Simplifying Data Recovery with Advance Techniques and Operations

[1]Advait Chandsarkar, [2]Suchitra Patil

[1,2]Dept. of IT, KJ Somaiya College of Engineering, Mumbai, Maharashtra, India

Abstract

"Data Recovery" is the process of salvaging data from deleted, formatted, damaged, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often the data salvaging is done from storage media such as internal or external hard disk drives, solid-state drives (SSD), USB flash drive, storage tapes, CDs, DVDs, RAID, and other electronics devices. In Data Recovery different techniques for overcoming logical & Physical errors in storage devices are used. This process may need an extra software and hardware support for accessing, restructuring, repairing the affected storage media for completing data recovery. Few such processes and techniques are discussed in this paper.

Keywords

HeadStack; Firmware; SSD; HDD;RAID; Flash Drive; USB; NAND Chip; TSOP-48

I. Introduction

In this digital era more data being increasingly condensed into smaller and more innovative storage media for paperless transitions. When storage media is working perfectly, but has deleted files, formatted drive, or lost data for some other reason, then this is referred as a "logical" problem in the industry. When storage media has physical errors and some of the mechanical or electrical components of the storage media does not function properly, then this is referred as a "physical" problem in the industry. Various tools and techniques are available for recovering data from such logical & physical errors. These techniques vary with the type of problem in each case.

II. Background

For the average individual, storage media is used to keep photos, notes and other personal effects in data form. Some information can be very important such as scanned images of ID documents, financial records and so on. Hence, a Harddisk/Flash memory crash or similar situation that results in the loss of data could be considered a tragic loss of sentimental and confidential data items. Others might have lost data related to their work or business. In such case, the loss could cause financial problems, issues with the receiver of revenue and stress related to the wastage of work hours spent in collection of data.

Also, there is the data loss associated with government or intelligence services, which influences not only the organization but entire communities or even nations. Such loss can have dire consequences economically, managerially, in terms of governance, socially and even politically. Furthermore, this issue could in some cases result in loss of life, such as in the healthcare system or military branches engaged in active duty.

All in all, information represents the building blocks of modern society in so many ways. For many individuals, business firms, government firms, healthcare institutions, investigation agencies, etc. the above are sufficient reasons to seek out the sought-after help of data recovery experts. Where this is the case, speedyand accurate data recovery services are exceptionally valuable.

III. Techniques for Data Recovery

A. For Logical Errors

1. Deleted/Formatted/Partition Loss

Any Operating System/ file system considers deleted files as just free space on the disk .So there are always chances that these will overwrite the lost files and make their recovery impossible. So the best practice would be to avoid starting the computer with lost files. Instead, disassemble it, disconnect the hard drive with lost files and connect it to another computer as secondary (Write-Blocked if possible) [14].

In any case, avoid installing the data recovery software on the disk that has lost files i.e. subject drive. Do not restore files or write images into the drive that contains deleted files.

It is also a good idea to create an image of the disk with lost files and save it to another disk. For preventing original data from accidental corruption.

There are various open source and license tools for such basic data recovery. Some of the open source tools are Photorec(Windows), Foremost (Linux), etc. Some popular licensed tools are EaseUSDataRecovery, R-studio, Recuva, etc.

In each tool there are prescribed procedures either command line or with GUI to process basic data recovery of Deleted/Formatted/ Lost Partition Cases [1,2,3].

2. RAID Partition Loss

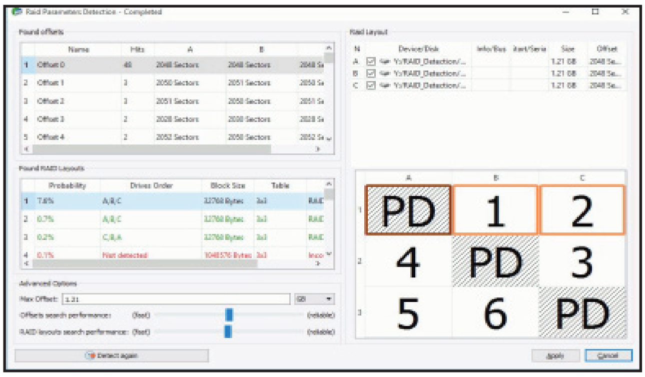
There are various types of RAID Systems configured these days in small/large business firms to increase performance and security of the servers. If such RAID partitions are crashed then processing of recovering data is different than conventional ways.

