International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-10, Issue-2, March 2022
https://doi.org/10.55524/ijircst.2022.10.2.101
Article ID IRPV1040, Pages 513-518
www.ijircst.org

Computer Forensics Data Recovery Software: A Comparative Study

Sai Niveditha Varayogula[1], Kiranbhai Dodiya[2], Parth Lakhalani[3], Dr. Arushi Chawla[3]

[1]Student, Department of Forensic Science, Parul Institute of Applied Sciences, Vadodara.
[2]Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad.
[3]Assistant professor, Department of Forensic Science, Parul Institute of Applied Sciences, Vadodara.

Correspondence should be addressed to Sai Niveditha Varayogula1; nivedithavarayogula@gmail.com

Copyright © 2022 Made Sai Niveditha Varayogula1et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

ABSTRACT: With the advancement of the information technology, computer has become more important for the people. Computer not only stores data but also increase the channels of storing data in digital devices like pen drive, hard disk, memory card. However, problem with these digital devices is that if data has lost it is very difficult to recover; so many researchers do research on it and suggested the method of data recovery. The term data refers to the combination of numbers or words, images, audio or video files or even a software program. Data restore is the procedure of recovery of information from media that is either corrupted or damaged physically. The data recovery software extracts the data that requires serving as an evidence from personal computers and digital devices in criminal cases that involve frauds, murder, corruption, money laundering, assault, smuggling, email scams, digital abuse, matrimonial frauds and much more. Here in this study, we combine probably all data recovery software and we will conclude that the best data recovery software in forensic sound manner. This study will help in future study to understand the overview of computer forensics data recovery software.

KEYWORDS:Acquisition, Computer Forensic, Data Recovery, DataForensic, Digital Devices.

I. INTRODUCTION

The continuous advancement of digital world also causing a rapid growth in cybercrimes. Cybercriminals improving their abilities of utilizing the modern digital devices for malicious activities[1]. Digital forensics acting a vital role in investigating and analysis of cybercrimes. The field of computer forensics is a subset of forensics science used for the investigation, extraction and analysis of digital evidence from digital devices such as computer, smartphones, tablets, etc. It is further classified into sub-branches such as Computers analytics, portable phone forensic, networking forensics, forensics information analytics, and databases ballistics are all examples of computers forensics. Every discipline of digital forensics has its own set of guidelines for investigating, extracting, and analyzing digital data [2].

Computer forensics is a branch of digital forensics, which includes the identification, collection, preservation and analysisof data from the computer devices in a forensic sound manner. As there is advancement in technology computers are being used by most of the population. It can be used as a medium in many criminal Owing of their pervasiveness, they may be used in a variety of methods [3]. A computer can be the target of a crime and it can acts as an instrument for committing crime. For instance, crimes such as information theft, financial frauds, denial of service, or other direct attacks are the circumstances where most of the criminals targets computer. It can be used to commit crimes against other computers by gaining unauthorized access and manipulating data from them. Non-computer offenses, like falsifying papers or counterfeiting cash, may also be committed using computers. In cybercrimes whether in a direct or indirect way computer takes the part of the attack. The investigation of cybercrimes are difficult sometimes due to the expiry of life of data within fractions of time. In such situations the main duty of the investigator is to Identify leftovers and present the findings. One of the biggest significant aspects of a cyber criminal investigations is the examination of the retrieved information. However, the analysis is not carried out directly on the suspect's computer.Instead of it, investigator creates a copy of the data for the analysis. This must be performed to protect the suspect's information on the hard disc from being tampered with or altered. The investigator copies the information of the accused's hard disc to one or several hard disks for additional inquiry.

