Analysis Of Data On StorageDeviceUsing Forensic Tools

Vikas

PG Scholar, Dept. of ISE, BMSCE, Bangalore,

Email:vikas.bmsce@gmail.com

***Abstract*: Data retrieval is the most important part of computer forensic, i.e. for retrieval of deleted data ,lost data, hidden data, any of these type of data from flash memory or hard drive is important for investigator for producing proof in court of law, the hidden data or deleted data will never be lost permanently and even the lost data due to quick format or system crash will be there, then to recover this data by using tools and up to what level the tools are efficient in recovering of various types data, so the focus of this paper is analysis of data using various computer forensic tools, to know the differences and similarities between tools and important thing is what extra features to be added to make enhancement of the tool for efficient recovery of data from storage device.**

***Keywords*:**

Computer Forensic, Forensic Tools, USB Sticks, Storage Device, Data Recovery, Computer Forensic Investigator.

1.INTRODUCTION

Definition: computer forensic is the discipline investigative techniques in the automated environment search, discovery, recovery, and analysis of evidence.it is the method of investigation and analysis of data maintained on and retrieved from storage device for the purpose of presentation in the court of law, civil or administrative proceedings, computer forensic involves the acquisition,identification, evaluation,documentation and interpretation of computer media for evidentiaryand/or root cause analysis. Computer forensic is necessary and used by criminal prosecutors, law enforcement officials, insurance companies, private corporations,individual/private citizens etc.

As we know internet is network of networks and every common man using internet it may be for banking, business application, online ticket reservations, communication, for information exchange across the world, due to this life of common man is depend on internet in one or other way, and this open the networks and individual machines to hosts of awide variety of threats and attacks by cyber criminals.

Cyber-crime is any activity in which computers or networks are tool, such as network intrusions and the dissemination of computer viruses as well as computer based variations of existing crimes, such as identifying theft, stalking, bullying ,terrorism, it may be theft of intellectual property , fraud.Cyber obscenity is one of the more known methods of cyber-crime. I.e.Pornographic material,such as child pornography, which generally includes the sexual images hidden on storage media.

So the Cyber-criminals are associated with one or more crimes, and these Cyber-criminals make the crime by sitting in any part of the world and to escape from the crimes are made by them the evidences may deleted ,hidden , formatted or taken into CDs, hard drive or removable, UBS Sticks or any other electronic storage media to collect and store on them, and for forensic investigator this becomes the difficult task to collect the digital resources used by them in crime and to recover and produce the summary report in front of court of law. For that the forensic investigator has to use the forensic tool for collecting evidences.

2. TERMS OF COMPUTER FORENSIC

2.1DISK IMAGING:”an image of the whole disk was copied regardless of any software on the disk and the important point was that the complete content of the disk was copied including the location of the data. Disk imaging takes sector by sector copy usually for forensic purposes and as such it will contain some

mechanism (internal verification) to prove that copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image" by Jim Bates

2.2DATA RECOVERY**:**restoration in full or part of the data stored in deleted or damaged data files. in case of file deletion, if the space originally occupied but deleted files is not overwritten the file may be recoverable through common 'undeleted' programs. in case of damaged files custom-written software and sophisticated equipment is required for any extent of recovery**.**

2.3DATA DISCOVERY:discovery of the files on a particular subjected system which includes existing normal files, deleted yet remaining files, hidden files, password-protected files and encrypted files

3.ANALYSIS OF DATA USING FORENSIC TOOLS

In this paper we have used the four types of forensic tools for data analysis, those are pro-discover basic, pc inspector file recovery, encase imager, FTK imager**.**

3.1PRO-DISCOVER BASIC:

pro discover basic from technology path ways is data analysis forensic tool that enables computer professionals to find all the data on a computer disk , and system such as Microsoft FAT and NTFS while protecting evidences and creating evidentiary quality reports for use in legal proceedings, it is not possible to hide data from pro discover forensic as it reads the disk at the sector level.it will alter any data on the disk-period ,it is able to recover the deleted , hidden files, pro discover can even dynamically allow you to preview, search and image the hard ware protected area of the disk utilizing a patent pending process pro discover forensics powerful search capability is fast and flexible.pro discover automatically creates evidentiary quality reports needed to document your results, complete with every file and hash signatures where evidence was found, this saves time and prevents error which might compromise your case.

