Enhancement of Existing Tools and Techniques for Computer Forensic Investigation

Gouthami Velakanti[#], Aditya Katuri[*]

[#]Computer Science and Engineering,Aurora's Research and Technological Institute
Warangal,A.P,India.
[*] Aurora's Research and Technological Institute
Warangal,A.P,India.

Abstract: **Data retrieval is the most important part of computer Forensic investigation. Any data written on the hard disk can be retrieved by the investigators. For that the investigators use many tools to search the files, retrieve the files which are deleted, encrypted, hidden. There are many techniques used to hide. So, how these type of data is recovered? The file which is deleted by the person using 'delete' or from recycle bin are never lost permanently. The address of deleted file is marked as free space to be allocated for new file. The main area from which data can be retrieved is file slack. In this we discuss different tools and techniques of searching and retrieving the data and enhancements to the existing tools for better performance.**

Keywords **: File slack, livesearch, Index search, tools.**

I.Introduction

Definition: Computer Forensics[6][7] is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. Computer forensics[2], also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer evidence [8] can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

Roles of a Computer in a Crime

A computer can play one of three roles in a computer crime. A computer can be

1.target of the crime - it can be the instrument of the crime.

2.evidence repository- Storing valuable information about the crime.

3.Instrument of the crime- It can also serve as a file cabinet storing critical evidence.

For example, a hacker may use the computer as the tool to break into another computer and steal files, then store them on the computer. When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role. Applying information about how the computer was used in the crime also helps when searching the system for evidence. If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and password files. If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked. Knowing how the computer was used will help narrow down the evidence collection process.

The Computer Forensic Objective

The objective in computer forensics is quite straightforward. It is to recover, analyze, and present computer-based material in such a way that it is useable as evidence in a court of law[4]. The key phrase here is *useable as evidence in a court of law*.

II.Overview

When a file is deleted many forensic tools are used to retrieve the data.The computer forensic investigator uses the tools for this purpose but does not have idea of where the data is stored or what happens internally with the Operating system when a file is deleted or created.Here we discuss three potential locations for this information**.**

III. Present System

Most users aren't very good at covering their tracks. This is because lack of knowledge of how computers manage memory and disks results in incriminating file or memory content stored in various locations invisible to the subject of an investigation[3].

There are three potential locations for this information –

1.Deleted files and slack space

2.Swap space,

3.Hibernation files.

*Deleted files and slack spac*e When an operating system writes a file to the disk, it allocates a certain number of sectors. The number of sectors allocated depends on the limitations of the operating system and configuration decisions made by the system administrator. The sectors allocated and their location on the disk are recorded in a directory table for later access. When the file is deleted, the space which is originally allocated to it is simply marked as unallocated and the actual data remains on the disk. But what happens if a new file is written to this same space? Figure 1 shows slack space .

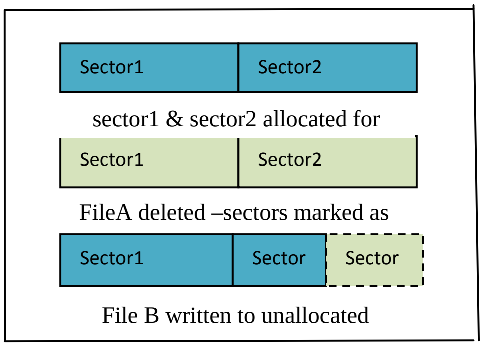

Sector1
Sector2
sector1 & sector2 allocated for
Sector1
Sector2
FileA deleted –sectors marked as
Sector1
Sector
Sector
File B written to unallocated

Figure 1.slack space

At some point in the past, File A was written to sectors 1 and 2. The sectors were completely filled by the file's content. When the user decides to delete the file, the sectors are marked as unallocated. However, the file content remains.Sometime after File A is deleted, the user requests the OS to save File B. The OS once again allocates sectors 1 and 2, but the file content doesn't completely fill sector 2. The unwritten portion of sector 2 is known as ***slack space,*** and it still contains content from File A. Slack space data can be read and analyzed by any of the popular forensics toolkits.

Swap space

The Operating System moves data in memory to a special location on disk in order to free RAM for additional operations. When the data on disk is needed again, it is moved back into RAM. The area on disk used for this purpose is called the ***swap file*** or ***swap space***. In Linux environments, the swap area is an actual disk partition. On a Windows XP machine, the swap space is a file called Pagefile.sys.Since everything in RAM is subject to being swapped to disk, some very interesting information can be found in a swap file. In addition to plain-text data that might be encrypted in a disk file, encryption keys might also be present. This is due to weaknesses in some applications that allow unencrypted keys to reside in memory. Further, information contained in e-mails or stored at remote locations might still reside in swap space. Any standard disk maintenance utility can access this information.

