International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

MICROSOFT WINDOWS BASED COMPUTER FORENSIC TOOL

A. Mohammed[1]; E.O. Nwachukwu[2]; D. C. Igweze[3]
Department of Computer Science, Faculty of Physical Science, University of Portharcourt, Nigeria[123]
Abdulmohammedabdul@yahoo.com[1]

Abstract:

Computer Forensics involves the identification, acquisition, analysis and presentation of digital evidence stored in the form of encoded information. This paper discusses computer forensics and how it is applied under Microsoft Windows environment. The focus of the research has been on NTFS file system and forensic science as applied to Microsoft Windows. The underpinning knowledge developed in the theoretical framework is specifically applied to NTFS computers. The design and implementation of an NTFSUNDELETE file Recovery tool application software, using Visual C++ was achieved. This tool can be used to recover deleted files during a Computer based forensic investigation. The file recovery tool could be used by any interested person to recover accidentally deleted files under NTFS file systems on Microsoft Windows computers.

Keywords: Computer Forensic, Digital Evidence, NTFS, Visual C

1. INTRODUCTION

In the last decade there has been an enormous increase in computer usage. The development of digital equipment and the availability of computer networks have had a great impact on business today. A lot of transactions that were earlier done by regular mail are today conducted through automated processes on the Internet. This shift has made corporations dependent on computers and computer networks. In the past, information was stored in large archives as paper documents. Today information is stored electronically in database and often made available over networks. All of these changes have made a lot of the work easier for companies but the downside is that companies (and private persons) are more prone to attacks in cyberspace.

Criminals and the crimes they commit have always followed the development of new technologies closely; as soon as a new technology is developed the criminals adapt to it and use it to commit crimes. Technology advancements have had a positive influence on business opportunities but where businesses can make money there is potential for criminals to make money as well. Criminals have now entered the digital world and more and more crimes are committed with the use of computers or other digital devices. Therefore, Forensic investigators have also been forced to enter the digital world and this result in an increased need of computer forensic investigators in the past years.

Companies have opened their eyes for computer forensic and many, often larger, corporations have started up their own computer forensic teams within the company. There are a few software packages that have been widely used by computer forensic investigators, but the license fees are quite expensive.

There are few "complete" research papers that take up the forensic (investigative) work, forensic applied to computers and the technical background of the files system that is to be investigated. To conduct a sound computer forensic investigation, the examiner needs to have good knowledge of both the computer forensic process and the underlying technology. Papers focused on the computer forensic process often prerequisite good knowledge of operating system and the file system. Papers focused on forensics examinations of a particular file system often prerequisites good knowledge of the forensic process. There is a need for an introduction to computer forensics that takes up both of these areas.

Tools and techniques used in computer forensics are undergoing rapid development. There are few well accepted tools that have been successfully "proven in court". These tools have undergone extensive testing to prove that they do what they are supposed to do.

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

In addition to these few "accepted" tools there are several tools that have been developed by companies trying to enter the market. Many of the tools are good, even though they may not be as complete as the market leading ones. The problem with most of the tools is, as with most software applications, the lack of scientific approach to development by the development team [3]. Therefore, there is a risk that errors are introduced that makes it hard for an investigator to draw unambiguous conclusions based on the results presented by the tool.

There is need for education in computer crime and computer forensics, not only for forensic specialists but security personnel as well. Computer forensic training is offered by several companies but the training is often intended for future forensic specialists.

The aims and objectives of this paper are to give an introduction to the computer forensics process and describe how to apply computer forensics to NTFS computers and to discuss the design and implementation of a file recovery tool using Visual C++ programming language. This tool shall be used to undelete deleted files in a Microsoft Windows NTFS file system environment.

2. LITERATURE REVIEW

Forensic analysis of crime scenes have gone from securing physical evidence such as fingerprints and DNA (Deoxyribonucleic Acid) to secure digital evidence. Technological advances have resulted in more sophisticated crimes using computers and other digital equipment. Sometimes the computer or digital equipment is not used to commit the crime but digital evidence can be found that help investigators tie a suspect to the crime and the crime scene[1]. Forensic investigators therefore need to secure digital evidence as well as physical evidence. Digital evidence can be found in many different devices like computers, scanners, printers, digital cameras, cell phones etc.

