Apple File System (APFS) & Digital Forensics

Liam Maher

I. Introduction

The Apple File System (APFS) is a modern file system developed by Apple, optimized for devices that utilize flash or solid-state storage. First introduced in 2017, APFS is now the default file system for all devices running MacOS 10.13 or later. APFS was designed to address the limitations of its predecessor, HFS+, and to offer improved performance, enhanced security, and advanced features like snapshots, cloning, and space sharing. These innovations, especially in handling modern storage technologies such as SSDs, are among the primary reasons for Apple's transition to APFS.

APFS offers four different formats: APFS (not encrypted or case-sensitive), APFS (Encrypted), APFS (Case-sensitive), APFS (Case-sensitive, Encrypted) [1]. Each of these formats provides specific advantages, such as encryption for protecting sensitive data or case sensitivity for developers requiring exact file naming conventions. These variations will be further explored later in this report.

Understanding the difference between file systems—such as APFS, HFS+, FAT16/32, and NTFS—is critical for digital forensic investigators. Each file system uses different techniques and methods for organizing, storing, and securing data. These differences are important to note to conduct a proper and efficient forensic analysis. Features like APFS encryption and cloning introduce both opportunities and challenges for investigators, underscoring the importance of mastering the intricacies of each file system.

II. History of MacOS File Systems

The file systems used in MacOS have evolved significantly over time to accommodate advancements in hardware as well as user needs. The first notable file system for macOS was the Hierarchical File System (HFS), which was introduced in 1985 after the brief use of Macintosh File System (MFS) from 1984-1985. HFS, which used 16-bit addressing, was designed for older storage devices such as floppy disks, with files being organized in a tree-like hierarchy [2].

As data storage requirements grew, Apple introduced HFS+ (Mac OS Extended) in 1998. HFS+ addressed many limitations of HFS by increasing the maximum volume size and number of files that could be stored. Most notably, HFS+ introduced 32-bit addressing, which allowed for more efficient use of disk space, especially on larger volumes. Another advantage of HFS+ is the ability to store long file names, up to 255 UTF-16 characters [3]. According to the New Technology File System (NTFS) official website from Lsoft Technologies, "On a 4GB hard drive, a file containing 4 KB of information would require 64 KB of space with HFS. With HFS+, it would only require 4 KB on the 4 GB hard drive" [3]. This highlights the dramatic improvement of storage utilization in the transition from HFS to HFS+. Apple also utilized multiple different formatting options for HFS+: Mac OS Extended (Journaled), Mac OS Extended (Journaled, Encrypted), Mac OS Extended (Case-sensitive, Journaled), and Mac OS Extended (Case-sensitive, Journaled, Encrypted) [1]. In Mac OS Extended, Journaled HFS+ was used to maintain the integrity of the file system across all different formatting options. Encryption was used to protect the partition with a password, and case-sensitivity was used to enforce differentiation between folders or files with similar names (ex. "Homework" vs "HOMEWORK") [1].

Since 1998, storage methodologies and mediums have continued to improve. In 2017, Apple developed and released Apple File System (APFS) as a replacement for HFS+, to address some limitations regarding HFS+. APFS is the current file system used across all new MacBooks and Apple devices. The main improvements in APFS included improved encryption, improved file system fundamentals, and space-sharing [1]. APFS also increased the read and write speeds for files. One major difference between HFS+ and APFS is how they handle free space. While HFS+ divides the storage into fixed partitions, APFS includes space sharing, which allows multiple file systems to share free space dynamically, leading to better efficiency and less wasted space.

III. Structures and Features of APFS

The APFS was designed to meet the growing demands of modern storage technologies. It introduces several key features that enhance performance, reliability, and security—crucial attributes for both end-users and forensic investigators. APFS implements 64-bit addressing, which allows for APFS volumes to support “up to 9 quintillion files” [4]. This scalability is essential for managing large data sets, particularly on devices like SSDs, where space and efficiency are critical for performance.

i. APFS Formats

Similar to Mac OS Extended (HFS+), APFS supports multiple formats: APFS (standard), APFS (Encrypted), APFS (Case-sensitive), and APFS (Case-sensitive, Encrypted). These variations allow users to tailor file systems to specific needs, particularly concerning security and data management. Contrary to Mac OS Extended using a simple encryption method that encrypts a specific partition, APFS implements an encryption on the volume as a whole.

In APFS, encryption is widely integrated into the file system, allowing different layers of data protection. A user can choose to encrypt an entire volume or individual files, each with its own key, making APFS robust in environments where data security is of particular importance [5]. However, these encryption capabilities also present challenges for digital forensic investigators. The use of encrypted files or volumes can impede the file recovery process. . In cases where encryption is used, forensic investigators must rely on decryption keys or forensic tools that can handle the encrypted files effectively. Without access to decryption keys, recovering data from APFS-encrypted drives can be exceedingly difficult, adding a layer of complexity to forensic investigators.

ii. APFS Snapshots

One of the most valuable features for forensic purposes in APFS is snapshots. APFS snapshots create read-only versions of the file system at a specific point in time. Snapshots do not duplicate data, but instead reference the original file structure, only recording changes made after the snapshot was created. In previous file systems, such as HFS+, multiple copies of a file were necessary to reference different versions. However, in APFS, snapshots allow users to maintain a single copy of the file while recording differences between the original and subsequent versions. This process significantly reduces storage requirements by saving only the changes (at the block level) between versions, rather than duplicating entire files [5].

