IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. II (Sept - Oct. 2016), PP 39-42
www.iosrjournals.org

Computer Forensic Investigation on Hard Drive Data Recovery: A Review Study

Anmol bansal[1], Aastha Agrawal[1], Mahipal Singh Sankhla[2], Dr. Rajeev Kumar[3]
[1]*Students of Bachelor of Computer Applications, School of Computing Sciences and Engineering, Galgotias University, Greater Noida.*
[2] *Student of M.Sc. Forensic Science, Division of Forensic Science, School of Basic and Applied Sciences, Galgotias University, Greater Noida.*
[3]*Assistant Professor, Division of Forensic Science, School of Basic and Applied Sciences, Galgotias University, Greater Noida.*

Abstract: *Computer Forensics is a science of seeking evidence found in computers and digital storage media. The main challenge before computer forensic investigatorsis to examine digital media with the aim of finding, collecting, preserving, recovering, analyzing and presenting facts about digital information and guaranteeing its accuracy and reliability.It is said that, "Once it is has been deleted it is gone forever!" This statement is not true. Deleted files can actually be recovered if effort to do so is made shortly after deletion. There are several tools and methods by which we can easily recover our data and get our data as it is back. This paper includes the various methods and tools to recover data from Hard Disk Drive (HDD), how data recovery tools works, in what situation you can lost your data permanently and in what conditions you can recover your data back. You can know about types of damages and techniques by which data can be recovered by this paper. This paper gives a glance of various methods used to recover data from Hard Disk Drive (HDD) and their corresponding forensic approach done by the computer forensic experts in the perspective of recovery.*
Keywords: *Computer Forensics, Hard Disk Drive (HDD), Recovery, Data, etc.*

I. Introduction

In today's world as the data is the most important part in human life so it is very necessary to know how we can lose our data and if we can recover it back or not. In the chapter of introduction firstly the definition means what is mean by data recovery & the other one is why it is needed. After this we will look after the recovery techniques and the challenges in data recovery**[1]**.Businesses are increasingly using computers to work with their internal and external documents, depending more and more on digital storage every day. Most attention has been focused on well-known problems such as viruses, exploits, etc. Attacks by intruders and insiders have led to billions of dollars in lost revenue and expended effort to fix these problems **[2].**

Definition: Data recovery is the process of recovering data from primary storage media when it cannot be accessed normally. This can be due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system. The loss of data can be due to logical and physical damages or due to over writing of data. And there are different ways to tackle all these three conditions.The data loss or impairment became very common due to the internal (software or hardware faults) or external (operator fault and environmental faults) faults**[1]**.For the most part, these attacks have been focused on software based vulnerabilities, while perhaps the most devastating vulnerability

In fact, physical attacks on storage hardware are common and may be the most likely and dangerous type of attack **[3]**. Although using this new, digital alternative to paper may seem to be easier and faster, inside these seemingly harmless computers lie devices which are recording and generating audit trails of all data ever accessed on them, potentially acting as an informant to whoever possesses the devices. In fact, overlooking these devices may give an attacker a chance to steal sensitive data. Also, this could be carried out by any personnel with physical access to the machines **[4].**

Need for Data Recovery: Increasing hastiness and pace of life resulting in accidental deletion of valuable useful data added to the agony. This reveal only one side of the importance of Data Recovery, the other side is nothing other than the forensic importance of the data recovery. The change that the forensic need have is, here the data may not be accidentally deleted but that makes a difference in the recovery mode also as in this face the recovery will be difficult as the deletion would have been performed in an intention that the data should never get recovered. These situations were the circumstances which lead to the need of recovering the lost data .In

such cases of accidental loss of stored data, we will be barely in need of such recovery software and some times more than software which can perform usual undlation. Hence the data recovery became important. The data recovery procedure became important irrespective of the file systems used. In each file system the data recovery process depends on the type of file systems and their features. Besides this there are drive independent data recovery methods also **[1].**