This section discusses basics of computer system and forensic analysis. How digital evidence is processed, how computers are searched for evidence as well as how to analyze the evidence found on computers are discussed. The following chapters will explain where to look for evidence on an NTFS computer

2.1 FORENSIC ANALYSIS OF COMPUTER SYSTEM

Forensic analysis of computer systems is performed with specialized computer forensic tools, but in order to find and preserve the integrity of the evidence the investigator must be aware of how a computer and its file system works.

Every piece of evidence has a forensic value, which describes the possibility to draw conclusions from the evidence [2]. Time stamp has a high forensic value since it makes it possible to reconstruct the order of actions on the computer.

Forensic quality refers to how believable the information is [2]. Information like time stamps is considered to have a high forensic value, but it doesn't say anything about the forensic quality. If there is a possibility that the evidence has been tampered with, the forensic quality decreases.

2.1.1 COMPUTER DISKS AND FILE SYSTEMS

Computer hard disk is used for storing non-volatile data such as program files, system files and user-created files etc. Non-volatile data refers to digital data that remain in memory even if the power is turned off. Volatile data on the contrary is lost when the computer is turned off or the power is lost. Volatile data is for example found in the computer RAM.

A hard disk may be divided into logically separate partitions, each formatted to a volume using a file system such as FAT or NTFS (Windows computers). Files are handled and stored differently on different file systems and this paper is focus on NTFS used by windows 2000 and XP operating systems. A hard disk may contain up to four primary partitions which all can have different operating systems and different file systems.

A hard disk is divided into sectors which normally are 512-byte in size (determined by hardware). Two or more sectors form a cluster and thus the cluster size is always a multiple of the sector size. Cluster size varies between different file systems and on NTFS it is possible to manually set the cluster size when formatting the volume. Larger clusters can make the disk blocks more manageable but with increased waste of disk space [9].

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

A file stored on disk allocates as many clusters as needed to fit the entire file. Allocated clusters always belong to a certain file and cannot be split between two files. If for example a small file is saved to the disk but do not fill the entire cluster with data, the unused space of that cluster cannot be used for storing any other data as long as that file exists. This unused portion of the cluster is called slack space [4]. The last cluster allocated by a file will always leave a little bit of slack space, since it is highly unlikely that the file fills the entire cluster. Therefore an increased cluster size will result in increased waste of disk space, because the average size of the slack space will be larger [9].

Disk space not currently allocated by any file is called unallocated space. This does not mean that unallocated space is "empty space" on the hard disk. There is often a lot of information that could be found in unallocated space like deleted files or fragments of deleted files [4].

2.1.2 DATA FILES AND DATA AREAS

During a computer forensic investigation the file system is searched for evidence. Evidence is often found in files, but there are other data areas that may contain evidence like slack space and unallocated space[10]. One way to divide files and data areas is into the following four categories: user-created files, user protected files, computer-created files and other data areas [7].

User-created files are files that the user is somewhat aware of; it could be files downloaded from the Internet and saved on disk or files created by the user himself, such as address book, emails files, database files, documents or text files, etc.

User-created files have high forensic value and are therefore important, and a lot of evidence may be found. If the suspect is engaged in illegal activity it is possible that he/she tries to protect the illegal information from being disclosed. This can be achieved by the use of encryption or by using steganography and there are other ways as well. These kinds of files are referred to as **User-protected files**. Some other examples of User-protected files include compressed files, password-protected files, encrypted files etc.

Computer-created files are files that the computer system creates during normal operation, and are usually a rich source of information of what have been done on the computer. Some of the files are possible to delete and there are a lot of tools that could aid a criminal to erase tracks left on a computer. Even if such tools are used there are often some traces left and there may also be possible to find evidence of that such tools have been used. Examples of computer-created files include Backup files, log files, cookies, printer spool files, configuration files, etc

Other data areas refer to files and data areas not covered by the first three categories. The following are some examples: Bad clusters, deleted files, free space, hidden partition, slack space, unallocated space etc.

