The Advanced Way Of Data Recovery

Bhagyashri P. Deshpande

M.E (P.T) Computer Science Department

Prof.Ram Meghe Institute of Engg.& Technology,Badnera

bhagyashri41@gmail.com

ABSTRACT: Data recovery refers to accessing logically or physically damaged data or over written data without the use any functioning backup. The advanced data recovery has two different methods where the first method - Part replacement which deals with the recovery from physically and/or logically damaged data. The second method of data recovery is the Magnetic recovery which deals with the recovery of the over written data. In this paper we are discussing about the methods and challenges for replacing, or refreshing firmware and system area information and for some part of the drive electronics. The magnetic recovery uses the Magnetic Force Microscopy for recovery of over written data. The backbone of the magnetic recovery is the interesting fact that the magnetic memory always remembers whatever is written on it till it is forced for a degauss under strong magnetic field. As far as the cyber forensics is considered the recovery of data after physical damage and over writing is of great importance. In this paper we discussed the limitations of current techniques and some probable future directions of data recovery. It is predicted that the data recovery is more important in near future.

1.INTRODUCTION:

In this paper we will see how data will be recovered from all types of damages like physical and logical. In this we will look after the need of data recovery in today's world as the data is the most important part in human life. 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. Depending on the field the data recovery is also refers to the result of data mining, decryption and decompression. In this paper data recovery means accessing data from logically or physically damaged media specifically from hard disk drives or to obtained a file or blocks that have no backups.[1]

1.1 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.

1.1 Why it is needed?

The data loss or impairment became very common due to the internal (software or hardware faults) or external (operator fault and environmental faults) faults.

This often poses the grave problem of losing all those outcomes of many hardships endured to achieve the specific task. Data which cost years of hardships may be lost in a flash due to a single mistake! We may be coming across such painful experiences too often. 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 undulation. 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.

2. Recovery from logical damage:

Logical damage is primarily caused by power outages that prevent file system structures from being completely written to the storage medium, but problems with hardware (especially RAID controllers) and drivers, as well as system crashes, can have the same effect. The result is that the file system is left in an inconsistent state. This can cause a variety of problems, such as strange behavior (e.g., infinitely recusing directories, drives reporting negative amounts of free space), system crashes, or an actual loss of data. Various programs exist to correct these inconsistencies, and most operating systems come with at least a rudimentary repair tool for their native file systems. Linux, for instance, comes with the feck utility, and Microsoft Windows provides chkdsk. Third-party utilities are also available, and some can produce superior results by recovering data even when the disk cannot be recognized by the operating system's repair utility.

Two common techniques used to recover data from logical damage are consistency checking and data carving. While most logical damage can be either repaired or worked around using these two techniques, data recovery software can never guarantee that no data loss will occur. For instance, in the FAT file system, when two files claim to share the same allocation unit (”cross-linked”), data loss for one of the files is essentially guaranteed.

2.1 consistency checking:

consistency checking, involves scanning the logical structure of the disk and checking to make sure that it is consistent with its specification. For instance, in most file systems, a directory must have at least two entries: a dot (.) entry that points to itself, and a dot-dot (..) entry that points to its parent. A file system repair program can read each directory and make sure that these entries exist and point to the correct directories. If they do not, an error message can be printed and the problem corrected. Both chkdsk and feck work in this fashion. This strategy suffers from a major problem, however; if the file system is sufficiently damaged, the consistency check can fail completely. In this case, the repair program may crash trying to deal with the mangled input, or it may not recognize the drive as having a valid file system at all. The second issue that arises is the disregard for data files. If chkdsk finds a data file to be out of place or unexplainable, it may delete the file without asking. This is done so that the operating system may run smoother, but the files deleted are often important user files which cannot be replaced. Similar issues arise when using system restore disks (often provided with proprietary systems like Dell and Compaq), which restore the operating system by removing the previous installation. This problem can often be avoided by installing the operating system on a separate partition from your user data

2.2 Data carving:

Data Carving is a data recovery technique that allows for data with no file system allocation information to be extracted by identifying sectors and clusters belonging to the file. Data Carving usually searches through raw sectors looking for specific desired file signatures. The fact that there is no allocation information means that the investigator must specify a block size of data to carve out upon finding a matching file signature, or the carving software must infer it from other information on the media.

