IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 13, Issue 1, January 2023, ||Series -II|| PP 01-04

Data Recovery in Forensics.

Purva Patil[1], Dhwaniket Kamble[2], Dipali Pawar[3],Nidesh Alimkar[4], Sampada Chauhan[5], Manvi Bhaldare[6], Mohanish Shinde[7],Umesh Vishwakarma [8], Diksha M. Bhalerao[9],Sumita Kumar [10].

[1] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[2]Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University, Maharashtra, Navi Mumbai-410210, India.
[3] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[4] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[5] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[6] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[7]Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[8]Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India
[9]Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University, Maharashtra, Navi Mumbai-410210, India.
[10]Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University, Maharashtra, Navi Mumbai-410210, India.

Abstract: Data recovery is crucial in the modern world, where forensics and cyber security are highly sought-after skills. Data recovery steps in when the convict damages or destroys the data storage devices, allowing for the data to be recovered from these artifacts. Many criminals are aware of this field of data recovery, and they constantly try to go around the existing recovery strategies, while organizations constantly look for better and more effective recovery techniques to deal with this issue. This paper focuses mostly on data recovery in cyber forensics and the different tools used to recover data.
Keywords: Data Recovery, Forensics, Preserving, Tools, and Techniques for data Recovery.

I. INTRODUCTION

The continuous advancement of the digital world is leadingto rapid growth in cybercrimes. Cybercriminals are improving their abilities to utilize modern digital devices for malicious activities [1].Digital technology can be applied as a tool in numerous criminal activities.A digital device such as a computer, smartphone, laptop, etc. can both be used as a tool for crime and become the target of it. For instance, most thieves target computers in situations involving information theft, financial fraud, denial of service, or other direct attacks, after performing crime Criminals tend to damage or delete data or destroy the footprints logically or physically such scenarios it becomes necessary to conduct a digital investigation, one of the most essential steps in the digital investigation is data recovery.

Data recovery is the process of making and storing copies of data that can be preserved from data leakage. Corporations opt to back up in the cloud to keep files and data accessible in the event of a system error, interruption of service, natural calamity,etc[2]. Backup in the cloud approximately means that the corporation can produce a copy of that data and reserve it dissimilar geographical location which can be used in case of data leakage or deception[2].

The storage media that includes internal or external hard disc drives (HDDs), solid-state drives (SSDs), USB flash drives, magnetic tapes, CDs, DVDs, RAID subsystems, and other electronic devices are where data is most frequently recovered. Recovery may be necessary if the storage devices have been physically damaged or if the file system has suffered logical damage that prevents the host operating system from mounting it (OS).

The most common data recovery scenarios include OS failure, storage device malfunction, storage device logical failure, and accidental corruption or deletion (typically, on a single-drive, single-partition, single-OS system), in which case the ultimate goal is simply to copy all important files from the damaged media to another new drive [2].

The term "data recovery" is also used in the context of forensic applications or espionage, where data is intentionally encrypted, hidden, or deleted, rather than damaged, which can only be recovered by some computer forensic experts [2].

II. METHODOLOGY

2.1 Steps in forensic data Recovery-

i. Obtaining a digital copy of the suspected system.
ii. Authentication and confirming system.
iii. Determining that the copied data is forensically acceptable.
iv. Recovering deleted files.
v. Finding the necessary data with keywords.
vi. Establishing technical support. [3]

2.2Types of Attempts to Damage data –

2.2.1Physical Damage:
The criminal tries to physically damage the device used to perform the crime by burning, smashing/breaking, magnetizing, etc. to permanently delete the digital evidence.

2.2.2 Logical Damage:
When the device is damaged logically, the physical parts are functional but the data inside the device is inaccessible by normal means. Logical damage includes corruption of data, virus attacks (like Ransomware) and memory overflow attacks, deletion of data, etc.

2.2.3Cybervandalism:
Cybervandalism is damage or destruction that takes place in digital form. Digital vandalism seeks to damage, destroy, or disable data, computers, or networks. [4]

2.3Recovery Techniques and Tools -
The tools, techniques, and methodologies of electronic investigation, gathering, and analysis have been tried and proven and are accepted in many countries [5]. While recovering the data the integrity of the original media must be maintained throughout the investigation. Forensic analysis tools are used for recovering information [6] [7].