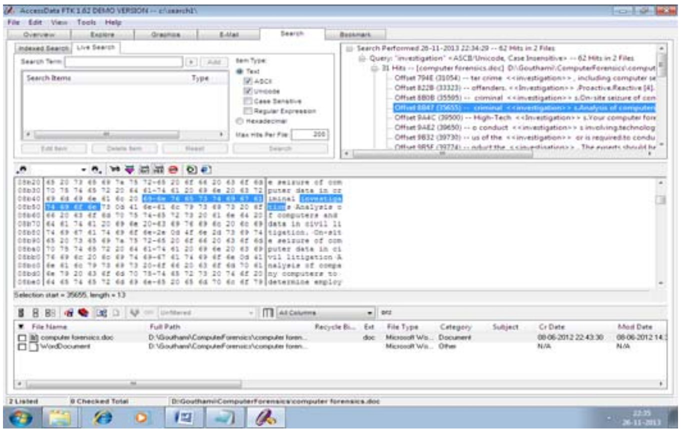
Hibernation files

Hibernation files are created when a system goes into sleep or hibernation mode. For example, a laptop running Windows XP writes the entire contents of RAM to a file when going into hibernation. Like swap space, hibernation files can contain a wealth of information not found anywhere else on the target system. The contents of a hibernation file can be accessed by a number of disk maintenance utilities.A target disk is usually full of useful information. An investigator just needs to know where to look and how to employ the proper tools and techniques[1] for extracting it.

IV COMPUTER FORENSIC TOOLS USED TO SEARCH DATA

FTK TOOL

FTK[7] can analyze data from several sources, including image files from other vendors.FTK also produces a case log file, where you can maintain a detailed log of all activities during the examination such as keyword searches and data extractions.FTK provides two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly.The other option is live search,which can locate items such as text hidden in unallocated space that might not turn up in an indexed search. Figure 2.1 shows how search is performed in FTK .



● Text
☑ ASCII
☑ Unicode
□ Case Sensitive
□ Regular Expression
○ Hexadecimal
Max Hits Per File: 200

Search Performed 26-11-2013 22:34:29 -- 62 Hits in 2 Files
Query: "investigation" <ASCII/Unicode, Case Insensitive> -- 62 Hits in 2 Files
31 Hits -- [computer forensics.doc] D:\Gouthami\ComputerForensics\comput
Offset 794E (31054) -- ter crime <<investigation>> , including computer se
Offset 822B (33323) -- offenders. <<Investigation>> .Proactive.Reactive [4].
Offset 880B (35595) -- criminal <<investigation>> s.On-site seizure of com
Offset 8847 (35655) -- criminal <<investigation>> s.Analysis of computers
Offset 9A4C (39500) -- High-Tech <<Investigation>> s.Your computer fore
Offset 9A62 (39650) -- o conduct <<investigation>> s involving technolog
Offset 9B32 (39730) -- us of the <<investigation>> or is required to condu
Offset 9B5F (39774) -- educt the <<investigation>> . The experts should he

```
e seizure of com
puter data in cr
iminal investiga
tions Analysis o
f computers and
data in civil li
tigation. On-sit
e seizure of com
puter data in ci
vil litigation A
nalysis of compa
ny computers to
determine employ
```

Selection start = 35655, length = 13

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
computer forensics.doc	D:\Gouthami\ComputerForensics\computer foren...		doc	Microsoft Wo...	Document		08-06-2012 22:43:30	08-06-2012 14:1
WordDocument	D:\Gouthami\ComputerForensics\computer foren...			Microsoft Wo...	Other		N/A	N/A

D:\Gouthami\ComputerForensics\computer forensics.doc

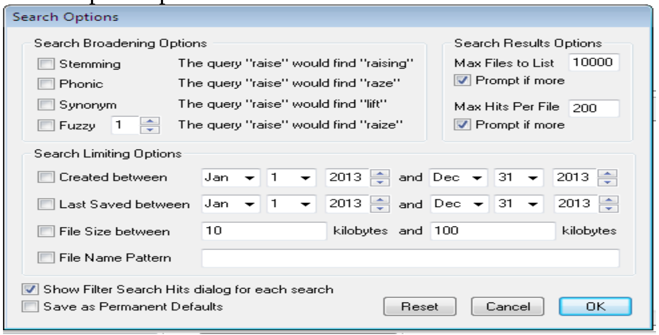
22:35
26-11-2013

Figure 2.1 Result of search option

Figure 2.1 shows the search result of word “investigation” in an individual file. In addition to indexed and live Searches FTK has several advanced searching techniques, such as

- **Stemming**:which enables to look for words with extensions such as “ing”, ”ed” and so on.
- **Phonic**:search for similar sounding word such as “raise”, ”raze”.
- **Synonym**:search for similar word such as “raise”, ”lift”.
- **Fuzzy**:search forwords like “raise”,”raize”.