Initially we have taken a pen drive and we have hidden some images and files and some files we deleted

Fig1.1 shows that the pro discover recovered the deleted files and hidden files from the pen drive**.**

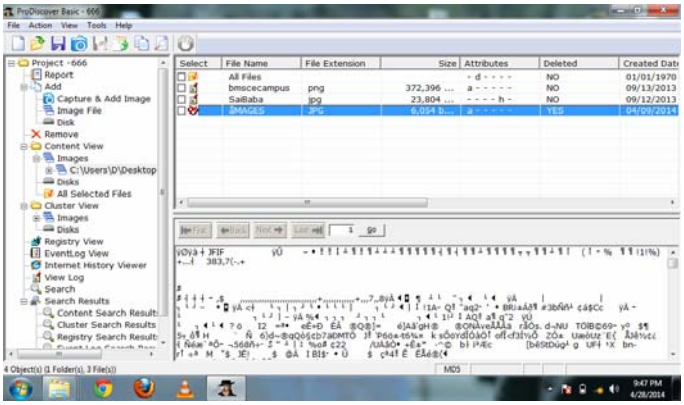
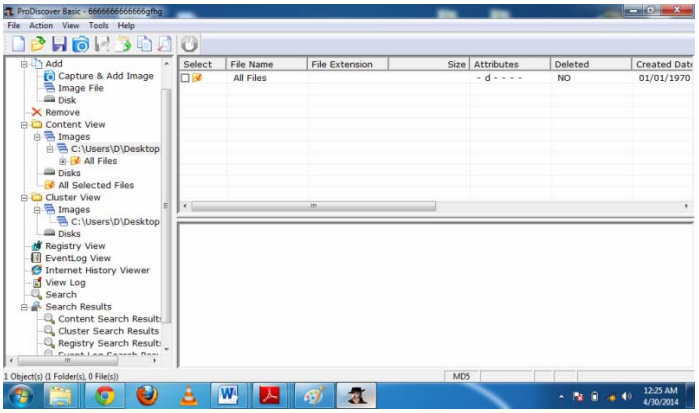


Fig1.2 shows that the pro discover cannot be able to recover lost data



3.2PC INSPECTOR FILE RECOVERY:

Pc inspector file recovery is a free available Computer forensic tool used for to recovering the deleted data and lost data, this tool is very effective at detecting the files very fast, The lost data can be recovered by the tool by performing sector by sector scan,but it cannot be able to recover the hidden data, all unreferenced files are associated with conditions, this condition can be either good or poor ,if the file condition is good then the probability of file recovery is better, it can also be used to find the lost drive.

Fig2.1 shows that the pc inspector files recovery can be able to recover the deleted

da**ta**

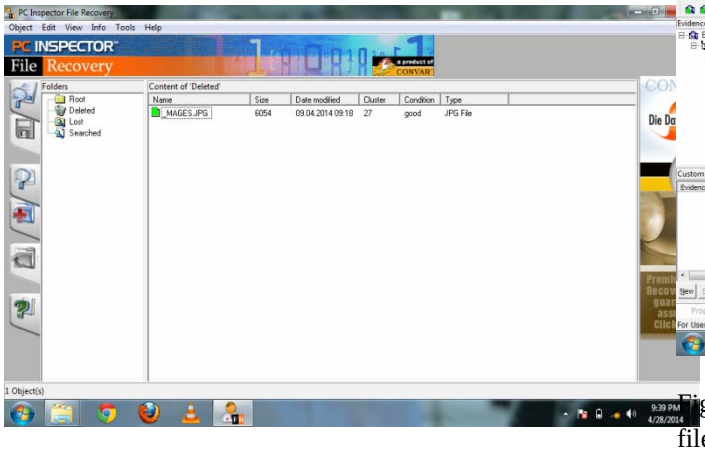
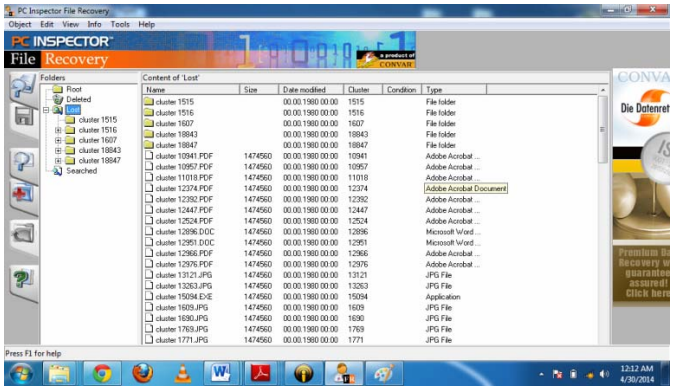