A. Overview of data recovery

Data recovery is a process of acquiring lost, corrupted or damaged data from different storage medium. Data recovery plays an important role when the data is unable to access by regular procedures. For instance, the data in an electronic device is corrupted or formatted completely, and also when the storage medium is damaged data recovery method is used to acquire the data[4]. In certain digital crimes criminals tries to delete logs, files and other useful data to erase their traces of evidence in crime. In such situations investigation officer requires certain data recovery software to acquire the essential data, which helps in further investigation procedures. Data recovery software or the techniques of data recovery are also required in situations where the loss of data is due to virus, accidental deletion and system failure [4]. Data losses may be caused by both computer and physical issues, while we can recover data by means of software and hardware ways.This study gives a brief knowledge of different types of data recovery software in forensic aspects.The information restoration process varies depending on the circumstances of the information recovery, the data restoration tool used to create the restore, and the standby destinations material. Many backup software solutions for desktops and laptops, for example, allow consumers to restore lost data easily, but recovering a broken databases from a tape back is a time-consuming process that necessitates IT support[5]. Information restoration solutions might also be utilized to retrieve data that originally not authorized and was accidentally erased from a desktops file systems, but is still strewn over the hard disk.Because a file and its associated information are kept in separate locations, data recovery is possible. The Windows operating system, for example, keeps track of which documents are on the hard drive and where they are kept using a file allocation table. The allocates tables resembles an author's table of topics, while the information on the hard disk resembles a book's covers.

B. Material and Methods of data recovery

During analysis of Non-volatile memory of digital devices there are number of tools that are used during analysis[6]. This section includes the different methods of data recovery software, which are used to acquire data from digital devices.

a. Recuva v.1.43

Recuva is a free Windows-based program that aids in the recovery of data that have been unintentionally erased from a computer[7]. This comprises documents that have been destroyed by user mistake from memory sticks and outside media like MP3 devices, as well as files that have been unintentionally cleared from the Recycle bin. Recuva is a file recovery program that can help with a wide range of file formats and can restore information from any rewriteable medium, including memory devices, portable hard devices, and USB devices, and USB drives. Recuva can aids even in the recoveryof documents that were 'lost' as a result of flaws, failures, or infections. The data of any size can be acquired within few seconds by the help of this software and it is a free software[8].

System requirements for recuva:
RAM- 512 MB
HDD Space- 5 to 10 MB
Operating system- Windows 95 to Windows 7
Processor- 2 GHz or Higher.

MINITOOL power information recuperation:

MINITOOL power information recovery is particularly developed to recover the lost data from different storage devices[9]. It is the professional data recovery software for windows- based computer system. Lost information rescue, lost sector healing, broken sector recovering, electronic asset recovering, and CD/DVD recovery are all possible with this program. It not only aids in the restoration of lost files, but also restores data from hard drives that have been damaged or reformatted. MINITOOL Fast Information Restoration isn't only for recovering information from hard drives and RAID arrays, but also aids in the process of data recovery from digital devices such as CD, memory cards, DVD disks, flash drives and memory sticks. Undelete Restoration, Damaged Partition Restoration, Lost Partition Recovery, Digital Media Recovery, and CD/DVD Recovery are the five information recover components included in MINITOOL Power Data Recovery. Each information restoration course concentrates on a certain kind of information lost[10].

System requirements for MINITOOL power information restore:
RAM- 512 MB and above
HDD Space- 20 to 30 MB
in commission system- Windows 95 to Windows 7
Processor- 2.00 GHz or higher

b. EnCase

EnCase programme is a completely window-base and forensic software. It is used in the analysis of digital evidence in crimes such as civil or criminal investigations, network investigations, electronic discovery and data compliance. It is used frequently by several law enforcement agencies[11]. It is recognized as one of the courts approved software for the analysis of computer crimes. The important features of EnCase software are analysis of File signature, to view deleted files and file fragments in unallocated space or slack space, recovery of folder, analysis of log files and event logs, external file viewer and registry viewer.

c. WinHex Tool

WinHex is a hexadecimal software,which is mostlyused in information restoration, electronic espionage, and low-level data processors It's a sophisticated tool for daily use. and also very helpful to use in emergency[12]. It Examines all sorts of files and retrieves damaged or damaged information from corrupted file structures on hard drives or electronic cameras devices. The features of WinHex tool includes:

1. Comparison and analysis of files.
2. Disk cloning and Disk imaging.
3. Calculation of hash for files
4. For every electronic assets, generates a folder and directories catalogue.
5. Various techniques of Data recovery
6. Interprets Data
7. Supports files of unlimited size.
8. Trying to unite and dividing uneven and even bytes/words, substring and separating data
9. Detects access to NTFS and ADS.