In digital forensics, snapshots provide a reliable way to look into the system's past state without the risk of overwriting or modifying critical data. Digital forensic investigators can extract these snapshots to analyze activities, tack modifications, and recover deleted files, making them very useful in cases involving data corruption or tampering. This is particularly useful in cases involving data corruption, tampering, or system compromises. Snapshots ensure that a forensic investigator can review historical system states, enabling them to piece together the sequence of events leading to an incident.

iii. APFS Cloning

Another feature that was introduced in APFS is cloning. Cloning allows multiple copies of files or directories to share the same data blocks. In traditional file systems, creating a copy of a file involves duplicating the entire file, takings up more storage space. However, APFS employs a copy-on-write mechanism. This means that cloned files only take up additional space if they are modified after the cloning process. Until changes are made, both the original file and it's clone point to the same data blocks, reducing the amount of disk space used [5].

For forensic investigators, cloning introduces many opportunities and challenges. Cloning can make it easier to track versions of files over time. However, the presence of multiple clones within a system can complicate forensic analysis. Investigators must carefully distinguish between cloned files and their originals to determine which version of the file is relevant to the investigation. Additionally, deleted files may still have active clones within the system, adding further complexity to the process of file recovery. Specialized forensic tools are often required to identify and differentiate between cloned files and original files.

iv. Space Sharing and Efficient Volume Management

A feature that further enhances APFS's efficiency is space sharing. With space sharing, multiple volumes can share the same storage container, allowing free space to be dynamically allocated among the volumes as needed [2]. This allows users to resize volumes without needing to re-partition the storage device, which was a common limitation in previous file systems. From a forensic perspective, space sharing can complicate data recovery. Since the size of volumes can dynamically change, the boundaries between volumes may not be as clear as they were in previous file systems. This may require digital forensic investigators to examine multiple volumes sharing the same container to ensure no relevant data is overlooked.

IV. Similarities and Differences between APS and FAT/NTFS

File Allocation Table (FAT) and New Technology File System (NTFS) are two file systems that are commonly encountered in modern computing. While all three file systems serve the same basic purpose—managing and organizing data on storage devices—they differ in their structure, performance optimizations, and capabilities. This section explores the main similarities and differences between APFS and FAT/NTFS, focusing on factors like file size limits, performance optimizations, and security features.

i. File Size Limits and Scalability

One major difference between APFS and both FAT and NTFS lies in their file size limits. APFS is a 64-bit addressed file system, meaning it supports a theoretical maximum of over 9 quintillion files on a single volume, and can accommodate files as large as 2^63 bytes (approximately 8 exabytes) [4]. This makes APFS highly scalable and capable of handling the large file sizes and high file counts that we typically see in modern data storage environments.

In contrast, NTFS has a maximum file size of 2 TiB, and FAT32 (32-bit version of FAT file system) has a maximum file size of 4 GiB [6]. Furthermore, NTFS has a maximum partition size of 256 TiB, and FAT32 has a maximum partition size of only 8 TiB.

ii. Performance Optimizations

APFS is optimized for SSDs and flash storage, employing many optimization features such as copy-on-write in cloning. In the previous section, we explored how cloning save's storage space by allowing multiple versions of a file to occupy the same data blocks. Additionally, APFS uses space sharing, which allows multiple volumes to dynamically share free space on a container, eliminating the need for partition resizing. These features make APFS highly efficient in modern storage environments where performance and space optimization are critical.

On the other hand, NTFS was originally designed for mechanical hard drives, making it not as optimized for SSDs as APFS. Similar to HFS, NTFS offers journaling, which helps to ensure the integrity of the data and file system in the event of a crash. In the case of FAT32, it offers very minimal performance optimizations, not utilizing journaling or compression. Both FAT32 and NTFS required fixed partition sizes, unlike the use of dynamic resizing in APFS. However, in NTFS you have the ability to resize partitions, although not as seamless as in APFS, and in FAT32 you can not.

iii. Security Features

APFS offers built in encryption capabilities, offering both volume level and file level encryption. APFS also uses different keys for different layers of encryption, making unauthorized access to data extremely difficult. While NTFS also offers encryption for the file system, it is not as deeply integrated as the encryption features for APFS. Additionally, FAT32 offers no built-in encryption capability, making it much less secure. The lack of security features in FAT32 is one of the reasons why it is rarely used in environments where data privacy and protection are critical.

V. APFS Forensics Tool Case Study

When it comes to forensic analysis of APFS, Magnet AXIOM, developed by Magnet Forensics, is a tool widely used in forensic investigations. As of AXIOM Version 3.0, AXIOM provides extensive support for modern file systems, including HFS+ and APFS [7]. Magnet AXIOM's ability to analyze modern file system structures and user-generated data makes it a top choice for digital forensic investigators.

i. Overview of Magnet AXIOM

Magnet AXIOM is designed to analyze, recover, and report on data from a wide range of devices from smartphones to cloud-based systems. AXIOM supports forensic investigations of FAT, NTFS, HFS+, and APFS file systems, and more. With regards to APFS, Magnet AXIOM excels in handling APFS snapshots, file encryption, space sharing, and cloning [7].