Data loss due to Physical Damage: Physical damage could be caused by various failures. Hard disk drives could undergo any of numerous automatic failures, like head stack crashes, tapes could just break Physical damage at all times causes as a minimum a few data loss, and in a few cases the logical formations of the file system are smashed too. Recovering data following physical damaged hard drives: **[5]** majorities of the physical damage could not be mended by end users. For instance, opening a hard drive within a standard environment could let airborne dust to resolve on the media salver and being fixed between the salver and the read-write head, leading new head crashes that further damage the salver and thus concession the recovery procedure. End users usually don't have the hardware or technological proficiency required to create these repairs**[1].**

Data loss by software issue: Virus, format, mis-partition, mis-clone, mis-operation, network deletion, power-cut during operation all may be the software reasons. The symptoms are usually mis-operation, read error, can't find or open file, report no partition, not formatted, password lost and troubled characters.
Computer Viruses: some malicious virus programs will destroy data, overwrite, or erase the data contents.
Mis-format: fast or completely format partition, thus changing the file system form (NTFS, FAT32) of partition.
Mis-Clone: when backing up the hard disk, mis-clone or overlay the original data on hard disk.
For these, we can use software tools to recover it. So called soft recovery means data can be recovered by software, not referring to hardware fixing operation for its fault is not because of hardware failure **[6].**

Cases in which data is unrecoverable:

Modern computer hard drives contain an assortment of data, including an operating system **[7,8]**, application programs, and user data stored in files. Drives also contain backing store for virtual memory, and operating system's meta information, such as directories, file attributes, and allocation tables **[7]**.
The most common ways of damaging hard drives include:

- Physically destroying the drive, rendering it unusable.
- Degaussing the drive to randomize the magnetic domains-most likely rendering the drive unusable in the process.
- Overwriting the drive's data so that it cannot be recovered **[9]**.
- In, Anthony Verducci states three methods of destroying files via:
- File by file method (Individual files eliminated, software remains intact)
- Thewhole-drive method (Entire drive is permanently erased, but still usable)
- The power tool method (Data is gone, hard drive is toast) **[10].**

Every computer storage device contains files (used space) and free space (unused space). Each time the computer is used it may modify the metadata of the files in the used space and may overwrite previously deleted data that exists in the unused space **[11]**. Deleting files using delete or erase commands denote the low-level expertise of the individual. But expert culprits follow the destruction through overwriting so that the original data cannot be recovered. One-way they follow to overwrite a hard disk is to fill every addressable block with ASCII NUL bytes (zeroes). If the disk drive is functioning properly, then each of these blocks reports a block filled with NULs on read-back. Sanitization is a technique for erasing/deleting sensitive information, or to increase the free space in the disk and therefore erasing of files sometimes can be referred as Sanitization of disk. It is obvious that deletion done by an unauthorized individual is a criminal activity. There is a possibility of using potential sanitization tools by the attackers/culprits to destroy the files of authorized individuals **[9].**

Techniques to recover: The tools, techniques and methodologies of electronic investigation, gathering and analysis have been tried and proven and are accepted in many countries **[12]**. While recovering the data the integrity of the original media must be maintained throughout the entire investigation **[13]**. The basic methods of recovering unrecoverable data are described in **[14**,**15]**. The forensic analysis tools are used for recovering hard-disk information. Forensic tools analyze hard disks or hard-disk images from a variety of different operating systems and provide an Explorer-style interface so that one can read the files. The international important forensic tools **[16]** are presented in

