BOOK CHAPTER | *"Total recall""*

Deleted Data Recovery Mechanisms

Ephraim Mawutor Adehenu
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: duaidangelo@gmail.com
Phone: +233274750660

ABSTRACT

According to a survey, 90% of all information never leaves the digital form. The fundamental importance of data preservation is quite clear, as a small inattentive move could lead to a loss of pertinent data which could inform a major decision. The majority of information these days is being created, modified, and consumed entirely in digital form. This means most spreadsheets, digital snapshots and databases will never make it onto paper. It is common to lose data due to storage errors or low performance. If this happens, the user/owner may want to quickly recover the files if the data is really important and if it is possible to retrieve the lost data. In this article, we look at ways data can be lost through deletion, recovery procedures and mechanisms, and recommendations to secure data against such events. (3)

Keywords: Deleted, Lost Data, Data Preservation, Security, Digital Data Forensics, Data Recovery Mechanism

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Ephraim Mawutor Adehenu (2022): Deleted Data Recovery Mechanism
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 363-372
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P58

1. INTRODUCTION

Operating systems provide commands to remove data from a hard disk or other media, such as menu items or commands used from a Command Prompt. When a file gets deleted using the Del key or commands in compliant programs, it is generally sent to the Recycle Bin. When this occurs, the user can recover the file. If the file is emptied from the Recycle Bin or deleted using other methods, one may need to use tools to recover the file. (2) Even if an entire partition is deleted, and the volume is formatted, this doesn't mean the data is gone. Data recovery and computer forensic tools may still be able to retrieve the data from a system. Although many data recovery tools are available on the market, not all of them should be used for computer forensics. What makes a device unique and valuable is its data. Losing that could be a nightmare, so it comes down to whether we are ready to deal with accidental information loss.

2. PREVIOUS WORKS

Overwriting of digital data can be defined as obliteration of evidence in digital world. In order to deal with the variations of digital evidences in situations it is necessary to have a variety of tools and not to rely on any single technology or methodology.

Guttmann P. (2006) (12) in his research claims that the Guttmann method uses three different algorithms to overwrite files with 35 passes of the hard disk, making it impossible to be retrieved back by any data recovery software.

Farrell (2009) (7) suggests tools that perform specific functions are constantly being developed and distributed in the academic and open source communities and these new functions are ultimately integrated into larger analysis suites. These suites can be large GUI - based programs that allow an analyst to explore data on a hard drive.

Medlin (2011) (8)suggested that, many of the hard drives built after 2001 have a built-in program for securely erasing data, entitled Secure Erase. The program can be accessed through a series of commands embedded in the hard drive. Additionally, this program works by overwriting every track on the hard drive. Most areas not touched by a simple deletion include bad blocks, directory structure, tracks not touched by the operating system, and unformatted sections of the disk, all of which can be touched by this embedded hard disk utility.

Sindhu et al. (2012) (11) in his research has clearly stated that digital information is highly fragile and can be easily modified and destroyed by data tampering. He explained that such possible tampering can be detected by using open source tools like Win-Hex.

Sansurooah et al. (2013) (10)claims simply deleting the data in question or formatting the storage device is not enough to ensure that the data cannot be recovered. In his studies he has successfully drawn a line of comparison between erasing software both commercial and open source and made an opinion that open source erasing software are very efficient in deleting the data on USB drives through repetitive overwriting.

Panchal (2013) (9) emphasized that overwriting might be caused by a variety of user activities, such as adding a new program or creating new documents that happen to be written to the space where the "deleted" files exist. It is only when the data is overwritten by new data that part or all of the files are no longer retrievable using forensic techniques.