d. ILook Investigator

ILook Investigator is a forensic based software includes a complete set of computer forensics tools, which helps in the analysis, and acquisition of digital media. It is mostly used by government and law enforcement agencies. It may examine electronic material recovered from confiscated laptops as well as other electronic information. Sophisticated email deconstructing and analysis, as well as full indexing capabilities, are among the characteristics of ILook, reporting, advanced unallocated space data salvaging capacity. It can run on both the versions of 32 and 64 bits of windows XP as shown in Figure 1.

e. Digital Detective Blade

The Digital Forensic Blades program is a Windows-based forensic data restoration software. Information restoration characteristics, Intelli-Carve®, and cellular device information restoration are just a few of the key features. Information restoration template assists the client in developing a data restoration picture for each kind of data that may be recovered. The identities are saved in a computer and may be retrieved instantly with any kind of recorded data. Intelli-Carve® assists in the verification of all returned information in order to validate the evidence's correctness and integrity. The restoration of photos, movies, and SQLite databases from cellular handset hex dumps is included in mobile phone recovery. There are two versions of this software: Standard and Professional. All main forensic image format standards, including JPEG, MPEG-4, DD , AFF, Clever Testimony, Accessible Data FTK, and Wrap E01, are supported by the standard version. The Professional edition not only includes all of the capabilities of the Standard version, but also adds modules for recovering emails from AOL and Outlook, hashing functions, picture formats converts, and SQLite databases. Because Electronic Investigator Sword lacks a file reader for viewing recovered files, extra application is necessary to cut into them[13].

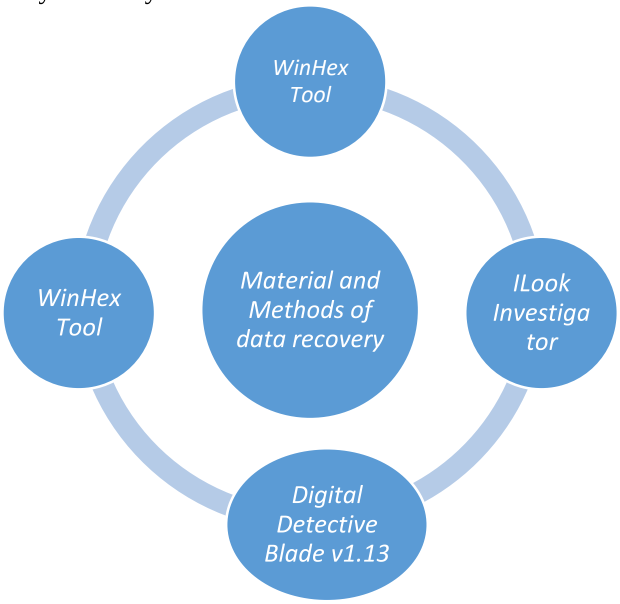
WinHex Tool
WinHex Tool
Material and Methods of data recovery
ILook Investiga tor
Digital Detective Blade v1.13

Figure 1: Diagrammatic Representation of Material and Methods of data recovery.

f. Forensic Toolkit(FTK)

AccessData's Forensics Toolbox, or FTK, is a computerized forensic application. It scans a hard drive for various pieces of data. The features of FTK are given below
Imaging and analysis of the computer file systems.
Rapid analysis of large amounts of data.
Includes the capabilities for the analysis of mobile devices.
Includes the hash checksums for the accuracy of data.
user-friendly graphical interface

C. Types of forensic toolkit(FTK)

a. Windows Forensic Toolchest (WFT):

Microsoft Forensics Toolchest is forensics application created specifically for capturing live data of volatile information on a Windows computer. It is used for the analysis of SQL Server Database as it can extract Information from the databases is extracted and analyzed, including current activity, error reports, and even data recovery. WFT can also help with MD5 and SHA-1 checksums of information to ensure its correctness. Finally, it provides a HTML report as an alternative for the summary and format of the findings of raw text report. [9]

b. Sleuth kit

The Sleuth kit provides both Windows and UNIX based tools for the forensic analysis of the computer systems. It aids in the analysis of disk imaging and recovery of data from it. With the help of these tools, it can be possible to identify the location of the partitions and extraction of partitions in order to analyse with file system analysis tools.