As a best practice, it is suggested that images of the stripped/ mirror sets of the RAID Array should be taken and numbered in order of their configuration.

For Stripped Sets it is important to check the consistency of parity of the data [3]. If it is ok then reconstruction process is started.

There are various tools for RAID volume set/stripped set/ mirrors recovery such as R-studio, RAID Reconstructor, FreeRaidRecovery, etc.

Fig. 1 Shows RAID parameters detection window in R-studio which ensures the processing is in correct way or not. If it is ok then next procedure is of partition recovery as seen before.



	Name	Hits	A	B	
1	Offset 0	48	2048 Sectors	2048 Sectors	2048 Se
2	Offset 1	3	2050 Sectors	2051 Sectors	2050 Se
3	Offset 2	3	2051 Sectors	2050 Sectors	2051 Se
4	Offset 3	2	2028 Sectors	2030 Sectors	2028 Se
5	Offset 4	2	2052 Sectors	2050 Sectors	2052 Se

N	Device/Disk	Info/Bus	Ident/Serial	Size	Offset
A	☑ Y:\RAID_Detection\...			1.21 GB	2048 Se...
B	☑ Y:\RAID_Detection\...			1.21 GB	2048 Se...
C	☑ Y:\RAID_Detection\...			1.21 GB	2048 Se...

	Probability	Drives Order	Block Size	Table	
1	7.6%	A,B,C	32768 Bytes	3x3	RAID
2	0.7%	A,B,C	32768 Bytes	3x3	RAID
3	0.2%	C,B,A	32768 Bytes	3x3	RAID
4	0.1%	Not detected	1048576 Bytes	3x3	Inco

Max Offset: 1.21 GB

Offsets search performance: (fast) (reliable)

RAID layouts search performance: (fast) (reliable)

	A	B	C
1	PD	1	2
2	4	PD	3
3	5	6	PD

Fig. 1: RAID Parameters Detection Window

3. Forensic Evidence Recovery

Digital Forensics is used to discover, recover, monitor or detect relevant information in order to analyze, inspect or resolve a wide range of computer crimes and misuses. The relevance of the inspected data can lead to termination of employment, arrests, preventing future similar activity and even prosecutions, depending on the act severity. Hence, it is important to have proper proof of the performed analysis while recovering evidences and reporting the evidences.

Mostly these evidences can be found in swap files, registry, volume slack, file slack, ram slack, unallocated area, etc.

The best practice is to always image the storage drive and work on forensic image for evidence recovery. For recovering such data (evidences) digital forensics tools like Encase, FTK, Winhex, etc are used. Processes like keyword search, binary search, damaged file carving, specific file type recovering, emails recovering, etc is done using these digital forensic tools [4,5,10,11].

4. Encrypted Data Recovery

Data/Device/Drive is encrypted either manually, accidently or by some attacks of malwares. To recover the useful data it is needed to have password or key to decrypt it. For recovery passwords, licensed tools like Passware kit, Elcomsoft's Passware or open source brute-force tools can be used. These process takes lots of time and logical creativity to execute correct dictionary attacks on encrypted data.

Normally the forgotten password/keys are found after carefully processing the manuals. But it is hardly possible if there is an attack made from ransomware/malware.

B. For Physical Errors

1. Head Stack Replacement

Two most important things needed in head stack replacement are cleanness and correct donor [7].

The donor is a hard disk drive head stack which is used to replace a damaged one in the original drive. The general requirements for choosing donors are: an absolutely identical to the recipient model type of the camera, identical spindle control, VCM chips and read/write channel chips. Besides that, for every manufacturer and for many drive series there are specific requirements for the donor selection given in Guide [13].

There are different ways to achieve cleanness. The most optimal way is to get or make a "clean chamber". Everything depends mostly on one's financial abilities, however, the successful rate of data recovery procedures depends exactly on a cleanness factor. Fig. 2 shows head stack placed at platters of hard disk.

The complete steps with the comb types required for hard disk, are given in online guide [13]. It is important to know the internal structure of hard disk before opening it, otherwise, slight mistake in opening screws or opening lid can damage the platters.

If there is only one head no worries, but if there is more than one then paired heads in the block can stick together. To prevent this Combs are used to store Head stack. Curved Plastic tweezers are used to pack access of heads.