3. RESEARCH FINDINGS

Digital technologies have penetrated deep into every aspect of our day to-day lives. This intrusion is continuously creating voluminous amounts of confidential and sensitive information residing in the hierarchy of directories and files. Users employ the file deletion operation provided by all operating systems when they no longer need some information, or want to remove every trace of it. However, the sensitive and confidential information that was deleted, in the belief that the information has been physically erased, can be recovered even by a novice hacker. For example, on Linux, using the /dev interface, a non-root user has access to block devices and, as such, can use various data recovery software tools to recover the information. (1)

A number of incidents arising from study into this issue gives us an idea of the problem - there are numerous ways in which we can lose data, not just by deletion. Many studies have been published in an ongoing research being conducted into the types of information that remain on computer hard disks that have been offered for sale on the secondhand market, revealing that over a period of five years there were clear indications that the number of disks that contain information relating to organizations and individuals is reducing. Unfortunately, we can agree that due to the increasing volume of storage capacity of the disk, the quantity of **non-sanitized data** – data that is not securely wiped from storage before being handed over as a secondhand device, appears to be increasing. We therefore need to ensure sanitization of storage devices properly before handing over to the secondhand market.

There are generally **two ways to securely delete data** – **encryption and wiping**. Encryption employs various techniques to encrypt data before it is stored on storage media and decrypt it on its retrieval. Wiping overwrites the metadata and user data of a file during deletion with some random values or zeros. In its simplest form, the file system or storage media can be wiped in its entirety and the process can be accomplished in both the user and kernel mode of an operating system, or assisted at hardware level. Magnetic disks can also be degaussed (destroyed). **(13)**

Deleted Data

One way to lose data is a hardware fault. This can be due to bad blocks, a damaged controller, or another bad component. Of course, in such cases, data is either gone or could be lost easily. Once a medium is faulty, storing any information on it becomes risky or impossible. Messing with it can cause problems such as invalid files, inaccessible valid files, a system unable to boot, impossible mounting or recognition of filesystems, and other unexpected behavior. Recovery of the data from a formatted hard drive depends upon a lot of parameters. Information from the formatted hard drive may be recoverable either using data carving technology or by using commercial data recovery tools. There are two possible ways to format a hard drive: **Full Format and Quick Format.**

Full Format – As the name suggests, this initializes the disk by creating the new file system on the partition being formatted and also checks the disk for the bad sectors. A full format operation will: Wipe the disk clean, Write zeroes onto the disk – write empty data onto the disk to prove the success of the format process Read the sectors back to ensure reliability.

Quick Format – This is never destructive except for the case of SSD. Disk format simply initializes the disk by creating the new file system on the partition being formatted. Information from disks cleared using a quick format method can be recovered by using one of the data recovery tools that support data carving. **(13)**

Data Recovery

Data recovery is the process of retrieving data from a storage medium that, for some reason, cannot be accessed normally. This process may be used to recover data from a variety of storage media, such as: hard disk drives, solid-state drives, other flash storage, mobile devices, or disk storage. The damage that causes data to be lost can be as a result of damaged or malfunctioning storage media - personal data recovery, or a software and/or file system preventing the data from being accessed by the host operating system or purposely encrypted or hidden to prevent others from accessing the data - forensic data recovery. **(2).**

Data comes in many forms. They can be audio files, and voice recordings, address books and contact lists, clickstreams, call and SMS history, backups to various programs, including backups to mobile devices, browser history, cookies, databases, event attendance, compressed archives (ZIP, RAR, etc.) including encrypted archives, etc. and can be stored on as many media as possible. Avenues for losing data are also very common. It can be more or less highly possible depending upon the following conditions:

- Deliberate action is taken to delete the data.
- Urgency of the situation
- Type of storage device like magnetic hard drive, flash memory card, or SSD drive.
- Criminal intent – holding data for ransom

Some scenarios where data recovery procedures would be necessary are:

1. There has been an operating system failure or some critical operating system files have been damaged, causing the device to not be able to boot up properly.
2. There has been a hard disk failure and there is physical damage to the storage medium This will often require the services of a specialized data recovery company
3. Files have been deleted from a storage medium. When an operating system "deletes" files, often times the data is not immediately removed from the drive. (4)

Data Recovery Process

For most operating systems, when a file is deleted on a hard disk drive, the contents of the file are not immediately removed from the drive. Instead, to improve performance, they simply remove references to the file in the directory structure and mark the space that they occupy as available so that other data can be written to it later. This means that the original data remains on the disk and may be recoverable using specialized tools. A standard process for recovering data, in any situation can have steps as outlined below:

Repair any damaged hardware of storage device. Repair the hard drive so that it is running in some form. This usually involves replacing malfunctioning or damaged parts.