Table 1: List of Recovery Tools

Tools	Platform	Description
Data Rescue PC3 [17]	Windows/Linux/Mac	By their own admission, Data Rescue 3 is built for hard disk drive recovery, but it still outperformed much of the competition when tested on solid-state devices. Among all the recovery software we tested, we experienced some of our most comprehensive results with DR3, which makes it a solid solution for logical data loss recovery. It's built-in disk imaging feature along with lab recovery options, information and excellent support adds value to an already exceptional product.
Ontrack Easy Recovery [18]	Windows/Linux/Mac	Kroll OntrackEasyRecovery Professional data recovery software is based on the company's real-world lab experience. In our tests the software performed particularly well at recovering our Microsoft Office files. It did provide us with an abundance of other file fragments that, with a little extra technical elbow grease and a third-party hex editor, could be made into complete files. The software's added support and an available recovery lab are also there in case you find yourself in over your head.
Stellar Phoenix Windows Data Recovery Professional [19]	Windows/Linux	Stellar Phoenix Windows Data Recovery Professional had the broad compatibility to take on all three of our test devices and perform very well. The software's additional features give you the opportunity to make even your most challenged recovery better.
Seagate File Recovery [20]	Windows/Linux/Mac	Seagate File Recovery for Windows has a definite talent for deleted file recovery, but its performance was somewhat hit or miss in other areas of our testing, depending on the type of loss we were trying to recover from. Regardless, it still provided the best recovery of files from a reformatted microSD card, and second best rate on recovering files from the reformatted HDD.
R-Studio [21]	Windows/Linux/Mac	While some of the brands we tested did perform better on the side of data recovery, the advanced tools available with R-Studio mean the right user can get better results with a manual recovery. However, the advanced tools require some level of expertise to employ. Other useful capabilities include remote scanning and a disk sanitation feature. However, the automated data recovery tools the software offers only did an average job at recovering data in our testing.
EaseUSData Recovery Wizard [22]	Windows/Linux	EaseUS Data Recovery Wizard Professional lacks some advanced recovery tools, but it is easy recovery software. Much of the functionality is not challenging, which lets you start your data recovery quickly so you won't be waiting long for results.
Recover My Files Professional [23]	Windows/Linux	GetData Recover My Files Professional ranks up there with the best data recovery software, but it's not for beginners. It's more geared toward the tech-savvy super user needing a complex data recovery solution. The included hex editor is based on file carving technology to give do-it-yourselfers a better-than-average chance at getting good returns doing their own data recovery. Unfortunately, it also gives you a chance at making your data loss catastrophic if you do it incorrectly.

II. Discussion

Of the large scale drive failure studies.It was analyzed data from about 100,000 disks over a five year time period**[25].** They found that failure rates increased over time, and error rates were not constant with disk age **[24].** It wasanalyzed data associated with over 100,000 disks over a nine month period. They used this data to analyze the correlation of disk failures to environmental factors and usage patterns. They found that the annualized failure rates were significantly higher for drives after the first year. It was studied various aspects of storage subsystem failures.Data left on donated hard drives can lead to devastating results. As indicated in this paper, some methods of data elimination may also prove inadequate. Whichever method is chosen either software wiping or physical destruction, individuals must take "reasonable measures" to safeguard their personal data**[28].** Although thoroughly sanitizing or destroying a hard drives takes some effort, the potential costs associated with compromised data make it an important task.There are very few studies of disk errors. Most disk fault studies examine either drive failures **[24, 25, 26, 27]**. Taking an example, let us discuss it further. In an investigation of a crime scene, the most important part of this investigation is to recover the data from Hard Disk Drive (HDD). As per our learning from this paper till now, we need to look out for the physical damage or logical damage. If it's a physical damage and the disk is harmed anyhow, we cannot recover the data in any case. If any part of the disk is harmed, data can be recovered by changing that particular part (Platters, Heads, PCB Circuit, Etc.). Taking into consideration a logical damage, the deleted data should not be overwritten.

III. Conclusion & Future Work

The current automated forensic tools play major role in the aspect of recovery. Each forensic tool has its own limitations and specifications. The best and simplest tool for the data recovery is "Data Rescue PC3". The existing tools puts efforts to recover the file when the disk is physically damaged or logically damaged i.e.

overwritten, by the experienced culprits. After concluding, we get to know that there is a timely need to enhance the tools we have discussed above and about the techniques to make the computer forensic analysis a full pledged and legally valid.In this paper I have talked about the HDD, in the future studies we can talk about the data recovery from USB drives, Flash drives, Phone memory and all the rest of data storages.

References

[1]. Bhagyashri P. Deshpande, (2013). "The Advanced Way Of Data Recovery", International Journal Of Computer Science And Applications, Vol. 6, No.2, Apr 2013.