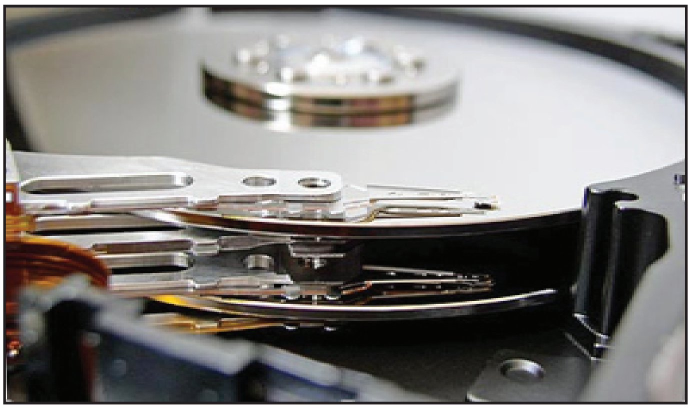


Fig. 2: Head Stack Connected to Platters of hdd

Hence, the heads are moved out and packed. Then the screw that holds the axis of a head stack is released carefully by moving directly up. The same procedure is done for to donor to get a set of good heads which should be used in recipient drive.

Next step is loading heads on the surface. That is actually the most difficult part and should be done carefully with given set of tools. After this the total assembly with magnet is again reconnected carefully.

If everything is done correctly and with decent accuracy then the drive will recalibrate, be detected, and data is rescued. Fig.3 shows replacing head stack and loading of heads on the surface of platters.

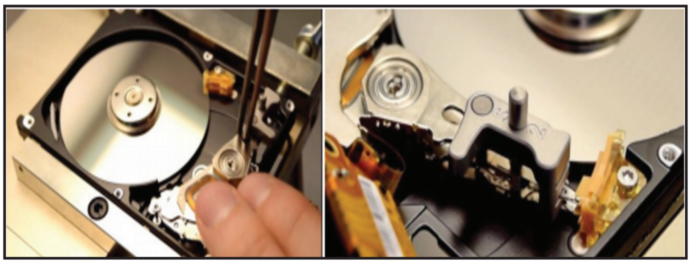


Fig. 3: Replacing stack and Loading Heads.

2. Platter Swapping

Platter swapping also needs cleanness and correct donor. The procedure is similar that of Head stack replacement upto the magnet removal and connecting security pin to the Head stack assembly to stick it to the inner wall of hard disk [7, 13].

Then as shown in Fig. 4 the Platter Extraction tool is used to carefully take out the platters from Hardisks. For the best practices, a pair of extraction tools is used at a time to take out the platters of both donor and recipient at a time and replace simultaneously. Though very carefully for the platters with required data.

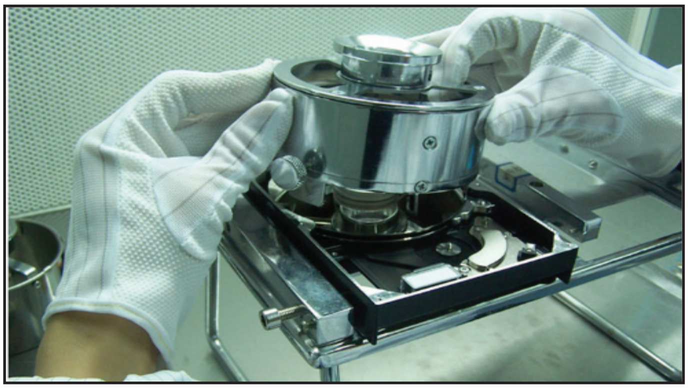


Fig. 4: Platter Extraction Tool

3. Modules/Firmware/SA issue in Harddisk

Sometimes the harddisk become inaccessible due to firmware/modules corruption problem, Service Area problem, Slow responding problem, etc. and sometimes harddisk is accessible but not allowing to access data due to Weak Heads.

In such cases, there is no need for Advance Dust free Lab techniques like head replacement or platter swapping because these are costly for average user.

So for above cases, Advance Data recovery tools like PC3000UDMA, EDR Tools' FLAME, MRT PRO are used to repair the firmware, modules, SA (Service area) issues and calibrate weak-head issue by selecting working heads only.