Image the drive to a new drive or a disk image file. It is important that no other data is written to the damaged drive before it can be imaged, to avoid overwriting the data you are trying to salvage.

Logical recovery of data - After the drive has been imaged, the original data can be retrieved using software such as a file carver. We can also attempt to repair the file system using certain tools.

Repair the recovered files - In the event that some files are damaged, you may need to use some software to try and reconstruct the data using, for example, a hex editor (12)

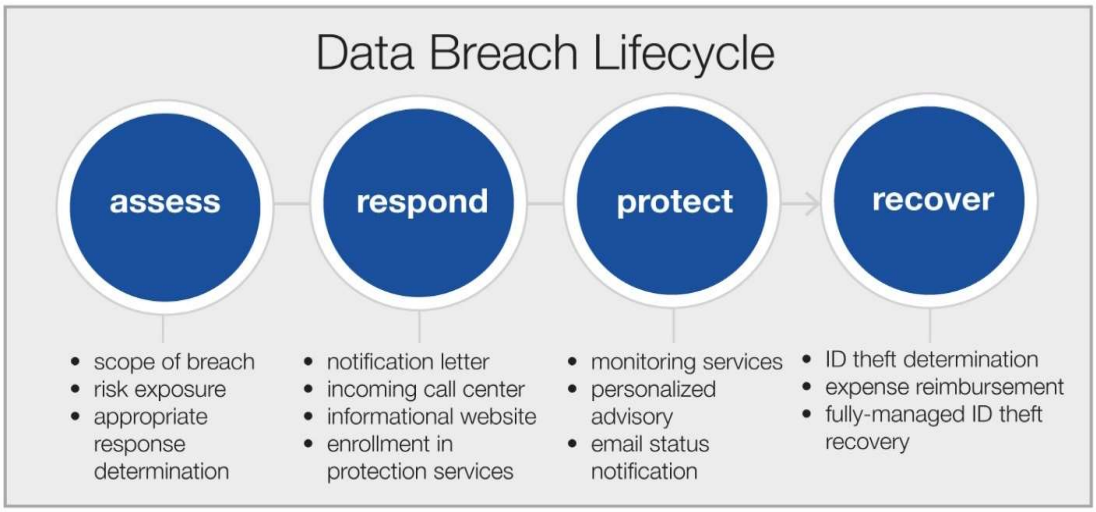

Fig 1: Lifecycle For Data Breach

The image above (17)illustrates an easily understandable lifecycle for data breach – when data gets lost due to deliberate or criminal intent, outlining a comprehensive approach to responding to data breach events that alleviates legal liability, manages public perception, and protects and restores individuals' identities from identity theft.

Data Recovery Tools and Techniques

If deleted files have no trace in the recycle bin like in case of the "Shift + Delete" command, then, in that case, you can use commercial recovery tools to recover the deleted evidence. One such example commercial tool is Disk Internals Partition Recovery. This kind of software looks for characteristic signatures of known file types by analyzing the file system and/or scanning the entire hard drive, one can successfully recover files that were deleted by the user, temporary copies of Office documents, temporary files saved by many applications, and renamed files. Information stored in deleted files can be supplemented with data collected from other sources. For example, the "chatsync" folder in Skype stores the internal data that may contain chunks and bits of user conversations. There is a possibility to recover user chat's even if the Skype database is deleted with tools like Belkasoft Evidence Center 2020.

