**U05A1 – Working with Windows, Linux, Mac, and CLI Systems**

**Chris Misch**

School of Business, Technology, and Health Care Administration, Capella University

IT4075: Forensics

Timothy Gillian

August 13, 2023

File Systems

“An effective file system is crucial for regular system operations because it regulates how, where, and when data is stored and retrieved from a storage device” (Kaplarevic, 2023). Essentially a file system is a way for an operating system to store necessary files and applications on a hard drive.

File systems hold all kinds of data metadata data encryption, fie access controls, etc. They organize where things can be stored on the hard drive. Without a file system, files would have zero organization when saved to a hard drive causing the hard drive to be very inefficient. Not only would things be inefficient but also difficult to find.

Before a file system can be installed on a hard drive it must be partitioned to allow for several logical regions to be created. Each logical region can then be managed as a separate storage device. This is done to separate the different functions of a file system and prevents one system from corrupting another system. Linux file systems is a good example. It has 3 partitions: one is dedicated to the operating system, the second one is for the user’s files, and the third is a swap partition allowing for extra RAM when needed.

As a forensics specialist it is important to know the difference between different file systems. Even though they share the same basic functions they have different ways of where and how they store information. So, knowing the type of file system used is very helpful in discovering evidence during an investigation.

Linux File System

The Linux system has evolved from the UNIX system to be a free opensource system. Since it is opensource it has many different variations. The file system was originally called MINIX but has since been changed to ext file system. There are four versions of ext: ext, ext2, ext3, and ext4. Each one adds better functionality and performance than the last. The ext3 kernel introduced journaling which allows it to keep a journal of all changes in the data structure. The ext3 file system according to Kaplarevic (2023) “reduces the risk of corruption or data loss.”

The most current file system for Linux is ext4. This file system can support a max file size of 16TiB allowing for much larger files than ext3. This new system allows for improved performance to support the larger files sizes. It includes backward compatibility for older versions of ext.

The Linux file system has 4 components that define the filing system: boot block, super block, inode block, data black. The boot block contains bootstrap which contains the files that boot up an operating system. According to Nelson, Phillips, & Steuart (2014) the super block contains all the vital information about the computer system and is considered a part of the metadata. It also manages the file system.

The inode block contains the first part of data just after the super block. The inode block contains file status, time of creation, time of modification, block address, and number of links to the file. This is a good place to find hidden or deleted files. Since the inode block contains metadata of a file or directory it is tied directly to the data block. The data block is where all the files and directories are stored.

The structure of the Linux file system consists of a root directory donated by a “/” followed by 14 subdirectories. I will only mention a few of them here but you can see the file structure in Figure 1: Linux File System Structure. The root directory is your home or system administrator. In most cases a user account will have their files and directories under ~/usr file. In the /user/var you will find logging files, cache files, and record locks.

The Linux file system suffers from fragmentation over time causing deficient performance the more it is used. It lacks native encryption so you would have to rely on a third party for data encryption of your files. Also, there is limited snapshot support reducing the ability of the system to revert to previous versions of a file if it is corrupted.

Mac File System

Mac systems are thought to be similar to the Unix file system. However, the macOS files system is only based on BSD (Berkley Software Distribution) and not on the Unix kernel (Das, 2023). Today’s Apple file system is called Apple File System (APFS). It has replaced the older HFS+ (Hierarchical File System). There are two parts that define the filing system: data fork and resource fork. “The data fork is an unstructured finite sequenced of bytes.” (Apple Filing Protocol Concepts, 2012). In the resource fork you will find OS resources, metadata, drivers, and data structure for mapping inside the fork. It can be important to know because when using a MS-DOS computer to access a Macintosh file it will not be able to see both forks.

APFS is designed to be used with SSD and other flash-based storage systems with a 64-bit inode (Nelson, 2021). According to Apple Filing Protocol Concepts (2012) the APFS file structure design presents a user-oriented view of the file system by hiding or renaming some files and directories. This creates 3 domains off the root “/” directory: local domain, system, domain, and user domain.

The system domain contains the software required for the system to run. You cannot add, remove, or alter files in this domain. The local domain contains resources that are local to the users of the computer. It consists of several directories on the local and root volume. Only the system and the administrator with root privileges are allowed to add, remove, or modify these files. The user domain contains resources specific to each user on the system. Each user has full access to their own user domain. The network domain is where shared resources are held.

The APFS is designed for the future by focusing on modern storage technologies. These new technologies ensure better encryption, more efficient use of space, and reduce corruption of files. APFS clone feature allows instantaneous file copies as you change a file while reducing the need for extra blocks. The snapshot feature creates a snapshot of a point in time that you can go back to. The advancement of the feature is that it uses exceptionally low resources. The encryption feature allows “strong full disk encryption using AES-XTS or AES-CBC modes.” (Nelson, 2021).