c. SANS Investigation Forensic Toolkit (SIFT)

SANS Investigation Forensic Toolkit (SIFT) is a Toolkit that is built on Ubuntu Server Live CD that offers a comprehensive set of tools in which you desire to undertake a rigorous forensic cybercrime or any event responding inquiry. This is a free downloadable SIFT forensic toolkit that is identical to any enhanced incidence enquiry and a tool that suite is also an extra component in the process of

SANS' Advanced Incident Response as shown in Figure 2. It suggests that efficient inquiries and admitting to the intrusions is the sole technique to complete the splitting and open-source-system equipment that is readily out there and are frequently upgraded.

d. Pro discovery forensic

It is a key forensics software that would assist the computers in locating data on the notebook hard drive and would also preserve the evidence it located and provide excellent quality of obtained data for any legal processes. This utility also recovers the lost data, examines the capacity in the device, periodically enables search in the drives. This utility extracts the data from a drive at a sector level, thus no data loss occurs in any catastrophic occurrences.

e. Volatility Framework

Volatility Framework was officially disclosed at BlackHat, and by the university study Centre, it is a sophisticated volatility analyzer. It also supplies a distinctive framework that will permit to cut-edge study to quick into the digital researcher hands. It is largely employed in military, business investigation, law administration, etc. across the whole globe.

f. Computer-Aided Investigation Environments(CAINE)

Computer-Aided Investigation Environments (CAINE) is a Linux Live CD to match up with the criteria of forensic reliability. It is a semi-automated report generating to receive the findings in very least time. In the current edition, CAINE is based on Linux and LightDM. It also offers a user-friendly UI to function successfully.

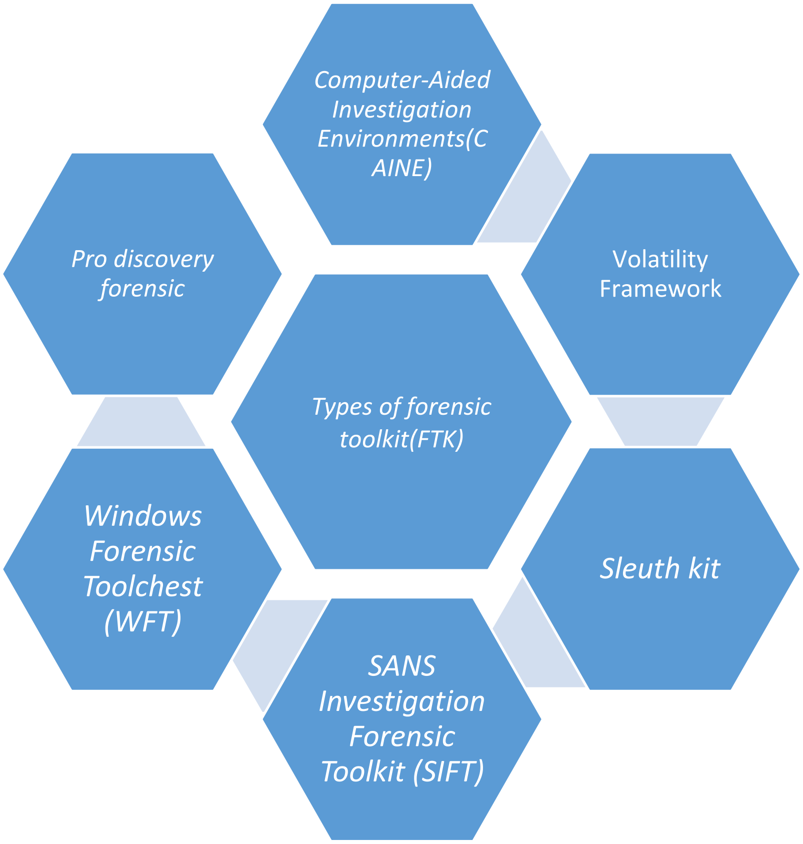
Computer-Aided Investigation Environments(CAINE)
Pro discovery forensic
Volatility Framework
Types of forensic toolkit(FTK)
Windows Forensic Toolchest (WFT)
Sleuth kit
SANS Investigation Forensic Toolkit (SIFT)

Figure 2: Diagrammatic Representation of Types of forensic toolkit (FTK).