A simple technique to regain access to data that is on a storage media that won't boot (due to, for example, logical damage to the operating system) is to mount it to another computer, or use a Live USB/CD to boot another operating system on the machine. Another solution is to use a tool such as Testdisk to try and recover lost partitions and/or make nonbooting disks bootable again. There are also a number of closed-source and/or commercial software solutions for data recovery, as well as some non-commercial and/or open-source tools. (5) A popular tool to look at is called PhotoRec (4)- a free and open-source file carving tool designed to recover lost files. It can recover data from all known storage media It recovers most common photo formats, audio files, videos, document formats, and archive formats. In all, it recognizes over 440 file extensions. It's a multi-platform tool, compatible with all known operating systems. (13)

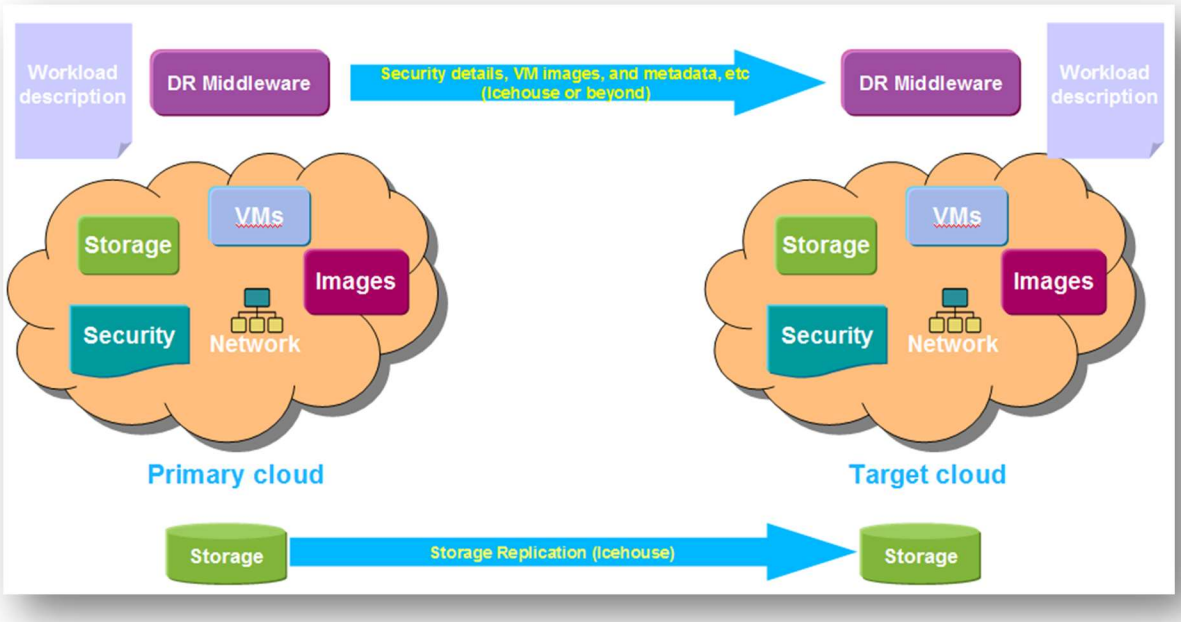

Fig 3: Data Recovery Open Stack
Source: https://wiki.openstack.org/wiki/DisasterRecovery

Bootable Toolsets
Operating Systems often run from the same device we may be trying to retrieve the data from, so we can't use any tools within our environment. To that end, there are packaged images, which contain rescue toolsets reinstalled in a bootable environment:

- Trinity Rescue Kit, a Linux environment primarily oriented towards Windows recovery
- Hiren's Boot CD, a universal Windows portable environment with lots of tools
- Ultimate Boot CD
- System Rescue, a Linux system rescue toolkit.

Using these is as easy as getting the image, writing it to a medium, and booting from that medium. Indeed, not booting from a device with lost or damaged data drastically increases the chances of restoring it.

Data Carving - bit-precise and sequential examination of the entire content of the hard drive. Carving allows identifying particular signatures or patterns that may give a clue that some interesting data can be stored in a particular spot on the disk, locating various artifacts that would not be available otherwise. It is one of the best ways for forensic investigators to determine root causes of data loss. **(2)**

4. SHORTCOMINGS FROM STUDY

The dilemma being faced by professionals upon research into this field appears to be in the **procedures** involved in analyzing what constitutes data loss, data recovery/retrieval, human resource – professional forensics **experts**, and the tools used for the work. The mechanisms for data recovery have gradually become obsolete and there are no new updates because people currently have no interest in the field – no need to retrieve what is lost. There have been arguments made for using open source software as a mechanism to assess reliability of digital evidence by pointing out the dangers imposed by proprietary forensic software - which leave behind distinctive features (digital fingerprints).