Note that **free space** is disk space not allocated by any partition, **unallocated space** is disk space not allocated by any file on a partition.

2.1.3 LIVE AND DEAD SYSTEM

When the investigator is to confiscate a live system there are some issues to consider before cutting the power. A live system refers to system that are up and running where information may be altered as data is continuously processed. Dead systems are systems that are switched off and no data processing is taking place [5]. To retain the integrity of the data it is often considered appropriate to cut the power supply to the computer, but this will have other implications.

There is a lot of information of evidentiary value that could be found in a live system. Switching it off may cause loss of volatile data such as running processes, network connections and mounted file systems. In contrast, leaving a computer running may cause evidence to be altered or deleted. The investigator therefore needs to decide what alternative is best in a given situation. Another approach is to use specialized tools to extract volatile data from the computer before shutting it down.

2.2 NTFS DISK STRUCTURE

NTFS Stands for "New Technology File System." NTFS is a file system introduced by Microsoft with Windows NT and is supported by subsequent versions of Windows, such as Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7,

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

released on October 22, 2009. NTFS is therefore a widely used file system on Windows systems today.

2.2.1 VOLUMES AND FILE SYSTEMS

A volume is a logical partition of the disk. There may be several volumes on one physical disk and each volume is represented by a drive letter and a colon (e.g. C: and D:) in Windows systems. Each volume is formatted with its own file system like FAT and NTFS on Windows systems or EXT2 and EXT3 in UNIX/Linux systems. NTFS offers higher security and more flexibility than the previous FAT file system.

2.2.2 CLUSTERS

A computer hard disk is divided into sectors and the file systems bundles one or more sectors together to form a cluster. A simple rule is that the larger the disk the larger the cluster size. Cluster size may be changed when formatting the disk. Table 2.0 shows the default cluster sizes for different disk sizes on NTFS formatted disks:

Table 1: Default Cluster Size on NTFS formatted disks

Volume Size	Default Cluster Size
512 MB or less	512 bytes
513 MB – 1,024 MB	1 KB
1,025 MB – 2,048 MB	2 KB
Greater than 2,048 MB	4 KB

On NTFS formatted disk all clusters have a Logical **Cluster Number (LCN)**. LCNs are the sequential order of the clusters from the beginning of the volume to the end. LCN 0 (zero) refers to the first cluster in the volume (the boot sector). NTFS converts the LCN to a physical disk address (byte offset of the volume where the cluster resides) by multiplying the LCN with the cluster size (Russinovich, 2003).

Clusters belonging to the same file are also given a **Virtual Cluster Number (VCN)**. VCNs are the internal order of the clusters in a file and do not need to be physically contiguous on the disk.

2.3 NTFS AND FORENSIC INVESTIGATORS

During an examination of a computer system the computer forensic investigator tries to find evidence that can answer the following questions: who, what, when, how, where and why? But is it possible to answer these questions, and what degree of forensic value and what forensic quality can be obtained?

NTFS, like most other file systems, was not designed with computer forensic in mind but there is a lot of information on the computer that could be used in an investigation.

It is possible to find evidence of computer usage because a lot of the actions taken by the user leave traces on the computer. Creating, deleting, renaming, modifying and accessing files will all cause changes to metadata files in the MFT. Executing programs will leave the same kind of traces, since a program is treated as a file like everything else. Printing documents will also leave traces, since the document is cached before it is printed. Examining files may therefore give an understanding of what programs were executed, what files were accessed and modified and so on.

2.3.1 THE IMPORTANCE OF METADATA FILES IN COMPUTER FORENSICS

Metadata contain a lot of information about files and are therefore a useful source of evidence in a computer forensics investigation. Examining metadata files may give evidence of user activities, the computer's current and previous configuration and so on.

Often when a suspect becomes aware that he/she is under investigation, he/she might try to eliminate all traces by deleting files that could be used as evidence. Locating and recovering metadata files might be enough to track user activities even if recovering of the actual data files is unsuccessful.