2.3.1 Disk Imaging-
Unless the disc is physically damaged, corrupt data can usually be recovered with the aid of specific software programs. A disc is copied bit-by-bit using the disc imaging technique [8].
steps in a data imaging process are -

- According to its IO configuration, the hard drive can be accessed independently depending on the OS.
- The problematic sector is read rather than skipped.
- The restarting commands are ignored while reading the disc [9].

This method is advantageous because it prevents commands that, in the event of an error, would restart the entire process while also restoring everything that can be read from the disc. Disk imaging on a physically flawed drive, however, may have a significant number of errors and instability [9][10].

2.3.2 File Carving-
Carving is the process of separating data (files) from undifferentiated blocks of raw data. File carving is the process of identifying and recovering files using file format analysis. In Cyber Forensics, carving is a useful method for locating deleted or hidden files on digital media. A file may be concealed in places on a disc or digital media such as missing clusters, unallocated clusters, and free space [11]. A file must have the standard file signature known as a file header to employ this extraction technique (start of the file). The file footer (the end of the file) is reached after a search to find the file header has been conducted. To verify the file, data will

be extracted and evaluated between these two locations. The extraction algorithm uses different methods of carving depending on the file formats [12].

2.3.3EnCase-
EnCase program is completely window-based 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 [13]. 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 signatures, viewing deleted files and file fragments in unallocated space or slack space, recovery of the folder, analysis of log files and event logs, external file viewer, and registry viewer [14][15].

2.3.4 Pro discovery forensic-
It is 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 obtained data for any legal processes [16]. This utility also recovers the lost data, examines the capacity of the device, and 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 [16][17].

2.3.5 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 generated to receive the findings forthe very last time. In the current edition, CAINE is based on Linux and Light-DM. It also offers a user-friendly UI to function successfully [18][19].

2.3.6 Email Forensic Carver-
Email carving tool to carve e-mail messages from corrupt or orphan mailboxes. Also helpful in email forensics and forensic search. Export reports in common formats, which are acceptable in courts [20][21].

2.3.7 Digital Detective Blade
Blade from Digital Detective will carve different categories of files such as archives, documents, graphics, audio, and video files. User-defined carving based on header + footer/length is available as well [22].

2.4 Factors affecting the Rate of Successful Recovery of Data:
The abovetools and techniques will help to recover the data efficiently, but some factors may affect the rate of recovery in such a manner that it may take more time to recover the data, and only a portion of data or fragment of data is recovered. Some of the factors can be listed as follows: -

- Overwritten data.
- Defragmented hard disk.
- Delay Period (time taken to start the process of recovery after deletion or loss).
- Size and format of the file.
- Type and extinction of damage caused.
- Available information about data to be recovered.

IV. CONCLUSION

Data recovery is the process of obtaining lost or deleted data from a device. Data recovery in forensics is the most essential step which helps in obtaining digital evidence from suspect devices. Cybercrime is increasing day by day which makes it mandatory for the IT enterprise to establish technics and tools for controlling such unethical acts. The database recovery process varies depending on the extent of the information loss, the data repair tool used for the restoration, and the standby media. For instance, the majority of computer and backup software programs make it simple for individuals to restore lost files but recovering corrupted databases using a cassette back is a trickier operation that requires IT experience. This paper discusses the various tools and techniques available for data recovery from a forensic perspective. However, each tool differs in functionality but has one aim of obtaining and preserving the digital evidence in an admissible format.

This research work aims to introduce you to the most effective tools and techniques available for data recovery. In this paper, we discuss data recovery and its need in today's world where cybercrime is on an increasing graph. With the increase in digital crime, the current automated forensic tool plays a major role in the aspect of finding digital evidence and process of data recovery. Each forensic tool has its specifications and limitations depending on the type of damage, available information, and many more aspects.

REFERENCES

[1]. Sai NivedithaVarayogula, KiranbhaiDodiya, Dr. Arushi Chawla, "Computer Forensics Data Recovery Software: A Comparative Study", International Journal of Innovative Research in Computer Science & Technology (IJIRCST), Vol-10, Issue-2, (ISSN 2347 - 5552), 2020, pp-513-518.