5 . IMPLICATIONS OF DATA RECOVERY SOLUTIONS ON THE CYBER SAFETY OF AFRICA

Enforcement of data compliance rules

The key to compliance - training and education. Core training areas should revolve around how to seek, record and manage information. Data compliance deals with data control issues like:

Transparency about how to collect, use and share data concerning an entity, the responsibility that requires companies to be good stewards of information

Strong enforcement through a strong central regulator and vigilant law offices that have the authority to enforce the laws governing investigations into the root cause of data loss, take actions to hold violators accountable when the cause is determined to be malicious. **(15)**

Regular data backups - Data backup can be seen as the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Cybersecurity laws require data to be available at all times, therefore we need innovative solutions to ensure that data is backed up to reflect the live data. Consider undertaking regular backup tests to contribute to the effectiveness of backups. **(14) (16)**

Equipping digital forensics professionals with up-to-date knowledge and skills can affect the entire region through. A standard for best practices would be a Cyber Security certification for acceptance into the field.

There will come an important need for legal controls over the flow of data in Africa, while the potential need to control the flow of data for privacy purposes can be made clear for ease of traceability and recovery. Technology developments, such as cloud services, are making data recovery even more feasible worldwide than we used to know.

6. RECOMMENDATIONS AND FUTURE TRENDS

Here are some guidelines to follow when attempting to mitigate the impact of data loss and/or protect against data loss, to ensure **Confidentiality, Integrity, and Availability** is either maintained or restored.

1. **Use data recovery tools and techniques to retrieve lost data** - In the case of an emergency, where data has already been lost, this allows the user to restore **availability** since you regain access to lost data.
2. **Encrypt sensitive data to maintain confidentiality** - Always encrypting sensitive/confidential data beforehand ensures that **Confidentiality** is maintained in the event of any data loss, since an attacker cannot access your real data without decrypting it.
3. **Use a RAID configuration for data redundancy** - Using a RAID configuration with your system allows you to maintain Integrity by having multiple copies of data across multiple drives. This provides a way to check for data consistency and ensure that **Integrity** remains intact.
4. **Keep computer security in mind (and/or use antivirus software)** - Maintain **Integrity** by avoiding suspicious links and programs that may be malicious. Such malicious software could cause logical damage to the storage medium, putting Integrity at risk.
5. **Regularly backup your data to external storage** - Having recent offline/external backups of your data will allow you easily restore your data in the event of physical or logical damage, restoring **availability**.
6. **Protect against physical damage** - Many instances of physical damage can be prevented by using the correct hardware and/or software. Protecting against physical damage therefore maintains **availability**, since you maintain access to the files, as well as **Integrity**, since you know they have not been damaged or modified. (1) (5)
7. **Leverage the cloud** - The advent of cloud technology provides a lot of protection against deletion in the form of automated cloud backups of local data.
8. **Use MFA delete to protect from accidental deletion** - Third party applications can provide individuals with multi factor authentication. This way data cannot be lost without authentication from data owner and careful observation
9. **Use data and file versioning** – this technology also provides safety as every change to a file or data gets saved remotely and logged. This way we can keep track of all changes made to pertinent data while saving each change to a separate file synchronously.

Although it is possible to recover data after losing it, there are certain factors that affect the chances of successful file recovery. It is recommended that you take certain precautions.

1. **Do not write new data once the drive is formatted** - As mentioned in this article, formatting a hard drive does not permanently erase data. Instead, that data is moved to somewhere you cannot find by yourself. If you write new data, then it overwrites those sectors that contain deleted files.
2. **Do not install software on the drive** - Installing the data recovery software on the same hard drive you wish to recover data from reduces the chances of recovery.
3. **Keep a backup of your data on a regular basis** - It is because the backup of your important data will help you to keep from any problematic situation and you will always have an option to recover your replaced file from backup.