2.3.2 FILE RECOVERY

MFT file records belonging to deleted files may be possible to harvest, because file records are not permanently deleted and will remain on disk until they are overwritten by new file records [5]. The chance to successfully recover deleted (marked for deletion) file records decreases with time, since NTFS overwrites deleted file records before allocating additional space for the MFT. The file

ISSN 2304-0777 www.jitbm.com

records contains the standard information MAC times amongst other things) and the file name. Such information could be very useful in an investigation. If the file record is recovered the data-runs for the file's non-resident data will also be known and could easily be recovered. Without the file record a physical search of the disk could still locate and recover the deleted file, suppose it is not fragmented. Fragmented files are very hard to recover completely through a physical search but even if only parts of the file are recovered it may include important evidence.

As explained above the possibility of recovering metadata files decreases with time since it is likely that they have been overwritten [5]. Metadata belonging to recently deleted files however may successfully be recovered (as when a criminal delete files in panic when the police are knocking on the door).

2.4 LOCATION OF DIGITAL EVIDENCE

There is often a tendency to argue how to recover deleted files and how to interpret file fragment when discussing evidence acquisition. But there is a lot of information that does not only exist in unallocated space or slack space and is therefore easily recovered [10]. Such files are for example files located in the Recycle bin, Shortcut files and so on. These files are rich sources of evidence and should be examined thoroughly.

2.4.1 RECYCLE BIN

Usually when a file is deleted on a windows computer, the file is moved to the Recycle Bin. That means that it is possible for a user to retrieve a file that has been deleted by mistake, supposed the Recycle Bin has not been emptied [5]. The user may however turned the Recycle Bin feature off or holding down the SHIFT key while pressing the DEL key, and in those cases the files will not be sent to the Recycle Bin. The file will still exist on the computer though and can be recovered. The Recycle Bin is found in the hidden system folder RECYCLER on NTFS computers [9].

On file deletion a copy of the file is moved to the Recycle Bin and the file is renamed to DC<index>.<extension>. The first file moved to the Recycle Bin gets the index number '1' and the second number '2'and so on. After the Recycle Bin has been emptied and the system rebooted the index numbering starts over.

Files found in the Recycle Bin have been deleted by the user and not by the system, because files deleted by the operating system are not moved to the Recycle Bin. When the recycled bin is emptied the INFO2 records are deleted, but it might be possible to recover them. The copies of the files are also deleted from the Recycle Bin folder, but with the INFO2 records, they might be recovered.

2.4.2 INTERNET ACTIVITY (INDEX.DAT FILES)

Internet is wide client-server network and when a URL is typed in the browser the client asks the server for the page. To allow for quicker access to sites already visited; internet explorer caches the content of the visited web page including the time of visit, the address, images, cookies etc. when revisiting a site internet explorer checks the web site server for changes to the page [6]. If there are any changes to the page, the new version is retrieved. If not the caches page is used. Web pages can therefore be opened from the local hard disk instead of downloading the page again. Websites often place small text on a user's computers to save information about web sessions, these files are called cookies.

2.4.3 INDEX.DAT (HISTORY FOLDERS)

Index.dat files in the history folders are used by Internet Explorer's auto complete function. An overview of the Internet history can be displayed in Internet Explorer (CTRL + H). In the history.IE5 folder there is one index.dat file and several subfolders. These subfolders are named using date(s) of the Internet activity it contains.

2.4.4 INDEX.DAT (COOKIES)

The index.dat file includes URL from where the cookies were received, the date and time, and the name of the cache cookie file. The cookie files are stored within the same folder [10].

2.4.5 SHORTCUT FILES (.LINK)

Shortcut files (or link files) point to a target file or application. Short cuts are used to quickly access or execute a file or a program, without having to locate the target on the system. Shortcuts are also used to access folders or devices such as printers and

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

scanners, and they can therefore tell a lot of the computer's current and previous configuration, file accesses, devices etc [5]. Shortcuts are often found on the Windows Desktop or in the Windows start Menu, but there are several other locations that hold shortcut files.

2.4.6 THUMBNAILS FILES (THUMBS.DB)

Windows creates thumbnails for graphic image files (JPG, GIF, PNG and BMP) which are used when listing files as miniatures in Windows Explorer. Thumbs.db may contain thumbnails for graphic images that have been deleted [5]. Other information that can be found in thumbs.db files is the original filename and last modified datel10]. On Windows 2000, the full path of the original image file can also be retrieved. On Windows XP the full path cannot be found, only the file name of the original image file can be collected.