Fig.5 shows workflow model of these tools. E.g. PC3000 UDMA has 2 sections Utility and Data extractor. The repairing of firmware/modules errors is done as per the manual of every company of Harddisk. Mostly the 3rd port on harddisk i.e. Terminal is used to communicate with harddisk PCB. There are a number of errors for various models of Harddisk. The commands and utility functions are different for every model.

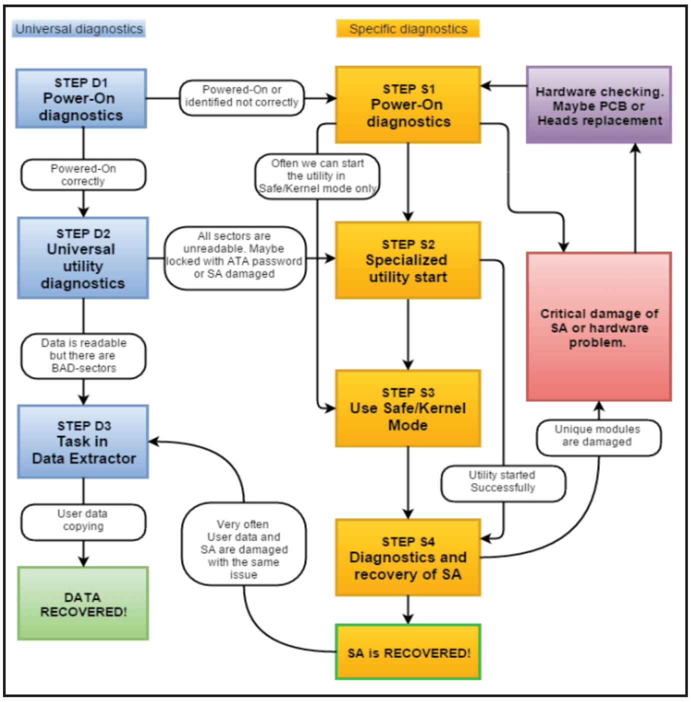

Universal diagnostics
Specific diagnostics
STEP D1 Power-On diagnostics
Powered-On or identified not correctly
STEP S1 Power-On diagnostics
Hardware checking. Maybe PCB or Heads replacement
Powered-On correctly
Often we can start the utility in Safe/Kernel mode only
STEP D2 Universal utility diagnostics
All sectors are unreadable. Maybe locked with ATA password or SA damaged
STEP S2 Specialized utility start
Critical damage of SA or hardware problem.
Data is readable but there are BAD-sectors
STEP S3 Use Safe/Kernel Mode
Unique modules are damaged
STEP D3 Task in Data Extractor
Utility started Successfully
User data copying
Very often User data and SA are damaged with the same issue
STEP S4 Diagnostics and recovery of SA
DATA RECOVERED!
SA is RECOVERED!

Fig. 5: Workflow Diagram

For Head weak problem, the other working heads can be selected and data available from them can be extracted. The selection of heads is done in Utility [6]. In all the above issues, the data recovery is done in data extractor.

As a best practices, imaging of the drive should be done first in the data extractor and then recovery should be done from the available image.

All these steps are well briefed in Fig. 5 [6].

4. Inaccessible SSD/NAND Chip/MMC Flash card:

Previously memory cards like SD,Memory-Stick, MMC and pen drives, contained a very simple classic structure with separated parts.controller, a PCB and a NAND memory chip in the TSOP-48 or LGA-52 package. In such cases, the full process of recovery was very simple to take out NAND chip and connect it to dedicated Data recovery tool [9,12].

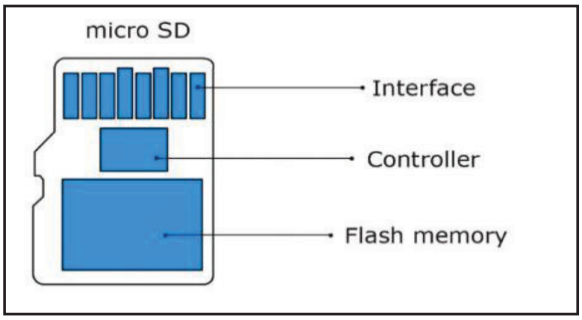


Fig. 6: Structure of Memory Chip

Modern NAND flash devices use a new type of architecture, where the interface, the controller and memory chips are integrated into a Monolithic structure. Fig. 6 shows the structure of Micro SD card. For recovery, the complete process of monolithic device soldering is complicated and requires good soldering skills and special equipment. First, the layer of ceramic from the bottom side should be removed using sand paper very carefully. This operation requires some time, if the pinout layer gets slightly damaged then data recovery becomes impossible [8].