There is a requirement that the beginning of the file still be present and that there is (depending on how common the file signature is) a risk of many false hits. Data carving, also known as file carving, has traditionally required that the files recovered be located in sequential sectors (rather than fragmented) as there is no allocation information to point to fragmented file portions. Recent developments in file carving algorithms have led to tools that can recover files that are fragmented into multiple pieces.

A good number of software tools are present now which can perform undulation, upto a great extend, even if data seems to be permanently deleted from the drive. The working of these tools are usually based on the nature of the file system that will never delete any data but only will mark it as deleted till it is over written next time. And these software can recover the data only before it is over written. These recovery tools are highly depended on the file system type.

The main disadvantage of these tools is that they can recover the data only when the drive is working properly and the data is not over written. In forensic needs it is needed to recover the data from physically damaged drives and also when the data is over written, because physically damaging the file and dumping the drive with junk data are not that much difficult jobs to be performed.

3.RECOVERY FROM PHYSICAL DAMAGE:

A wide variety of failures can cause physical damage to storage media. CD-ROMs can have their metallic substrate or dye layer scratched off; hard disks can suffer any of several mechanical failures, such as head crashes and failed motors; and tapes can simply break. Physical damage always causes at least some data loss, and in many cases the logical structures of the file system are damaged as well. This causes logical damage that must be dealt with before any files can be recovered. Most physical damage cannot be repaired by end users. For example, opening a hard disk in a normal environment can allow dust to settle on the surface, causing further damage to the platters. Furthermore, end users generally do not have the hardware or technical expertise required to make these sorts of repairs; therefore, data recovery companies are consulted. These firms use Class 100 cleanroom facilities to protect the media while repairs are made, and tools such as magnetometers to manually read the bits off failed magnetic media. The extracted raw bits can be used to reconstruct a disk image, which can then be mounted to have its logical damage repaired. Once that is complete, the files can be extracted from the image.

3.1.Causes of 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: [1] 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.

There are two techniques to recover data from physically damaged drives.& they are first is Replacing or ”refreshing” the system area information and Replacing the drives electronics. These two techniques are called ’Part replacement’ methods.

*3.2 T*he part replacement:

Techniques for recovering data from physically damaged hard disk can be described as part replacement [1-2] whereby printed circuit boards (PCBs) are swapped; heads are transplanted; motors and base castings are replaced by remounting the disks onto the spindle of a donor drive;[1] and firmware or system information is replaced or refreshed by rewriting it. Placing the disks in a donor drive swaps everything except for the on-disk system information. Data stored on portions of the magnetic layer of the disk that have been physically removed; such as due to a slider (head) scraping away the surface, cannot be recovered.

The ultimate part replacement operations are re-mounting disks onto new drives and transplanting head stacks. In these two extreme cases there are six difficult challenges to overcome for successful data recovery.

1. Re-optimizing preamp read settings.

2. Recalibrated repeatable run-out (RRO) and head offsets.
3. Control spindle rotation and head positioning, typically using the magnetic servo patterns on the disk surfaces.
4. Determine the layout and format of each surface, defects and defect mapping Strategies.
5. Detect the binary data in the analog head signal and
6. Decode the preceding, scrambling, RLL, parity-assist ECC, and any other codes to reveal user data.

The sectors or blocks created from the detected and decoded user bits must still be assembled into useful files. It is at this latter task where logical recoveries typically start. Interestingly, data forensic examinations can only begin after the physical and then the logical recoveries have been completed.

3.3 Refreshing the system information:

Current state-of-the-art research for system area refreshing focuses on developing algorithms that can quickly and adequately re-optimize all important channel, preamp, and servo system parameters without rewriting over data.[1] This capability is needed both when the system area information is corrupted and when a head stack transplant is necessary.

The system information includes the drive
specific hyper-tuned parameters along with the normal characteristic parameters of the hdd.The system area may become corrupted due to malfunctioning circuits, firmware bugs, exceeding the operational shock specifications of the drive, or position system errors. Another, more common, reason for system area corruption is a loss of power during an update of the system area itself.