2.4.7 REGISTRY ENTRIES

The registry on Windows computers are rich source of evidence, and it contains information about settings for installed hardware and software. It also contains the user specific settings and preferences on the computer, thus changes made on the computer, for example in the control panel or to installed software, is reflected in the registry entries [11].

2.4.8 PRINTER SPOOLER FILES

Printing jobs are done in the background and make use of temporary files created by the spooling process. The content of the printing job is writing to a spool (.spl) file and information such as username, document name, and data type (RAW or EMF) is written to a shadow (.shd) file. The data type found in the shadow file determines if the spool file is a RAW or Enhanced Metafile (EMF) file. EMFs are used by the default Windows NT print spooler, and EMF files are encoded to provide printer independence. If the spool file is in RAW format the spooled data is formatted for a particular printer, thus RAW spool files are device-dependent [5].

The .spl and .shd files have the same file name, usually a number such as 00002.SPL and 00002.SHD. By default, both files are written to the following location:

C:\WINDOWS\SYSTEM32\SPOOL\PRINTERS

When the printing job is done both files are deleted automatically, but as with all files that have been stored on a hard disk it might be possible to recover the files from unallocated space.

3. METHODOLOGY

3.1 CONCEPT OF NTFS UNDELETE

The methodology used in this design is the Structured System Analysis and Design Methodology (SSADM). SSADM uses a combination of text and diagrams throughout the whole life cycle of a system design, from the initial design idea to the actual physical design of the application. Five steps of SSADM were applied in the development of this application: Feasibility Study, Requirements Analysis, Requirements Specification, Logical System Specification and Physical Design.

Data Flow Modeling and (high-level) Logical Data Modeling are the techniques applied during development of this tool.

3.1.1 NTFS RECOVERY TOOL DESIGN

A class diagram is used to describe the types of objects in the system and the various kinds of static relationships that exist among them. It is a graphical representation of a static view on declarative static elements and a central modeling technique that runs through nearly all object-oriented methods. This tool is made up of two classes. These classes are very useful to read the NTFS files. The function of each class is explained as follows:

CMFTRecord class: This is the lowest class which does the file reading and attributes extraction.

CNTFSDrive class: This class loads the MFT table and manipulates the file according to the user request.

See the following class diagram for more detail on each of these classes.

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

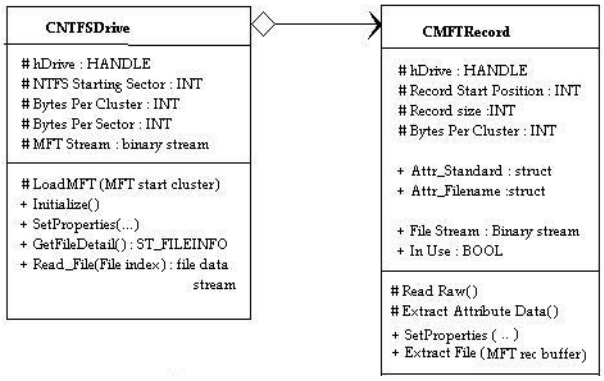

Fig. 1: NTFSUndelete Class Diagram

A sequence diagram is also used primarily to show the interactions between objects in the sequential order that those interactions occur. In addition to their use in designing new systems, sequence diagrams can be used to document how objects in an existing (call it "legacy") system currently interact.

Figure 2 depicts how **CNTFSDrive** handles the **CMFTRecord** class for file extraction.

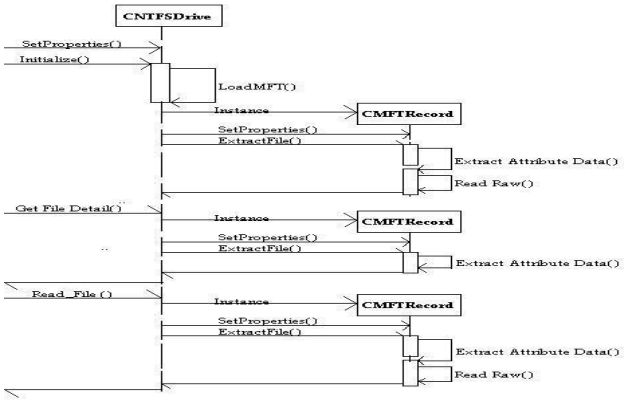

Fig. 2: NTFSUndelete Sequence Diagram

4. RESULTS

The NTFSUNDELETE application software was successfully used in recovering deleted files on NTFS file system as shown in figure 3.

