## Research Topic:

### FORENSICS WITH NTFS: DEPTH OF DATA RECOVERY AND DELETION

## ABSTRACT

This technical research on NTFS shows the affecting sections of data deletion and recovery of the file in the NTFS file system, this comprehensive research focuses on the behavior or working of the file system on top of that we will consider some pointers as to what happens when files or folders get deleted from the system or files gets empty from the recycle bin, at last, what happens after the metadata is overwritten. These important aspects of data deletion and how these files and folders can be recovered will be outlined in this paper with a technical overview of findings where we will focus on general steps of locating deleted files in FTK imager using some example evidence for better understanding.

## INTRODUCTION

The greater expansion of technology requires advanced processing tools to access data and transforms the way to store it, this substantial breakthrough introduces the digital storage systems, now the release of the NTFS file system along with Windows plays an efficient role by indulging greater performance, credibility, and compatibility over it one of the predecessors FAT file system, as this filed of digital storage system grows the negative side of this environment also gets bigger with potential cybercrime significances which require tools and procedures for data recovery and forensic investigations.

There remain significant challenges in data recovery, particularly with NTFS file systems, despite advances in data recovery techniques. In addition, detecting the origin directory of deleted files further complicates the recovery process. NTFS is difficult to recover deleted files, particularly non-resident, compressed, or encrypted files.

This research will focus on these challenges and propose the relevant solutions or techniques to recover data by integrating various recovery methods within a single framework. The whole research is to scrutinize MFT (Master File Table) entries within the NTFS file system and gather relevant observations to support our research, MFT also helps in the identification of deleted files and is one of the stages of file storing after deletion from the NTFS-enabled system this paper will show the proposed recovery methods and identification of deleted files.

## METHODOLOGY

**NTFS (New Technology File System) – Windows-Based File System**

The New Technology File System (NTFS) is the default file system for Windows operating systems developed by Microsoft, introduced with the release of Windows NT 3.1 in 1993. NTFS is robust and more efficient beating up its predecessor, the FAT (File Allocation Table) file system, and provides greater support for advanced computing environments. One of the strengths of the NTFS file system is the management of large-scale files and the storage of enormous data, as it is essential for the handling of big data and high-performance computing*(Kai, En and Qinquan, 2010)*.

When it comes to computer forensics, NTFS is essential for recovering destroyed information. Data in those Hard drives using the NTFS file system are not completely erased or destroyed by the system it goes through multiple stages. Rather, it assigns the values to the area where old files or deleted files exist as free or inactive so that when a new file requires space on the disk it will assign that space area to write new files. This indicates that even after significant amounts of time have passed, the data may still be retrieved utilizing specific tools and methods(Jason Gerend, 2021).

**Internals of NTFS**

A thorough understanding of NTFS internals is essential for a more in-depth investigation of file storage, deletion procedures, and the complex workings of the file system. Understanding the complexities of file management encourages us to explore the fundamental elements of NTFS, such as file metadata, data clusters, and Master File Table (MFT), these concepts are explained below:

1. File Metadata: metadata is the data about data that helps in identifying files through their properties or the file information stored on the system. Every file has metadata that NTFS carefully keeps track of. This metadata includes important facts including the file type (read-only, hidden, system), timestamps (made, changed, accessed), and ownership information.
2. Data clusters: NTFS stores data in the clusters, these clusters are the contiguous disc space blocks that are assigned to files, so it becomes more important to understand the allocation and management of the clusters in the NTFS file system to delve into the working of the NTFS and knowing how it stores the data associated with each file.
3. Master File Table (MFT): In NTFS it plays a crucial role in maintaining records for all files and directories on the disk. MFT contains file metadata, pointers to data clusters, and other attributes that define file characteristics. We will delve deeper into the concept of MFT when we look for the stages through which a file undergoes after deletion.

These are important elements of NTFS and many other fundamental elements of NTFS not discussed above that play a crucial role in the NTFS file system such as FRS, File storage, and file deletion mechanism these concepts will be discussed later in the findings section for a broader overview *(van der Meer, Jonker and van den Bos, 2021)*.