D. Advantages of data recovery method

a. Security

Data safety have been an increasing issue in the last several years, driving firms to establish effective data privacy measures. Incorporating trustworthy data backup services will help you secure your data from dangerous actions. Most systems provide data security with the assistance of encryption to shield your backed-up data from theft and breaches[14]. Data security is a basic right. Organizations need to convince their consumers that their stored data is secure with them, since identity theft incidents related to data loss are on the increase.

b. Ease of Management

One of the most challenging jobs that an organization may undergo is data management during its restoration. This recovery procedure, if done manually, might be unreliable. Most data recovery solutions let you develop a thorough backup plan for your data while making a distant backup and maintaining the data within. Storing a backup of your data might aid you in times of crisis if your business encounters data loss. With a current and comprehensive backup to recover from, organizations can get return to work fast following an effective data recovery.

c. Reliable Replication

Data backup and recovery applications provide replication capabilities. This may be used to produce real-time clones of your data and store them elsewhere, making your data disaster-proof. This replication enables you to effectively reverse your work and start over in event of a data loss. Replication feature is the easiest approach to extract data and saving time on the recovery process. This doesn't generate any delays in business procedures.

d. Standards of Compliance Observance

Under numerous data privacy standards, obtaining and preserving your organization's data is required. Organizations are required by laws like as the Californian Customer Privacy Act to gather and securely keep consumers information on their servers. Neglect to do so may result in significant penalties and possibly criminal charges. In order to completely comply with regulatory audits, data authorities demand enterprises to back up their SQL databases in a data center. Backup and recovery solutions allow you to preserve a back up of the info center servers and monitor them on a daily, quarterly, and annual basis for auditing reasons.

e. There is no effect on performance

Data recovery may be time-consuming, necessitating the allocation of resource to the recovery procedure. The loss of data may be a huge setback for a company. Due to a shortage of resources, they are playing catch-up with everyday activities without a robust data recovery solution.

f. Cost-cutting

If a business loses data, it is likely that they will need to employ a third-party service to assist them in recovering their data. This may be expensive and time-consuming, as well as allowing a third-party exposure to corporate data. Integrating a reliable backup and restore system protects your data's privacy while also lowering your company's expenses.

II. DISCUSSION

Many years back all the firms should preserve all information and statistics on papers and notebooks but with existence of technology, everything has changed. One of this technology is computing. Nowadays all the organizations utilize computers in their work systems and preserve all the data on it. This information are highly vital for business for example, data regarding financial systems, economic sources, hidden information of firm, long-term and short-term strategy of business and many more significant information. By dealing with several difficulties such as: data theft, program theft, accidently deleting, mistakenly converting and so on, the firms recognize that they require having a mechanism to recover their data. Because of this significant and vital demand, the complete software producer businesses sought to make data recovery software. In addition, this manner data recovery arrived to our lives and became a crucial component of our existence.

Data Recovery may be required for causes as varied as mechanical breakdown, (the tape has been 'chewed' up, the hard disk drive has failed, the user has intentionally destroyed the computer or digital device, or it might have suffered fire or water damage). All of those conditions will demand the use of a competent information restoration agency if the information was of such significance that the cost of the service was less than the imagined importance of the information that were lost. From the study, we have found that that Recuva gives best data recovery outcome. Recuva is an open source and effective data recovery software and recovers data based on file extensions. Recuva software undeletes or recovers the data quickly and safely whatever the type of file it may be. It runs on any windows computer system. It can even restore any unsaved documents, which got deleted accidentally. It helps in the recovery of data even from damaged or newly formatted disks. Plugin features an extensive deep scan option that exhaustively searches your disk for any evidence of lost items.