[2]. Freeman, William, Long, Darrell, Miller, Ethan, Reed, Benjamin (2001). Strong Security for Distributed File Systems; in Proceedings of the 20th IEEE International Performance, Computing, and Communications Conference (IPCCC 2001), Phoenix, AZ, April 2001, pages 34-40.

[3]. Hasan, Ragib, Lee, Adam J., Myagmar, Suvda, Yurcik, William (2005). Toward a Threat Model for Storage Systems; in Proceedings of the 2005 ACM workshop on Storage security and Magnetic Data Recovery survivability, Fairfax, VA, USA, 2005, pages 94-102.

[4]. Goldschlag, David M., Landwehr, Carl E. (1997). Security Issues in Networks with Internet Access; in Proceedings of the IEEE, Vol. 85, No. 12 (December 1997).

[5]. Charles H. Sobey, LasloOrto, and Glenn Sakaguchi "Drive-Independent Data Recovery: The Current State-of-the-Art", IEEE transactions onMagnetics, IEEE volume 42 February 2006.

[6]. Data Recovery E-Book V1.5 (Visit http://www.easeus.com for more information).

[7]. Peterson, Siberschaz, Galvin, "Secondary Storage Structure, Advanced Operating Systems", 6th Edition.

[8]. Andrew S.Tanenbaum, "Modern Operating Systems" Prentice Hall, Dec. 2007.

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

[10]. Anthony Verducci, "How to Absolutely, Positively Destroy Your Data": DIY Tech, February 2007. http://www.popularmechanics.com/technology/how_to/4212242.html

[11]. Michele C. S. Lange, Kristin M. Nimsger, ''Electronic evidence and discovery'', American Bar Association, 2004.

[12]. Wofle, Henry B, Computers and Security, El sevier Science, Ltd, pp. 26-28. http://www.sciencedirect.com

[13]. Thomas Rude CISSP, "Evidence Seizure Methodology for Computer Forensics". http://www.crazytrain.com/seizure.html.

[14]. Charles H Sobey, "Recovering unrecoverable data", Channel Science white paper, 14th April 2004.

[15]. David Icove, Karl Seqer, William Von Storch, "Computer crime: A Crime-figher's Handbook", O'Reilly Media, Inc, USA (1 Aug 1995).

[16]. Simson L. Garfinkel and AbhiShelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices", IEEE Security & Privacy, Vol. 1, 2003, pp. 17-27.

[17]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/data-rescue-pc-review/

[18]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/ontrack-easyrecovery-review/

[19]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/stellar-phoenix-review/

[20]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/seagate-file-recovery-review/

[21]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/r-studio-review/

[22]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/data-recovery-wizard-review/

[23]. http://www.toptenreviews.com/software/backup-recovery/best-data-recovery-software/recover-my-files-review/

[24]. E. Pinheiro, W. D. Weber, and L. A. Barroso. Failure Trends in a Large Disk Drive Population. In Proceedings of the 5th USENIX Symposium on File and Storage Technologies (FAST '07), San Jose, California, Feb. 2007.

[25]. B. Schroeder and G. A. Gibson. Disk Failures in the Real World: What Does an MTTF of 1,000,000 Hours Mean to You? In Proceedings of the 5th USENIX Symposium on File and Storage Technologies (FAST '07), San Jose, California, Feb. 2007.

[26]. S. Shah and J. G. Elerath. Disk Drive Vintage and its Effect on Reliability. In The Proceedings of the 50th Annual Reliability and Maintainability Symposium, pages 163–167, Los Angeles, California, Jan. 2004.

[27]. S. Shah and J. G. Elerath. Reliability Analyses of Disk Drive Fail- ure Mechanisms. In The Proceedings of the 51st Annual Reliability and Maintainability Symposium, pages 226–231, Alexandria, Virginia, Jan. 2005.

[28]. W. Jiang, C. Hu, A. Kanevsky, and Y. Zhou. Is Disk the Dom- inant Contributor for Storage Subsystem Failures? A Comprehensive Study of Failure Characteristics. In Proceedings of the 6th USENIX Symposium on File and Storage Technologies (FAST '08), San Jose, California, Feb. 2008.