Fig2.2 pc inspector file recover can be able to recover the lost data.



3.3FTK IMAGER:

Forensic tool kit imager is a commercial forensic tool developed by Access Data.it scans hard drive or storage device looking for information. this can be able to recover the deleted files and hidden files but cannot be able to recover the lost data,Access Data FTK imager takes data base approach when analyzing the data located on the storage device, this tool can be able to generate either MD5 or SHA hash values for all visible and accessible files,the MD5 hash values are generated and presented to the investigator as part of completed process notification to guarantee the integrity of the original files.

Fig3.1 shows the data recovery of deleted and hidden files done by the FTK imager

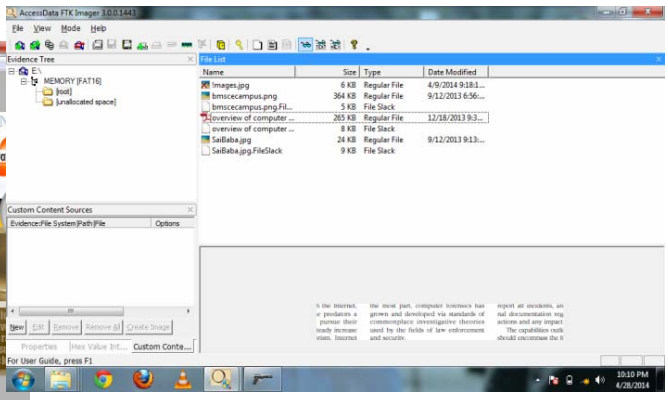
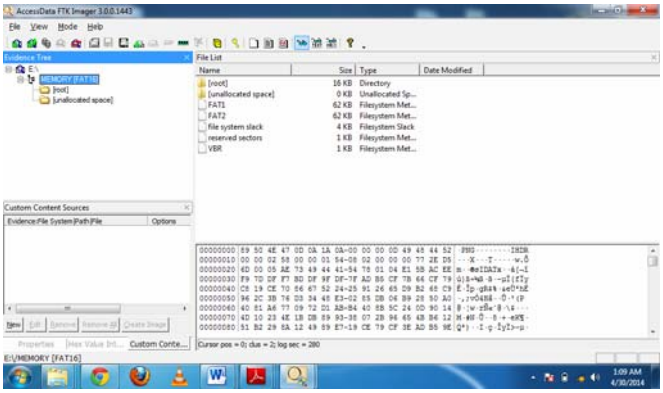


Fig3.2 shows that the FTK imager cannotrecover lost files



3.4ENCASE IMAGER:

Encase Imager is developed by Guidance software this the efficient forensic tool used for discovery of deleted data, hidden data , but it cannot be able to discover the lost data due to quick format or system crash, encase gives the important capabilities that ensures you will never miss an important comment, bookmark, or other piece of important information when producing and sharing report, with the reporting capabilitiesit exports information into various file formats as needed for reporting and analysis.

An forensic investigator using the encase would typically begin investigation by seizing and imaging the storage device to be investigated, encase consider the resulting image as the evidence file, The evidence file is the image of storage device. this encase software then checks the integrity of the image file

and original storage device the hash function such as the MD5 hash function, so as that investigation to proceed , the imaged file is mounted by the tool to eliminate the need to restore the seized storage device.