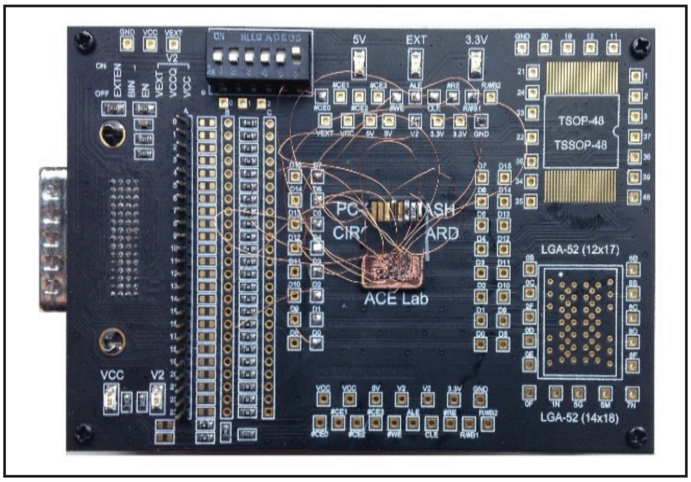


Fig. 7: MicroSD connected to Circuit Board

This Monolith is connected to Circuit board as shown in fig. 7 with the help of various Pin-out diagrams provided for soldering circuit points. The circuit board then connected to computer using flash dedicated recovery tools like PC3000FLASH, EDR Tools, etc to recover the files. If the connections are correctly done and no damage is done on memory chip then the data can be extracted.

IV. Data Recovery Myths and Facts

A. Myth: The Platters of the hard drive can be removed from one hard drive and read inside another drive easily.

Fact: Replacing the platters of Hard Disk is a difficult process. It becomes more difficult in today's multi-platter drives. Any person trying this may jeopardize the possibility of any recovery. Accurate donor drive should be selected and process requires dust free environment.

B) Myth: Heating, Freezing, Hitting, dropping is helpful in rejuvenating the storage media.

Fact: If the problem is Head stuck at the start of platter then hitting the hard drive has helped some users with very low success rate. But mostly these things makes the hard drive more defective and hence recovery harder or impossible.

C) Myth: Physical problems in a hard drive or MMC card can be fixed by software.
Fact: If the storage media has physical problem then its appropriate surgery is needed to gain the access again. These operation requires software as well as hardware for analysis and repairing operations to access hard drives.

D) Myth: Hard Drive becomes dead when its spindle motor fails to work.
Fact: The spindle motor only stops after there is another problem associated with PCB or Head. Spindle Motor in 99.9% cases works well and physically it is the last thing to get malfunctioned in the hard drive.

E) Myth: Any deleted data can be recovered.
Fact: If data is not overwritten after deleting then only it can be recovered. Recovery of overwritten data is hardly possible. Also if the platters of hdd are improperly handled, then the data recovery becomes impossible.

F) Myth: Replacing the Hard disk's logic board (PCB) with an equal one from a hard drive in working condition in order to revive a dead one.
Fact: This is the most sensible myth. The replacement of the PCB works in some cases where the problems are related to circuit elements and the information like firmware and modules is completely stored in the controller IC or bios.

G) Myth: RAID Servers are most robust storages.
Fact: The storage hard drives are same whether it is RAID or normal PC. Only difference is that RAID storage systems are more secure than conventional storages. As it gives redundancy and backup with respect to their designs. But HDD functionality checkups in regular intervals are required otherwise RAID servers also face many inaccessibility issues.

IV. Future Developments

The increasing demand for higher storage capacity of hard drives will approximately increase the storage density 4 times in next generation hard SATA drives. It will become more challenging to rescue data especially in physical problems.

It is also predicted that Solid State Drive (SSD) will replace 2.5inch hard disk drives in laptops soon. SSD is more robust, gives high speed and performance compared to hard disk drive (HDD). It is observed that SSDs coming under physical problems are also tough to recover from. Hence, more advance NAND flash recovery tools are needed in future.