III. CONCLUSION

The database recovering process differs based on the situation of the information defeat, the data repair tool utilized to make the restore, and the standby destinations medium. For illustration, most computer and backup software systems allow users to restore lost files easily, but recovering corrupted database using a cassette back is a more difficult task that necessitates IT expertise. Information restoration solutions might also be utilized to retrieve data that was not backed and was accidentally erased from a smartphone's file structure, but is still strewn over the storage disk. The purpose of this study is to offer the most efficient techniques for data analysis in computer systems. Throughout our practical, we discovered that there are several instruments accessible on the marketplace. Here we introduce the most effective technique, which is best among all other tools and this tool can be helpful to collect, examine and preserving digital evidence of computer forensic crime.

REFERENCES

[1] V. D. Tran and D. J. Park, “A survey of data recovery on flash memory,” Int. J. Electr. Comput. Eng., 2020, doi: 10.11591/ijece.v10i1.pp360-376.

[2] S. Wang, J. Yuan, X. Li, Z. Qian, F. Arena, and I. You, “Active Data Replica Recovery for Quality-Assurance Big Data Analysis in IC-IoT,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2932259.

[3] B. K. Oh, B. Glisic, Y. Kim, and H. S. Park, “Convolutional neural network–based data recovery method for structural health monitoring,” Struct. Heal. Monit., 2020, doi: 10.1177/1475921719897571.

[4] L. Liu, Q. Guo, D. Liu, and Y. Peng, “Data-Driven Remaining Useful Life Prediction Considering Sensor Anomaly Detection and Data Recovery,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2914236.

[5] G. Fan, J. Li, and H. Hao, “Lost data recovery for structural health monitoring based on convolutional neural networks,” Struct. Control Heal. Monit., 2019, doi: 10.1002/stc.2433.

[6] T. Zhou, Z. Cai, B. Xiao, L. Wang, M. Xu, and Y. Chen, “Location Privacy-Preserving Data Recovery for Mobile Crowdsensing,” Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol., 2018, doi: 10.1145/3264961.

[7] J. Sahoo, S. Mohapatra, and R. Lath, “Virtualization: A survey on concepts, taxonomy and associated security issues,” 2010, doi: 10.1109/ICCNT.2010.49.

[8] B. K. Sahu, S. Pati, P. K. Mohanty, and S. Panda, “Teaching-learning based optimization algorithm based fuzzy-PID controller for automatic generation control of multi-area power system,” Appl. Soft Comput. J., 2015, doi: 10.1016/j.asoc.2014.11.027.

[9] S. Panda, B. K. Sahu, and P. K. Mohanty, “Design and performance analysis of PID controller for an automatic voltage regulator system using simplified particle swarm optimization,” J. Franklin Inst., 2012, doi: 10.1016/j.jfranklin.2012.06.008.

[10] G. Das, P. K. Pattnaik, and S. K. Padhy, “Artificial Neural Network trained by Particle Swarm Optimization for non-linear channel equalization,” Expert Syst. Appl., 2014, doi: 10.1016/j.eswa.2013.10.053.

[11] M. Biswal and P. K. Dash, “Measurement and classification of simultaneous power signal patterns with an s-transform variant and fuzzy decision tree,” IEEE Trans. Ind. Informatics, 2013, doi: 10.1109/TII.2012.2210230.

[12] R. P. Mohanty and A. Prakash, “Green supply chain management practices in India: An empirical study,” Prod. Plan. Control, 2014, doi: 10.1080/09537287.2013.832822.

[13] M. R. Lohokare, B. K. Panigrahi, S. S. Pattnaik, S. Devi, and A. Mohapatra, “Neighborhood search-driven accelerated biogeography-based optimization for optimal load dispatch,” IEEE Trans. Syst. Man Cybern. Part C Appl. Rev., 2012, doi: 10.1109/TSMCC.2012.2190401.

[14] S. Panda, S. C. Swain, P. K. Rautray, R. K. Malik, and G. Panda, “Design and analysis of SSSC-based supplementary damping controller,” Simul. Model. Pract. Theory, 2010, doi: 10.1016/j.simpat.2010.04.007.