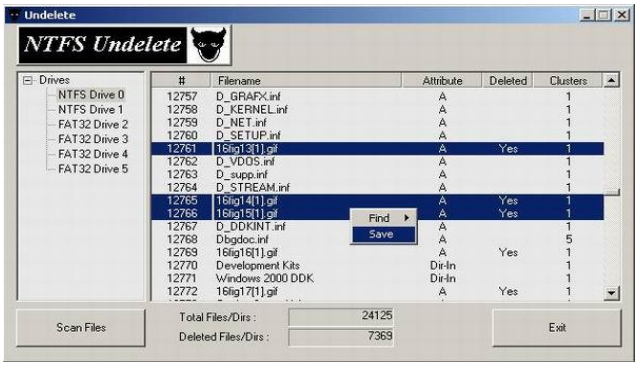

Fig. 3: NTFSUndelete Sample Output

The paper focuses on how to apply forensic science on NTFS computers, but in order to put the subject in a bigger context the forensic process and location of evidence on NTFS had to be covered. The application of forensic science to NTFS computers was discussed. Various sources of evidence were covered such as index.dat files, cookie files, print spooler files, thumbs.db files, registry files, INFO2 file etc. These and other sources of evidence outside the computer should be examined such as DNA, finger prints, notes on paper, etc.

5. CONCLUSION

Searching several sources of evidence increase the possibility for the investigator to draw unambiguous conclusions about what has happened. All evidence collected is to be used in the relational, temporal and functional reconstruction of the crime. Analyzing and combining evidence collected from the various sources help the investigator to reconstruct the crime and draw unambiguous conclusions.

One of the major concerns in an investigation is to link the evidence to a physical person. It could be hard to prove that the suspect is connected with the evidence found on the computer. This is the biggest challenge for the investigator, since anyone could have used the computer especially if password protected accounts have not been used. Physical evidence may tie a suspect to the computer, for example it may be possible to prove that a specific person has used the computer if fingerprints are found on the computer keyboard. Knowing that the suspect has used the computer makes it easier to draw further conclusions. This is one of the reasons why securing evidence outside the computer is important.

International Journal of Information Technology and Business Management
29th July 2014. Vol.27 No.1

ISSN 2304-0777 www.jitbm.com

File recovery pervades much of the forensic work during a computer forensic investigation, whether it is to recover the actual deleted files (word documents, graphics image files etc.), temporary files (printer spool files) or files containing metadata (index.dat, thumbs.db, INFO2). File recovery is important in an examination of a computer, since a lot of the information may be deleted. Deleting file on NTFS computers does not mean that the file is permanently deleted. The file is often recoverable from unallocated space or slack space. Even if the data has been overwritten and the file is not successfully recovered there may still be a lot of traces left on the computer that can give evidence of the files existence. The chance of successfully recovering files decreases with time, because the clusters in unallocated space may be overwritten. NTFS also overwrites MFT records relatively quickly, making file recovery harder.

Software tools are part of the solution in an investigation and the tools should be tested to verify that they behave in a certain manner. It is always important to understand how a tool handles different tasks and this is even more important if the tool is new and has not been thoroughly scrutinized by independent bodies. Other tools that are less used and developed for a specific task may also be used but the investigator should be prepared to answer questions in court related to the tool and its inner workings. The decision on which tool to use should depend on the purpose of the investigation. The investigator's knowledge and skill with various tools could also be of importance.

No matter how skilled an investigator is with a tool it is important that he is familiar with the file system running on the computer. Understanding how the file system works will help the investigator to interpret the data found.