On of the issues with Apple’s APFS, according to Adzo (2023) is that it does not support older macOS’s This could be an issue in the forensics lab by not allowing older files or apps to be accessible. A second issues Adzo (2023) mentions is that Time Machine uses the older HFS+ and is not supported in the new system making this application useless in accessing. A third issue is that APFS does not have as much third-party support as Linux or NTFS. This will limit you to the tools you can acquire requiring you to create home grown scripts and tools for your forensics needs.

Windows File System

Windows based systems use the NTFS (New Technology File System) since 1993 with the release OF Windows NT3.1 (Fisher, 2023). This system is supported in Linux and Unix but only has read only support for Apple’s APFS. Windows file systems are groups of sectors that form into clusters ranging from 512 bytes to 32,000 bytes each. These clusters are numbered sequentially starting from zero. In the first cluster, Windows NTFS will partition it as the Partition Boot. The second partition is the Master File Table (MFT). The third and fourth partitions are named System Files and File Types.

The Partition Boot sector allows the system to boot up the operating system and enables the NT loader program to find the MFT (metadata) during startup. The MFT sector holds the master file table and its mirror record in case the first MFT record is corrupted. The metadata here are sectioned into small directories of 512 bytes or smaller. The four directories are standard information, file or directory name, security descriptor, and index. If the directory is larger than 512 bytes, the excess data will be organized into B-trees. The B-trees will use pointers to external data clusters.

The file types hold the file attributes of each file. These attributes hold the name, bitmap, index allocation, and security information about the file. The system files folder is hidden from view. It contains the metadata to implement the file system. The system files here are MFT, log file, boot sector, and volume.

The benefit of using NTFS is that it works well with other operating systems and has many third-party applications that work with it. The NTFS allows for journaling, which works in the same way as in Linux file system. NTFS offers full disk encryption with BitLocker creating an extra layer of security. A third benefit of NTFS is that theoretically, it can support up to 16EB on a hard drive (Fisher, 2023).

There are not too many drawbacks to using NTFS, however one drawback to using NTFS is that it is not as compatible with macOS. So, if you are using any Apple products you will have to have a secondary file system to allow full read and write capability. A second drawback is its popularity in usage. This makes it a large target for hackers and malicious activity.

Forensic and Investigative Tools for Linux, Mac, and Windows

Tools used for gathering and retaining evidence in a forensics investigation need to work with several types of file systems easily. Forensics tools for investigation with Windows and Linux operating systems are Autopsy/Sluth kit, FTK imager, Wireshark, and Volatility. For Mac you can use Autopsy/Sluth kit, Belkasoft, and FTK.

The best tool that will work with all three systems would be Autopsy/Sluth kit. Sluth kit allows you to analyze file system data through a library of command line tools. Autopsy is a GUI digital forensics platform that adds to Sluth kit’s abilities. When you are using this tool in the command line on Linux or Mac you will need to add sudo before each command.

Basic Steps Using Autopsy/Sluth Kit

To use this tool, you will create a new case by adding an image of the evidence to a new case. Next you calculate the hash value of the image using Split Image Confirmation. This allows you to ensure the integrity of the evidence. You can then analyze the image and search for any key words from your investigation.

Summary

I recommend that Mega Corporation use NTFS as their primary forensics file system. This is because the NTFS is already the main file system used in the corporation. The exception there are some employees that are using Mac or Linux system. The NTFS is user friendly and has the most flexibility when it comes to choosing different tools for forensics. Even though NTFS has only read privileges of APFS it is still able to read files from a Mac system whereas if Mega Corporation went with APFS it would not be able to read NTFS. By using an open-source forensics tool like Autopsy accessing Mac files won’t be too much of a problem.

References

Kaplarevic, V. (2023). Introduction to the Linux File System. *Knowledge Base by phoenixNAP*. https://phoenixnap.com/kb/linux-file-system

Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer Forensics and Investigations (6th ed.)*. Cengage Learning.

Mfillpot. (2010, September 16). *Linux File Structure - Linux.com*. Linux.com. https://www.linux.com/training-tutorials/linux-file-structure/

Sharma, M. (2023). Best forensic and pentesting Linux distros of 2023. *TechRadar*. https://www.techradar.com/best/best-forensic-and-pentesting-linux-distros

Das, A. (2023). What is the Difference Between macOS and Linux? *It’s FOSS*. https://itsfoss.com/mac-linux-difference/

*Apple Filing Protocol concepts*. (2012, December 13). Copyright 2018 Apple Inc. All Rights Reserved. https://developer.apple.com/library/archive/documentation/Networking/Conceptual/AFP/Concepts/Concepts.html

Nelson, T. (2021, July 10). What Is APFS (Apple's File System for macOS)? *Lifewire*. https://www.lifewire.com/apple-apfs-file-system-4117093

Adzo, K. (2023, June 28). Pros And Cons of APFS The New Apple File System - Apple Gazette. *Apple Gazette*. https://www.applegazette.com/mac/pros-and-cons-of-apfs-the-new-apple-file-system-successor-of-hfs/

Fisher, T. (2023). What is the NTFS file system? *Lifewire*. https://www.lifewire.com/ntfs-file-system-2625948

Tables

Figure :Linux File System Structure