[2]. Monisha and Venkatesh Kumar, "Cloud Computing in Data Backup and Data Recovery", International Journal for Trend in Scientific Research and Development, Vol. 2, Sep-Oct 2018.

[3]. VV. D. Tran and D. J. Park, "A survey of data recovery on flash memory," Int. J. Electr. Comput. Eng., 2020, pp360-376.

[4]. Yogesh Gite and Ankush Pawar, "Efficient Data Backup Technique for Cloud Storage", International Journal of Engineering Research in Computer Science and Engineering, Vol. 5, Mar 2018.

[5]. E. M. Adehenu, "Deleted Data Recovery Mechanism," Advances in Multidisciplinary and Scientific Research Journal Publication, vol. 1, no. 1, Jul. 2022, pp. 363–372.

[6]. Z. Mohammed, "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches," Organizational Cybersecurity Journal: Practice, Process, and People, vol. 2, no. 1, Nov.2021.

[7]. Yoichiro Ueno, NoriharuMiyaho, Shuichi Suzuki,MuzaiGakuendai, Inzai-shi, Chiba,Kazuo Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications,2010, pp 256-259.

[8]. DaghmehchiFiroozjaei, Mahdi, Arash Habibi Lashkari and Ali A. Ghorbani. "Memory forensics tools: a comparative analysis.", Journal of Cyber Security Technology 6 (2022):

[9]. Shivang Modi, Yash Dakwala, Vishwa Panchal, "Cloud Backup and Recovery Techniques of Cloud Computing and a Comparison between AWS and Azure Cloud", International Research Journal of Engineering and Technology (IRJET), Volume: 07, Issue: 07, July 2020.

[10]. Anmol Bansal, Aastha Agrawal, Mahipal Singh Sankhla, Dr.Rajeev Kumar, "Computer Forensics Investigation on Hard Drive Data Recovery", IOSR Journal of Computer Engineering, September 2016.

[11]. Dr.K.Rajasekaran, P.Nisha M.C.A., "Data Backup And Recovery Methodology In Cloud Environment", Journal of Information and Computational Science, Volume 10, Oct.2020.

[12]. K.Laxmi, K.Deepika, N.Pranay ,V.Supriya, "Data Backup and Recovery Techniques in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology,Volume 3, Issue 4, ISSN: 2456-3307, April 2018.

[13]. Mr. ManasjyotiSaharia, Mr. Bidyut Kumar Sarma, Mr. Sailen Dutta Kalita, Mr. Dhriti Mohan Sarma, "An Analysis on Data Recovery and Backup Technologies in Cloud Computing", International Research Journal of Engineering and Technology (IRJET), Volume: 08,06 June 2021.

[14]. Vijeta Bharti1, Mr. KiranbhaiDodiya, Dr. Shivani Pandya, "A Comparative Study of Software for Data Recovery", International Research Publication House, 2020.

[15]. 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.

[16]. Intellipaat[Online]: Available: https://intellipaat.com/blog/what-is-cyber-forensics/. [Accessed: July 21, 2022]

[17]. C. Hoffman, "Bad Sectors Explained", Available: https://www.howtogeek.com/173463/bad-sectors-explained-why-hard-drives-get-bad-sectors-and-what-you-can-do-about-it/. [Accessed: August 17, 2022]

[18]. 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.

[19]. Softpedia [Online]: Available: https://www.softpedia.com/get/System/Back-Up-and-Recovery/EnCase-Data-Recovery.shtml. [Accessed: August 02, 2022]

[20]. Cyber Forensics [online]: Available: http://www.cyberforensics.in.[Accessed: July 21, 2022]

[21]. ProDiscover [online]: Available: https://prodiscover.com [Accessed: August 01, 2022]

[22]. WIKIPEDIA [Online]: Available://http://en.wikipedia.org/wiki/Data_Recovery [Accessed: June 29, 2022]

[23]. A.Shirobokov, "Disk imaging: a Vital Step in Data Recovery ", Available: http://www.deepspar.com/wp.html[Accessed: June 10, 2022]

[24]. Cyber Forensic [online]: Available: http://www.cyberforensics.in. [Accessed: July 21, 2022]

[25]. WIKIPEDIA [Online]: Available://http://en.wikipedia.org/wiki/Data_Forensics [Accessed: July 27, 2022]