Encase imager also Includes relevant evidences, investigator comments, search results, search criteria, pictures, and exports the those onto RTF, PDF, and HTML formats for easy distribution to everyone from fellow investigator to the attorney's office. This tool offers the cluster by cluster view of all files detected on the storage media, i.e. Information such as last access, time created, and last modification of the file are all provided by this tool. The figure shows how deleted, hidden files are viewed through the encase imager tool**.**

Fig 4.1 show the hidden files and deleted files discovered by the encase imager

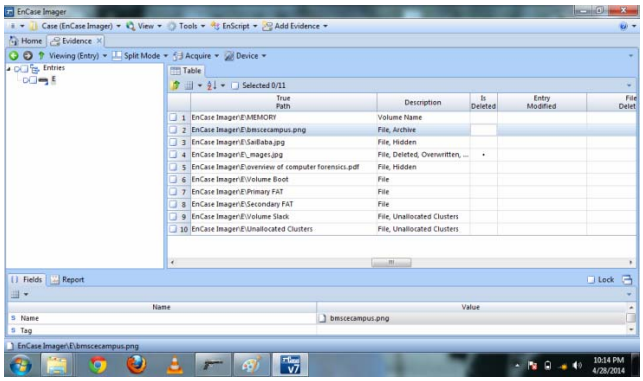
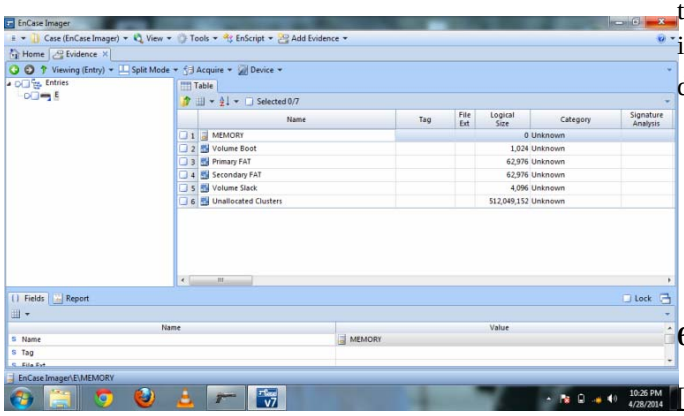


Fig 4.2 showing that encase imager cannot be able to discover the formatted data



4.THE SIMILARITIES AND DIFFERENCES BETWENN THE COMPUTER FORENSIC TOOLS

	Pro discover basic	**Pc-inspector file recovery**	**FTK imager**	**Encase Imager**
deleted data discovery	**High**	**High**	**High**	**High**
Hidden data discovery	**High**	**Low**	**High**	**High**
Lost data discovery	**Low**	**High**	**Low**	**Low**
Hidden data recovery	**High**	**Low**	**High**	**Medium**
Lost data recovery	**Low**	**Medium**	**Low**	**Low**
Deleted data recovery	**High**	**High**	**High**	**Medium**
Disk-imaging	**High**	**Low**	**High**	**High**

Efficiency:High, Medium, Low

5.CONCLUSION

From this paper we want conclude that forensic tools are very necessary for investigation of cyber-crime and most of the tools are not efficientin all the ways to recover the data of all the types, so this paper shows some of the inefficiency of the tools which has to be overcome, so that single tool will be sufficient in handling all data types by investigator in order to detect the crime in better way**.**

6.REFERENCES

[1]"FTK Imager" https://www.accessdata.com

[2] "Computer forensic definition"

http://searchsecurity.techtarget.com/definition/computer-forensics

[3]http://www.isfs.org..hk

[4]"Encase imager"

https://www.guidancesoftware.com/products/Pages/Product-Forms/Forensic-Imager-download.aspx

[5]"pc inspector file recovery"

http://www.pcinspector.de/?language=1

[6]"pro discover basic"

http://www.techpathways.com/desktopdefault.aspx?tabindex=8&tabid=14

[7]"disk image defined"

http://www.techterms.com/definition/diskimage

[8]"data recovery defined"

http://www.pcmag.com/encyclopedia/term/40834/data-recovery

[9]"data discovery defined"

http://www.datadiscoverynut.com/2012/02/what-is-data-discovery.html

AUTHOR PROFILE

Vikas is pursuing MTech in computer network engineering at BMS College of Engineering, Bangalore, Karnataka, his area of interest is computer forensic.