4. **Keep your antivirus software updated** and do not forget to scan your device for viruses on a regular basis.
5. Always **shut down your computer in a proper** way. Avoid being in a hurry and just put your laptop's screen down.
6. **Do not download applications** from any unauthorized source because these can harm your device. **(2)**

7. CONCLUSION

This research draws from a fragmented and disparate set of sources to present digital forensic examiners a more complete view of the deleted data recovery mechanisms in general. In using this information to analyze how deleted data is recovered, we discover that deleted information is recoverable if it has not been overwritten, though it may not be entirely trustworthy. All platforms behave quite similarly and hence can be considered when designing solutions to protect individuals from losing their data through whatever means.

REFERENCES

1. Keith Brown - What Is A Security Descriptor. pluralsight.com (2005) Available from: http://www.pluralsight.com/wiki/default.aspx/Keith.GuideBook/WhatIsASecurityDescriptor.html [ported 18.01.2005, accessed 09.03.08] Google Scholar
2. Gerganov, Hiks recover lost and deleted data in linux - Last modified: February 9, 2022 available from: https://www.baeldung.com/linux/recover-lost-deleted-data.
3. Recovering Deleted Digital Evidence Last updated: 23 Feb, 2022. Available from: https://www.geeksforgeeks.org/recovering-deleted-digital-evidence/
4. AnyRecover Data Recovery - How to Recover Data from Crashed Internal Hard Disk? Available from https://anyrecover.medium.com/fixed-how-to-recover-data-from-crashed-internal-hard-disk-2afa46eca78f accessed - Dec 24, 2020
5. ZHAO, Z.Y. and HUANG, S.H., 2011. Forensic Analysis of Windows Deleted Files. Netinfo Security. https://www.sciencedirect.com/science/article/p2/S1742287608000303
6. Bhat, W. A., & Quadri, S. M. K. (2012). After-deletion data recovery: myths and solutions. Computer Fraud & Security, 2012(4), 17–20. doi:10.1016/s1361- 3723(12)70032-5
7. Farrell, P. (2009) "A framework for Automated Digital Forensic Reporting" Available at: http://cisr.nps.edu/downloads/theses/09thesis_farrell.pdf
8. Medlin, B. Dawn (2011). "A Study of Hard Drive Forensics on Consumers' PCs: Data Recovery and Exploitation." Journal of Management Policy and Practice vol. 12(1)
9. Panchal, Esan P. (2013), "Extraction of Persistence and Volatile Forensics Evidences from Computer System," International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 5–May 2013, available at: http://www.ijcttjournal.org
10. Sansurooah. K, Hope. H, Almutairi. H, Alnazawi. F, Jiang. Y (2013), "An investigation into the efficiency of forensic data erasure tools for removable USB flash memory storage devices", originally published in the Proceedings of the 11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013, available at http://ro.ecu.edu.au/adf/127
11. Sindhu. K. K, Shweta Tripathi, Dr. B.B. Meshram (2012) "Digital Forensic Investigation on File System and Database Tampering", IOSR Journal of Engineering (IOSRJEN) - Vol. 2 Issue 2-Feb.2012, pp.214- 221, available at: http://www.iosrjen.org
12. Guttmann, P. (2006). "Secure Deletion of Data from Magnetic and Solid-State Memory." In Proceedings of the 6th USENIX Security Symposium, San Jose, California, U.S.A.

13. https://www.coursehero.com/file/116603227/Data-Recoverypdf/
14. https://www.linkedin.com/pulse/six-implications-data-protection-afcfta-agreement-adedoyin/
15. https://blogs.microsoft.com/on-the-issues/2020/10/16/privacy-laws-open-data-economic-recovery/
16. https://www.backup-systems.co.uk/6-gdpr-implications-on-data-backup-and-disaster-recovery/
17. http://idsafeguards.blogspot.com/