The G-list, or grown defect list, holds information about the location of defects that have been found in the field during drive operation. The G-list is typically used for sector swapping, or sector reallocation. Related o this is the P-list, or primary defect list that stores the location of media defects that were found during manufacturing.

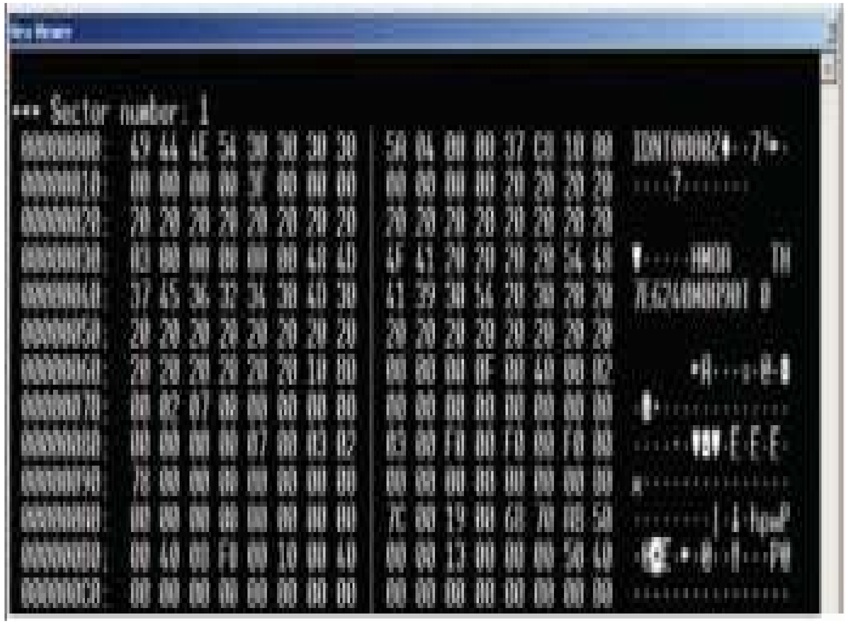

Fig:3.1 The beginning of the identification sector (IDNT) of the system area for a 2.5 Hitachi drive

For some drive models, the system area contains only a small amount of information, such as a unique drive serial number, the P-list and G-list, S.M.A.R.T. data, and a drive password possibly encrypted

3.4 Replacing the drive electronics

Current state-of-the-art research for drive electronics replacement focuses on developing faster and more robust methods for determining the servo sector track ID and wedge ID and the data sector encodings. Additionally, timing, equalization, and detection methods are being advanced to recover data from the drives that are being built today and in the future. These are likely to employ iterative equalization and decoding, LDPC (low-density parity-check) codes, and new timing recovery schemes.

For flyable media, the most cost-effective way to spin the disk is with its original motor and base casting or with from of a donor drive. All that is required is a standard HDD motor controller and related programming capability.[2] Once a compatible head stack is in place and the disks are spinning, the signal from the preamp needs to be acquired and used: first for servo positioning and then for data detection. To acquire a good signal, the read bias currents must be approximated for each head.[1]

Fig 3.2: The dull ring near the middle diameter of this spinning disk is the result of a head crash.

4. Recovery of overwritten data:

A good part of the computer users are still to know about the most important and interesting feature of our most common storage media, the magnetic storage media, which is it's capability to remember anything ever written on it till it is completely destroyed by a degauss under strong magnetic field. Magnetic hard drives are used as the primary storage device for a wide range of applications, including desktop, mobile, and server systems. All magnetic disk drives possess the capability for data retention,[5] but for the majority of computer users, the hard disk drive possesses the highest lifespan of all magnetic media types, and therefore is most likely to have large amounts of sensitive data on it.

In reality, magnetic media is simply any medium which uses a magnetic signal to store and retrieve information. Examples of magnetic media include: floppy disks, hard drives, reel-to-reel tapes, eight-tracks, and many others.[6-7] The inherent similarity between all these forms of media is that they all use magnetic fields to store data. This process has been used for years, but now that security concerns are being brought more into focus, we are now starting to see some of the weaknesses of this technology, as well as its well-known benefits.