In FTK search can also be limited.Figure 2.2 shows the search options present in FTK.



Search Broadening Options

□ Stemming The query "raise" would find "raising"
□ Phonic The query "raise" would find "raze"
□ Synonym The query "raise" would find "lift"
□ Fuzzy 1 The query "raise" would find "raize"

Search Results Options

Max Files to List 10000
☑ Prompt if more
Max Hits Per File 200
☑ Prompt if more

Search Limiting Options

□ Created between Jan 1 2013 and Dec 31 2013
□ Last Saved between Jan 1 2013 and Dec 31 2013
□ File Size between 10 kilobytes and 100 kilobytes
□ File Name Pattern

☑ Show Filter Search Hits dialog for each search
□ Save as Permanent Defaults

Figure 2.2 search options in FTK

V. Computer Forensic Tools Used To Retrieve Data

ProDiscover Basic

ProDiscover Basic[7] from Technology pathways is a forensics data analysis tool.It can be used to acquire and analyze data from several differentnfile systems such as Microsoft FAT and NTFS ,Linux Ext2 and Ext3 and other UNIX file system. Figure3.1 ,Figure 3.2 ,Figure 3.3 shows how ProDiscover Tool is used to retrieve deleted data from a pendrive. Initially the complete data in the pendrive is deleted,and we try to recover the deleted data.Figure 3.1 shows the pendrive is empty.

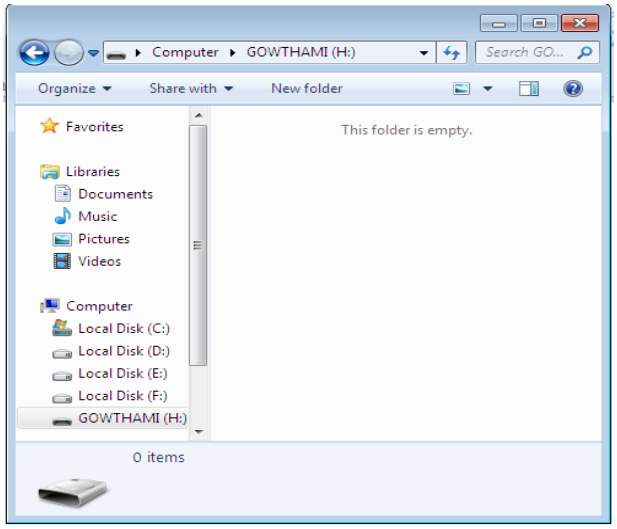


Figure 3.1 Pendrive is empty.

Now we need to perform data acquisition[5][9] of the pendrive.Figure 3.2 shows data acquisition .

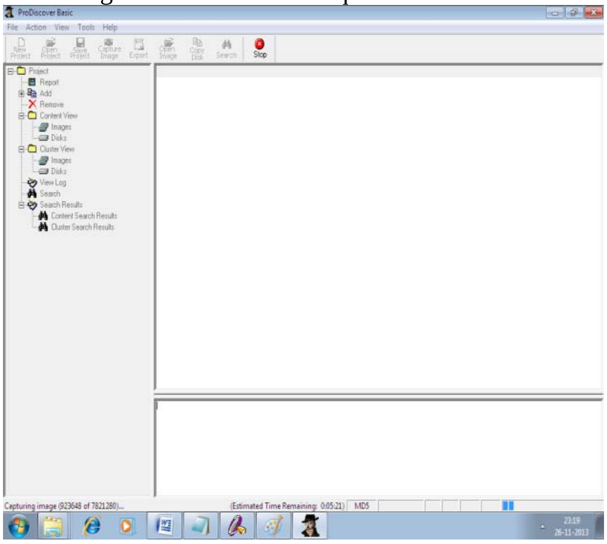
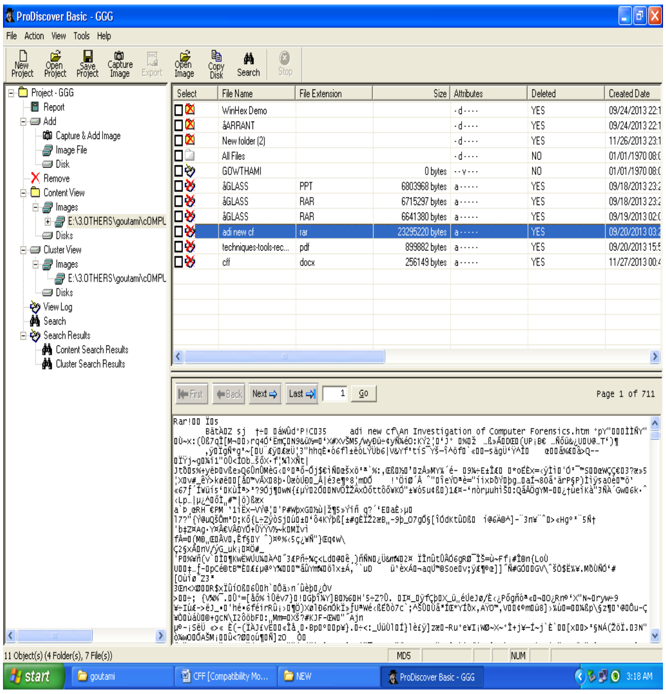


