert users from testing this robust application.

SAMInside is a light weight tool, since it does not require installation. This means that the program can run from a CD/DVD disk or a USB drive. The application will be able to perform at the maximum speed of the CPU, since the recovery code is completely written in Assembly language.

Figure 7 presents SAMInisde window running a SAM file. The SAM file is usually located on MS Windows computers inside the following directory C:\Windows\System32\Config.

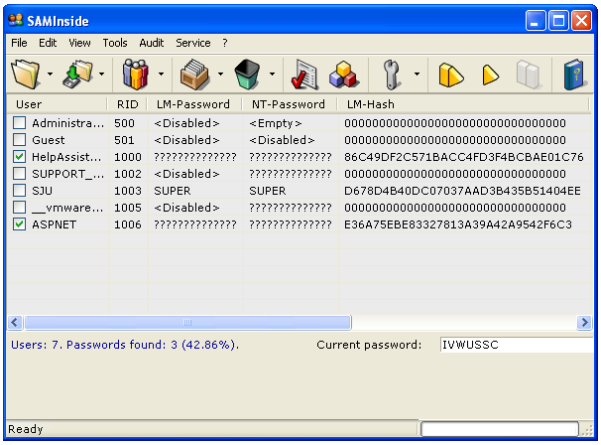

Figure 7
SAMInside Main Window

CONCLUSION

There are hundreds of Digital Forensics Tools available on the Internet. Most of these tools are specialized tools in a particular area of computer forensics. By selecting the correct tool, any new user or experimented digital investigator will be able to recover or analyze any data file. Since the digital forensics field is so wide, there is not a

simple tool that would do all types of analysis or data recover. It would be really difficult to find a tool that can do steganography, read thumbnails, read exif info from an image, get logon passwords and be an hexadecimal editor at the same time. The user has to determine which application to use depending on the data that wants to analyze or recover.

The seven tutorials created should be considered as a starting point for new digital forensic users. Each tutorial provides the description and uses of a specific tool, as well as examples and practical exercises. These tutorials are intended to expose new users to digital forensics applications, while leaving room for self experimentation with these tools and for the searching of other available tools.

REFERENCES

[1] "Computer Forensics For Law Enforcement", Retrieve on May 14, 2010, www.infosecwriters.com/text_resources/pdf/Forensics HStacy.pdf

[2] "Exif Reader Image Data File Analysis", Retrieve on March 7, 2010, www.takenet.or.jp/~ryuuji/minisoft/exifread/english/

[3] "X-Ways Software Technology AG", Retrieve on March 11, 2010, http://www.x-ways.net/

[4] "Thumbnail Database Viewer 2.0", Retrieve on March 22, 2010, www.softpedia.com/get/Multimedia/Graphic/Graphic-Viewers/Thumbnail-Database-Viewer.shtml

[5] "Recuva Home page.", Retrieve on April 4, 2010 www.piriform.com/recuva

[6] "General Purpose Hash Functions Algorithms – by Arash Partow.", Retrieve on April 7, 2010 www.partow.net/programming/hashfunctions/

[7] "Steganography", Retrieve on May 10, 2010, www.garykessler.net/library/steganography.html

[8] SAMInside Home page. Retrieved May 10, 2010 www.insidepro.com/eng/saminside.shtml