4.1 Wise drives:

When data is written to the disc platter, it is stored in the form of ones and zeroes. This is due to the binary nature of computers the data in question is either on (1),or off (0). This is represented on the disk by storing either a charge (1), or no charge(0). The data is written to the actual disc platter in what are called tracks. These are concentric rings on the disc platter itself, which are somewhat similar to the annual rings of a tree. As data is written to these rings, the head actually writes either a charge (1), or no charge (0). In reality, as this is an analog medium, the discs charge will not be exactly at a 1 or 0 potential, but perhaps a 1.06 when a one is written on top of an existing 1, and perhaps a .96 when an existing 0 is overwritten with a 1.The main idea to grasp here is that the charge will never be exactly 1 or 0 on the disc itself. It will be different, due to the properties of the magnetic coating on the disc.[6]In this way, data is written to the tracks of the disc. Each time data is written to the disc, it is not written to exactly the same location on the disc.

Some common methods used to gather data from drives which might have very important information to investigations include: Magnetic Force Microscopy (MFM)and magnetic force Scanning Tunneling Microscopy (STM).[7] Other methods and variations exist, but are either classified by governmental intelligence agencies, or are not widely used yet. We will deal with MFM and STM.

4.2 Magnetic force microscopy

MFM is a fairly recent method for imaging magnetic patterns with high resolution and requires hardly any sample preparation.[7] This method uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface of the disc, where it picks up the stray field of the disc. An image of the field at the surface is formed by moving this tip across the surface of the disc and measuring the force (or force gradient) as a function of position. The strength of this interaction is measured by monitoring the position of the cantilever using an optical interferometer or tunneling sensor. In this way, data can be extracted from a drive. The fact that magnetic media contains residual charges from previous data even after being wiped or overwritten several times makes complete data destruction next to impossible.[5]

5 CHALLENGES:

The Recovery of data using part replacement and magnetic recovery methods are now implemented in robust ways and hence the challenges it is facing or the areas where the improvements have to be made are the improvements in efficiency of the steps in the recovery procedure, in most occasions. The challenges are.

• The data can be recovered only if the magnetic platter is not damaged; although Researches are there for improving the part replacement methods there is no active researches that is intended to over come this challenge.

• The recovery is highly complicated in case of some particular ultra hyper-tuned hard disk which has highly customized system area ; Active researches are there to overcome this challenge, besides the manufacturers have also now started designing the drives amenable for recovery.

• The part replacement methods and the magnetic recovery are usually of high-cost.

6.CONCLUSION:

From above discussion, we can say that the data recovery is possible and it is not that much difficult. As we are recovering a data from physical and logical damaging without loosing the content of data.[1]

The recovery data from the logically and/or physically damaged disk drives, and the recovery of over written data is now been done with a good amount of success. The data recovery now have become a handy tool to the end-users as far as the logical damages are concerned, although the recovery of data from the physically damaged drives and over written data, which is done by the magnetic data recovery methods have still to reach at the end users, the data recovery industry has grown through heights of technology, that nowadays the situation is such that, data can be recovered from any physically damaged drive untill it's magnetic platters remain as such.[5] And in case of the magnetic recovery also the present state-of-the-art has contributed alot to the data recover industry that the magnetic recovery had reported recover of data that had been over written upto 17 times. .[4-7]

7.REFERENCES:

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

[2] Bennison, Peter F, and Lasher, Philip J, "Data security issues relating to end of
life equipment", Electronics and the Environment Conference, 2004 IEEE International Symposium on May 10-13, 2004

[3] Cranor, Lorrie Faith, and Geiger, Matthew, "Counter-Forensic Privacy Tools: A
Forensic Evaluation" February 1, 2006

[4] Commonwealth of Australia, "Protecting and handling magnetic media"January
31, 2006

[5] Garfinken, S.L. Shelat, "Remembrance of Data passed: a study of disk sanitiza-
tion",Security and privacy, IEEE International Symposium on February 2003

[6] Joshua J Sawyer, East Carolina University, ”Magnetic Data Recovery The Hid-
den Threat”, infosecwriters, December 2006

[7] L. Gao, L.P. Yue, T. Yokota, et al., ”Focused Ion Beam Milled CoPt Magnetic
Force Microscopy Tips for High Resolution Domain Images, IEEE Transactions on Magnetics, IEEE Volume 40, 2004