World has seen malware attacks like Ransomware encrypts the user data where recovery is hardly possible. Such attacks will get more advance in the futurewith respect to their magnitude and technique. Hence, Advance Data Security and Backup Plans are required by both enterprise and household users.
The data recovery tools will get advanced increasing their reach to analyze proprietary file systems used in CCTV or other audio-video recording devices. This will make easier to recover such files. The new technological era will require data recovery from IOT (Internet of Things), Cloud Storages, smartphone memory, etc. It will be important to analyze the file systems used in IOT, Volume of the array in Cloud Storage, and the technology of integration of phone memory chip on Smartphones.

VI. Conclusion

Data Recovery from both physical and logical problems in storage devices, requires careful handling of these devices before deciding recovery procedures for every issue. Recovering data in logical problems can be done using software (freeware/shareware) only. For solving physical issues software equipped with hardware tools are needed.
In logical issues, it is better to take image of the disk and work on the disk image. Though in physical problem use of damaged storage device can't be avoided. Hence, it is more sensitive data recovery and should be done with accurate procedure and required precaution. In physical issues always try to repair the service area modules and firmware issues of the disk before opening or scratching the storage devices.
It requires more time to analyze new technologies like Smartphones, IOT, Next Generation HDD/SSD, Cloud/Server Arrays, etc. for data recovery operations.

References

[1] Photorec Tutorial [Online]. Available: http://www.cgsecurity.org/wiki/PhotoRec_Step_By_Step
[2] Foremost-Scalpel Tutorial [Online]. Available: https://help.ubuntu.com/community/DataRecovery#Foremost
[3] R-studio Recovery Manual [Online]. Available: http://r-studio.com/downloads/Recovery_Manual.pdf
[4] Guidance Softwares' Encase v7.10 User Guide 2014.
[5] X-ways Solutions' Winhex Manual 2016[Online]. Available: http://www.x-ways.net/winhex/manual.pdf
[6] Ace Labs PC3000 UDMA Utility and Data Extractor Manuals.
[7] Changing Head Stack Tutorial [Online]. Available: http://hddguru.com/articles/2006.02.17-Changing-headstack-Q-and-A/
[8] PC300 Flash Monolith extraction [Online]. Available: http://blog.acelaboratory.com/pc-3000-flash-circuit-board-and-msd-card-preparing-and-soldering.html
[9] Virtual NAND Re-constructor [Online]. Available: http://rusolut.com/visual-nand-reconstructor/vnr-software/
[10] Bora Park, Antonio Savoldi, Paolo Gubian, Jungheum Park, SeokHee Lee, Sangjin Lee,"Recovery of Damaged Compressed Files for Digital Forensic Purposes," Multimedia and Ubiquitous Engineering, 2008. MUE 2008. International Conference, pp. 365 - 372.
[11] S. Lee, A. Savoldi, S. Lee, J. Lim, "Password Recovery Using an Evidence Collection Tool and Countermeasures," Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on, Kaohsiung, 2007, pp. 97-102.
[12] B.J.Philips, C.D.Schmidt, D.R.Kelly,"Recovering data from USB Flash memory sticks that have been damaged or electronically erased," e-Forensics-Forensic Applications and Techniques in Telecommunications, Information, and Multimedia.
[13] Guide for Head Change tools [Online]. Available: hddsurgery.com/pdfs/samtshbfinal.pdf
[14] Software/Hardware Write Blockers [Online]. Available: forensicswiki.org/wiki/Write_Blockers

Mr. Advait Chandsarkar is currently pursuing M.Tech Information Security from K.J. Somaiya College of Engineering, Vidyavihar, Mumbai. He is working as Digital Forensics Analyst and has expertise in Data Recovery. He received his BE (Electronics) from SSVPS's BSD College of Engineering, Dhule. His research interests include Digital Forensics, File Systems, Information Security, etc.

Ms. Suchitra M. Patil has received B.E. (Computer Science and Engineering) degree from Visveshwaraiah Technological University, Belgaum in 2004. She is working as lecturer in K. J. Somaiya College of Engineering, Mumbai and has teaching experience of more than 10 years. She is currently pursuing M. E. from Thadomal Shahani Engineering College, Mumbai. Her areas of interest are Image processing, Database Systems, Data mining and Web Engineering.