Figure 3.3 ProDiscover tool capturing Image of Pendrive

After capturing image of the pen drive the deleted data is recovered from pendrive which is shown in Figure 3.4



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date
□	WinHex Demo			-d----	YES	09/24/2013 22:1
□	åARRANT			-d----	YES	09/24/2013 22:1
□	New folder (2)			-d----	YES	11/26/2013 23:1
□	All Files			-d----	NO	01/01/1970 08:0
□	GOWTHAMI		0 bytes	--v---	NO	01/01/1970 08:0
□	åGLASS	PPT	6803968 bytes	a-----	YES	09/18/2013 23:2
□	åGLASS	RAR	6715297 bytes	a-----	YES	09/18/2013 23:2
□	åGLASS	RAR	6641380 bytes	a-----	YES	09/19/2013 02:0
□	adi new cf	rar	23295220 bytes	a-----	YES	09/20/2013 03:2
□	techniques-tools-rec...	pdf	899882 bytes	a-----	YES	09/20/2013 15:5
□	cff	docx	256149 bytes	a-----	YES	11/27/2013 00:4

Figure 3.4 Results of data retrieval

VI.Proposed System

The grep program allows files to be searched for a particular sequence of characters: the word "place" or the phrase "the meeting is " for example. The real power of grep, however, lies in its ability to utilize metacharacters. Metacharacters are certain characters which have a special meaning to the grep program and provides great flexibility while searching in the process of finding evidence. For example the metacharacter "." (i.e. a full stop, without the quotation marks) means "any character" to grep, thus searching for "fa." might result in matches for "fan", "fat", "cab" and so on if these sequences of characters were present in the file being searched.

Grep has for a long time been one of the most useful tools for forensic investigators and as well as being a standard program on UNIX systems is also included as part of Encase. As we discussed the features of FTK which provides different search options, but still if we include 'grep' as part of FTK search option will be more flexible with more options. And if this complete search options along with ProDiscover tool data recovery techniques a new tool can be developed where search and data recovery can be done using a single tool which will be more flexible for investigators.

VII. Conclusion

The field of computer Forensics is highly dependent on Tools with more features. A computer forensic tool should be useful for multipurpose. Such kind of tools should be developed. In the paper we want to enhance the feature the FTK tool features by incorporating Grep program. And a new tool can be developed where search and data recovery can be done with a single tool.

REFERENCES

[1].Bhanu Prakash Battula, B Kezia Rani, R SatyaPrasad & T Sudha”Techniques in Computer Forensics: A Recovery Perspective” International Journal of Security (IJS), olume (3) : Issue (2).

[2] Nathan Balon ,Ronald Stovall ,Thomas Scaria ”Computer Intrusion Forensics Research Paper” CIS 544.

[3]. Sonia Bui,Michelle Enyeart,Jenghuei Luong, COEN 150,Dr. Holliday,” Issues in Computer Forensics“,May 22, 2003.

[4]. Mark Reith, Clint Carr, Gregg Gunsch,” An Examination of Digital Forensic Models”, International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3.

[5]. SWGDE Best Practices for Computer Forensics Version 2.1 (July 2006).

[6].”computer-forensics-computer-crime-scene-investigation-networking-series.”,John R.Vacca

[7].” Computer Forensics and Investigations”Bill Nelson, Amelia Phillips , Frank Enfinger , Chris Steuart

[8].Information security and Forensics Society(ISFS) found at http://www.isfs.org.hk.

[9].NIST CFTT. Disk Imaging Tool Specification, 3.16 edition, Oct 2001.

AUTHORS

V.Gouthami,completed M.Tech in Software Engineering,presently Working as Associate Professor in the department Of CSE in Aurora’sResearch and &Technological Institute.Her area of intrest is Computer Forensics,Network Security, DataStructures and Web Technologies.

.

Aditya.K Pursuing B.Tech in CSE final year From Aurora’s Research and Technological Institute.