One of the most useful aspects of AXIOM is it's decryption capabilities for FileVault 2.0. When in possession of the decryption key or password for the device, AXIOM can acquire data from both encrypted and decrypted partitions. AXIOM also has the capability of cracking passwords in the event that the investigator does not hold the user's password. It can even show password hints in some scenarios on an image with an APFS partition [8].

Once an image that contains APFS is decrypted (or if it was not encrypted in the first place) forensic examiners will be presented with numerous artifacts to help in their investigation.

These artifacts include network profiles, MRU files, Bluetooth devices, messages, and more [7]. AXIOM can also display APFS metadata, such as file timestamps and volume history [8].

ii. Benefits of Magnet AXIOM

One of the significant benefits of Magnet AXIOM is its ability to handle complex APFS structures, including encrypted volumes. AXIOM's built in decryption functions and password-cracking capabilities, combined with it's user-friendly interface, make forensic investigations on APFS volumes a much easier task. Magnet AXIOM also excels in its ability to recover deleted files, which is particularly important in APFS investigations may still be recoverable through snapshots or residual file fragments [8].

iii. Potential Limitations of Magnet AXIOM

Magnet AXIOM is not without it's limitations. Like most forensic tools, the ease of decrypting an APFS volume depends on having access to user passwords or decryption keys. Furthermore, when decrypting an APFS volume, it is essential to have a separate storage device with at least the same capacity as the encrypted partition to store the decrypted data. For instance, if the encrypted volume is 1 TB, a 1 TB or larger drive is necessary to write the decrypted files. Without this additional storage space, it will be impossible to access or analyze the decrypted data effectively [7].

iv. Magnet AXIOM's Effectiveness in Real-Life Case Studies

Magnet AXIOM has been successfully used in various digital forensic investigations and has received positive reviews across a wide range of published sources. However, there are currently no widely publicized investigations where it was specifically used on APFS. This does not imply that the tool has not been applied in such cases. It possible that investigations involving APFS may not be high-profile or are being kept confidential due to the nature of the data involved.

VI. Conclusion

In this report, we explored the Apple File System (APFS) and its key features, including encryption, snapshots, cloning, and space sharing, as well as their relevance to forensic investigations. APFS was designed to address the limitations of its predecessor, HFS+, and is optimized for modern storage technologies such as SSDs. While APFS offers enhanced security and performance, it also presents challenged for forensic investigators, particularly when dealing with encryption and the dynamic nature of space sharing.

We also compared APFS with other file systems like FAT32 and NTFS, highlighting differences in file size limits, performance optimizations, and security features. These distinctions emphasize the importance of understanding each file system's structure and behavior for effective digital forensic analysis.

Finally, the case study involving Magnet AXIOM demonstrated its capabilities in handling challenges specific to APFS, such as encryption. While there are currently no widely published APFS investigations involving AXIOM, the tool's versatility and features make it a valuable asset in forensic investigations across various file systems.

References

[1] Apple Inc., "File system formats available in Disk Utility on Mac," Apple Support, Oct. 4, 2023. [Online]. Available: https://support.apple.com/guide/disk-utility/file-system-formats-dsku19ed921c/mac. [Accessed: Oct. 20, 2024].

[2] Apple Inc., "File system details," Apple Developer Documentation. [Online]. Available: https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemDetails/FileSystemDetails.html#//apple_ref/doc/uid/TP40010672-CH8-SW1. [Accessed: Oct. 20, 2024].

[3] "HFS+ File System Overview," NTFS.com. [Online]. Available: https://www.ntfs.com/hfs.htm. [Accessed: Oct. 20, 2024].

[4] "APFS Structure," NTFS.com. [Online]. Available: https://www.ntfs.com/apfs-structure.htm. [Accessed: Oct. 20, 2024].

[5] Apple Inc., "About Apple File System," Apple Developer Documentation. [Online]. Available: https://developer.apple.com/documentation/foundation/file_system/about_apple_file_system. [Accessed: Oct. 20, 2024].

[6] F. Kandah, "03 – Introduction to file systems; 04 – FAT16-FAT32 storage scenarios," lecture notes, Auburn University, 2024. [Accessed: Sep. 15, 2024].

[7] Magnet Forensics, "APFS File System and New Mac Artifact Support in Magnet AXIOM 3.0," Magnet Forensics. [Online]. Available: https://www.magnetforensics.com/resources/apfs-file-system-and-new-mac-artifact-support-in-magnet-axiom-3-0. [Accessed: Oct. 20, 2024].

[8] Magnet Forensics, Magnet Forensics Documentation. [Online]. Available: https://docs.magnetforensics.com/docs/axiom/html/Content/Search.htm?q=APFS. [Accessed: Oct. 20, 2024].