There is also another side of computer forensics where tools developed for the purpose of computer forensic examinations may be used with a malicious intent. Such tools may be used to steal sensitive information or keep an eye on someone. Using a forensic tool makes it possible to bypass security measures like password protected accounts, but there are several ways to protect the computer and the information stored on it. Some examples of security measures that could be used is the password protection of BIOS, enable the ATA-password and use of EFS.

Given the enormity of task in cyber crime control and policing, the absence of dearth of trained and qualified computer forensics law enforcement officers, there is urgent need for the Federal Government to pay attention to the training of adequate EFCC and police officers in the computer forensic sciences to enhance effective policing of the ever increasing cyber criminals. The problem is serious, particularly now that the Federal Government has passed the information Technology Bill for this purpose. A law made but cannot be enforced is no law. Cyber criminals will be forced to retreat if a large percentage of fraudsters are arrested, prosecuted and punished at first attempt. It is strongly recommended that Polytechnics and Universities should establish Computer Forensics certificate, diploma and degree courses to meet the ever-increasing demand for this type of urgently needed personnel. The provision of adequately qualified experts will beef up their deployment in the police and military. This may well be antidote to the fast eroding confidence in e-commerce and international trade in Nigeria.

In conclusion, this paper should give the reader the knowledge and skill needed to begin analyzing Microsoft Windows computers and to assist forensic teams during computer forensic investigation. The file recovery tool could be used to recover accidentally deleted files under NTFS file systems on Microsoft Windows computers. This software is license free.

6. FUTURE WORK

This paper covers Windows NTFS file system, but computers may use other file systems. Windows computers may, for example use FAT and or NTFS file systems while Linux computers use EXT2 or EXT3 file systems. A computer may also have several operating systems and different file systems on one physical hard disk. Future studies could be done on file systems not covered by this paper and should at least cover the most widely used file systems on computers today.

Computer forensic tools can help find hidden data in unallocated space or in hidden partitions, but as far as I know, there is no tool that looks for data in clusters marked as bad by NTFS. It is possible to manually

ISSN 2304-0777 www.jitbm.com

mark and unmark bad clusters and therefore logically it could be possible to hide information in such data areas. Future studies should be made on this topic.

A research could also be carried out on a single tool that operates on different operating system; multiplatform computer forensic tool.

Reference:

[1] Albert J. Marcella, Jr. and Dough Menendez (2008). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, (2nd Edition): Taylor & Francis Group, LLC.

[2] Buchholz, Florian and Spafford, Eugene**. On the Role of file system metadata in digital forensics:** Digital Investigation Volume 1, Issue 4, Pages 18-23 (December, 2004)

[3] Carrier, Brian (2003). **Defining Forensic Examination and Analysis Tools Using Abstraction Layers:** International Journal of Digital Evidence Winter 2003, Volume 1 Issue 4

[4] Casey, Eoghan (2000). **Digital Evidence and Computer Crime:** Academic Press; 1st edition (March 15, 2000)

[5] Casey, Eoghan (2001). **Handbook of Computer Crime Investigation:** Academic Press; 1st edition (October 15, 2001)

[6] Jones Keith J., (2002) **Forensic Analysis of Internet Explorer Activity Files Http://www.foundstone.com/pdf/wp_index_dat.pdf** (Retrieved on July 5, 2009)

[7] NIJ, (2001) National Institute of Justice. **Electronic Crime Scene Investigation: A Guide for First Responder:.** Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2004. NCJ 187736. http://www.ojp.usdoj.gov/nij

[8] Russinovich, Mark(2003). **Inside NTFS:** http://www.windowsitpro.com/Articles/Index.cfm?IssueID=27&ArticleID=3455 (Retrieved on August 5, 2009)

[9] Solomon, David A. and Russinovich, Mark E (2000). **Inside Microsoft® Windows® 2000, Third Edition:** Microsoft Press, Redmond, Washington.

[10] Svensson, Anders (2005). **Computer Forensics Applied to Windows NTFS Computers:** Stockholm's University Kista, Stockholm, Sweden**.**

[11] WinGuides,(2006). **Windows Registry Tutorial** http://www.winguides.com/article.php?id=1&guide=registry (Retrieved on August 22, 2010)