ITMS 538 Assignment 05a_rds

Alan Palayil

Due Date: 11/18/2022

FAT vs NTFS vs EXT File Systems

For forensics investigations, we will discuss the various file systems NTFS, FAT, and EXT. Each of the file system have their own advantages and downsides during investigations.

Definitions:

- Of the three file systems, NTFS has the most features and support because it is the most recent. It is a journaling file system, which means it logs changes made to the file system. Because it can assist in the reconstruction of what took place on a system, this is useful for forensics. Encryption of files is another feature of NTFS that can make it challenging to access data on an NTFS drive. It is also the most intricate, which may make analysis more challenging
- The older FAT file system lacks encryption and journaling capabilities. This means that data stored on a FAT drive can be accessed more easily, but no one can tell for sure what has changed or been deleted. It is popular and simpler than NTFS, making it possible to analyze it. Nevertheless, it lacks some of NTFS's features and support.
- Compared to NTFS and FAT, EXT is a more recent file system that offers journaling and encryption support. Although it is possible to reconstruct what took place on the drive, this makes it more difficult to access data stored on an EXT drive. Because it isn't used as much as the other two file systems, it may be harder to find support and tools for forensics analysis.

After providing an explanation for each file system, we can begin discussing the evidence-specific file system, which is crucial to an investigation for the following reasons:

First and foremost, the file system has the power to control what data is accessible and how it is stored. For instance, the NTFS file system is a journaling file system, which means that it keeps a log of all changes to the system. This information can be used by forensics to help recreate what happened on a computer, which is a useful skill. NTFS also supports file encryption, which may make it more challenging to retrieve data stored on an NTFS drive. The FAT file system is an older format that does not support encryption or journaling like more recent file systems do. This makes it easier to access data stored on a FAT drive, but there is no way to know for sure what has been changed or deleted on the drive.

In addition, the file system can control how data is accessed. The more recent file system known as EXT supports encryption and journaling, two features. Accessing the data stored on an EXT drive becomes more difficult as a result, but it is still possible to recreate what happened on the drive.

Considerations to make when selecting a study's file system:

Consider the requirements of the investigation as well as the capabilities of the forensic tools when selecting a file system for an investigation. NTFS might be the best option if the investigation needs a lot of data. FAT might be a better option if the investigation requires quick access to information. EXT may be the best option if the investigation requires specific features. Different file systems may use different file formats, and thus different techniques or tools may be necessary to view, open, and analyze the different file systems

From a forensics point of view, each of these file systems has its own unique set of benefits and drawbacks because they may use different file formats. Although NTFS is the most difficult file system to use, it also provides the highest level of security. Despite its ease of use, FAT does not guarantee that the data will not be altered. EXT is a format that is relatively easy to use while still offering features like journaling and encryption. It strikes a satisfactory balance between the two formats.

Conclusion:

Thus, based on the description alone, NTFS is the best choice for an investigation if the goal is to collect as much data as possible and if the goal is to quickly access information, then FAT may be the better choice. If the goal is to use specific features, then EXT may be the best choice.