## FINDINGS

**File deletion in the NTFS file system**

This section of research majorly focuses on the deletion of files or folders within the NTFS file system as we all know from the perspective of computer forensics the files and folders that are being deleted can be recovered because NTFS follows critical processes when any files and folders get deleted from the system and those files and folders go under various stages which makes it easy to recover. So in this section, we will discover the major points of concern such as from what stages those files go after deletion or what happens when files and folders get deleted, removed from the recycle bin, or metadata is overwritten.

Some stages need to be considered when discussing File deletion in NTFS:

**Master File Table (MFT):**

Maintaining records for all files and directories on a disk is a critical function of the Master File Table (MFT) in NTFS. The actual data is not replaced by subsequent files, instead, it stays undeleted until the item in the MFT corresponding to the deleted file is recognized as deleted. Employing the technical procedures for locating files and exploring the applicability of MFT about forensic examination it is crucial to know how the MfT functions and how it is related to the deleted data*(GeeksforGeeks, 2023)*.

A screenshot of a computer

Description automatically generated

**Steps to be considered while looking for Deleted Files in the MFT:**

1. At first we need to find MFT in the NTFS volume, to find it we need to simply look for the file record number or we can use an FTK imager where we can load an image of the drive when investigating evidence there we can locate MFT under the root folder of the drive.
2. Then we can employ a forensics tool to scan MFT entries as we know each entry of the MFT holds metadata of the file, timestamp, and other details.
3. In this step we will locate the deleted file in the MFT, as entries of MFT have a file record flag which helps in identifying the deleted files in the NTFS, this flag indicates that the file is no longer active but still not removed from the file system.
4. Now we will parse the attributes of the MFT as we know MFT entries of every file consist of various attributes like standard information, file name, type, and more.
5. Then we will search for the file signature i.e., the unique pattern of the file resides at the starting of the file data identifying the type of file and format we can also identify this through magic numbers where each format or type of file has it unique pattern.
6. Analyze the flags of the MFT entry which states the file status, for deleted files the status is ‘in-use’ which means space allocated to the file is no longer in use or the file is now inactive.
7. Exploring the resident and non-resident files in the MFT as resident file records will reside in the MFT entries and can be retrieved from there only, but for non-resident files MFT record is not and there is the pointer for external cluster, so runlist needs to be parsed for accessing data.

**Unallocated spaces and Orphan Files:**

Unallocated spaces and Orphan Files are directly related to file deletion in the NTFS file system when performing forensic examination, the verified evidence or the image of the NTFS using Drive contains two folders named Orphan files and the Unallocated spaces these sections or folders consist of the deleted file now if we delve deeper in the concept:

A screen shot of a computer

Description automatically generated

1. **Unallocated spaces:** this folder or section of the file system belongs to that file or directory which do not exist anymore, this area is not used actively by the file system as it is formed by the deletion of any file, disk formatting, or any activity to free up spaces. For forensic relevance, these spaces are crucial parts as they contain deleted files that can be of important use. Also, we know files that get deleted fall under the section of unallocated spaces.
2. **Orphan Files:** We consider Files and Folders as orphans because their parent directories no longer exist which can be in result of incomplete file deletions, directory corruption, etc. The Master File Table (MFT) item that corresponds to a deleted file is marked as deleted file is marked as deleted as well. Nevertheless, the file becomes orphaned if the directory entry linking to it is not correctly updated or deleted. Orphan files may also arise if the deleting procedure is problematic.

**File Recovery in the NTFS file system.**

**General File Recovery Procedure for Deleted Files**

Several methodical procedures are involved in file recovery from NTFS partitions. Each stage is examined, and its consequences are explored in the analysis that follows:

1. **Scanning NTFS Partitions**: In this step, we will scan NTFS Partitions to locate MFT entries as we know MFT stores crucial information about each file and directory on the disk, this helps forensic investigators to use forensic tools like FTK imager efficiently. Information gathered from this step helps in identifying the nature of the deleted files, their locations, and the recovery strategy.
2. **Identification of MFT Entries:** after locating MFT we can now look for the specific entry related to the deleted file we are concerned about while investigating, this step will improve our point of view by specifying or focusing on the specific entries as each MFT is associate with a unique file on the disk.
3. **Searching employed on File Signatures and Processing on File Attributes:** For the identification of file type, we will search for file signatures within the MFT entries as we know file signatures are the distinctive patterns also known as magic numbers, these magic numbers help in signature analysis as shown in the fig below:

**A screenshot of a computer

Description automatically generated**

This figure shows the hex signature and its description with the extension it uses along with. Timestamps, file sizes, and other important file metadata (such as read-only, hidden, and system) are among the qualities found in MFT entries. Reconstructing the file’s metadata properly requires processing these characteristics. The result of file signature and processing attribute searches have a direct bearing on how recovery plans are developed. Investigators adjust their strategy according to the recognized file types and related metadata.

1. **Analyze Deleted Files:** Certain flag bytes in the MFT records are examined to identify deleted files. To separate files that are designated as deleted from those that are active this step in the processing is essential. By examining the $DATA property, one may learn where the file’s contents are located, which helps in guiding further steps in the recovery procedure.
2. **Content Recovery from Resident Files:** The recovery procedure for resident files, whose contents are kept inside the MFT entry, encourages moving the data to an outside location. Since this stage retrieves data directly from the MFT without relying on external clusters, it guarantees that the restored file is intact and good to go.
3. **Parsing Non-Resident Files:** as we know non-resident file stores their data on the external cluster on the disk, parsing the run list, which specifies the sequence of clusters along with their location on the disk as they are stored on the external cluster. It is necessary to understand the run list structure for accessing and recovering unorganized data clusters in non-resident files.
4. **$BITMAP Attribute:** after analyzing the run list we will look after the $BITMAP attribute to check the allocation status of clusters referred to in the run list, so here it is our observations from the run list if the allocation status is 0 the recovery of deleted file is possible if it is 1 this means partial recovery is possible and conversely if all clusters are allocated then recover is not possible as new file has allocated or overwritten the old file and clusters of old file is no longer exist.

**File Recovery Procedure from Recycle Bin**

Files deleted by the user are not removed permanently from the device the first go to the Recycle bin if they are not intentionally removed from the recycle bin, so the files that are residing in the recycle bin are just marked as removed from the system and moved to the hidden folder named recycle bin from where the file can be retrieved, there are some points to be noted which indicates the working of the NTFS recycle bin:

1. The recycle bin is just a temporary folder for storing the deleted file, retaining the original name and attributes like the timestamp details of the file.
2. File restoration is simple as a user can simply go to the recycle bin select the file and click the restore option.
3. To permanently delete a file user can simply click the empty recycle bin option, and then the system will mark the folder as inactive or ready for the new file if new files are created then the recovery of the files will be challenging for forensics investigators.

## CONCLUSION

In conclusion, observations on forensic recovery and NTFS file deletion have shed light on the complexities of data storage and retrieval in Windows operating systems. since the NTFS file system is an essential part of Windows systems, this research focuses on the stages the file stored after deletion and recovery procedure which employs various technical tools and techniques for identification and guiding the way to the end. This research paper attempts to contribute to the larger area of digital forensics by thoroughly examining the various stages of file deletion and the associated recovery procedures.

The identification and analysis of MFT entries for deleted files and directories play a crucial role in our findings and for a better understanding of the NTFS file system, exploration of orphan files and unallocated spaces leads us to the section of the NTFS where possibilities of deleted files are maximum and where we can recover those file and analyze them in-depth, In this research at every step of knowledge there is the challenge of doing more as every stage require good practical knowledge of digital forensics, as the consideration of multiple sections of forensics is being employed in the research.

## APPENDICES

References

Kai, Z., En, C. and Qinquan, G. (2010). Analysis and Implementation of NTFS File System Based on Computer Forensics. *2010 Second International Workshop on Education Technology and Computer Science*. doi:https://doi.org/10.1109/etcs.2010.434.

GeeksforGeeks. (2023). *What is a Master File Table?* [online] Available at: <https://www.geeksforgeeks.org/what-is-a-master-file-table/>.

Jason Gerend (2021). *NTFS overview*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview.

‌

‌

‌