**Level 1: Windows File Systems**

Refer to the following document when answering the questions for Level 1.

<https://fossbytes.com/fat32-vs-ntfs-vs-exfat-difference-three-file-systems/>

1. What is the definition of a file system?

A file system is a set of rules used to decide how data is stored and fetched in a storage device, regardless if it’s a hard drive, flash drive, or something else.

1. What are the three file systems used on Windows computers?

FAT32, NTFS, and exFAT.

1. What are the properties of the FAT file system?
   1. The FAT file system was the original Windows 95 file system. When was it introduced?

It was introduced in 1977.

* 1. How is the FAT16 file system different from the FAT32 file system?

The FAT32 file system can store more data on it than the FAT16 file system.

* 1. What is the file size limit of the FAT32 file system?

FAT32 allows you to store files of size up to 4GB.

* 1. What is the disk size limit of the FAT32 file system?

The maximum disk size can go up to 16TB.

* 1. What other devices currently use the FAT file system?

Gaming consoles, HDTVs, DVD & Blu-Ray players, and practically any device with a USB port can support the use of the FAT file system. All versions of Windows and Linux distributions support the FAT32 file system, and Apple’s MacOS provides complete support for it.

1. What are the properties of the NTFS file system?
   1. The NTFS file system is what is used on current Windows computers. When was it introduced?

It was introduced in 1993.

* 1. How is the NTFS file system different from the FAT file system?

The NTFS file system is different from the FAT file system because it was developed as the result of an association between Microsoft and IBM to develop a new age operating system with better performance in terms of graphics, while FAT is only associated with Windows.

* 1. What is the file size limit of the NTFS file system?

The file size limit of the NTFS file system is 16 EB.

* 1. What is the disk size limit of the NTFS file system?

The disk size limit of the NTFS file system is 256 TB.

* 1. What are some notable features of the NTFS file system?

Its notable features include reparse points, sparse file support, disk usage quotas, distributed link tracking, and file-level encryption. The NTFS file system supports backward compatibility with the previous versions.

It’s also a journaling file system which proves to be an important aspect when it comes to reviving a corrupt file system. It maintains a Journal, a data structure which keeps track of any potential modifications to the file system and is used to recover the file system.

* 1. What are some limitations regarding how other devices support the NTFS file system?

A limitation of the NTFS file system is that it is only supported by Windows XP and later versions. Apple’s MacOSX provides read-only support for an NTFS-formatted drive and only a few Linux variants are able to provide write support for NTFS.

1. Provide a summary of the exFAT file system.

The exFAT file system has the same 16 EB file size limit as NTFS, but it is way lighter as it doesn’t contain many of the extra features that the latter has. Introduced in 2006, most modern digital cameras use exFAT. High capacity SDXC memory cards are now pre-formatted with the exFAT file system, because it is lighter in contrast to NTFS and supports file sizes more than 4GB. Microsoft’s stubbornness to make the exFAT available freely has triggered the development of custom implementations of the file system. full read and write support is provided by Mac, Android, and Windows operating systems. But for Linux distributions, the appropriate software facilitates the support.

**Level 2: Windows NTFS Permissions**

Refer to the following document when answering the questions for Level 2.

<http://www.ntfs.com/ntfs-permissions.htm>

1. Read the information provided on the “Setting Permissions” page.
   1. Summarize how to view and set file and folder permissions.

On any Windows network, you can set sharing permissions for drives and folders. Known as the "Security Descriptor", this information controls what kind of access is allowed for individual users and groups of users.

1. Read the information provided on the “Advanced Permissions” page.
   1. List the advanced permissions that affect files.

~Execute File: Allows or denies running program (executable) files.

~Create Files: Allows or denies creating files within the folder.

~Write Data: Allows or denies making changes to a file and overwriting existing content.

~Read Data: Allows or denies viewing data in files.

~Read Attributes: Allows or denies viewing the attributes of a file or folder

~Read Extended Attributes: Allows or denies viewing the extended attributes of a file or folder.

~Append Data: Allows or denies making changes to the end of the file but not changing, deleting, or overwriting existing data.

~Write Attributes: Allows or denies changing the attributes of a file or folder.

~Write Extended Attributes: Allows or denies changing the extended attributes of a file or folder.

~Delete Subfolders and Files: Allows or denies deleting subfolders and files.

~Delete: Allows or denies deleting the file or folder.

~Read Permissions: Allows or denies reading permissions of a file or folder.

~Change Permissions: Allows or denies changing permissions of the file or folder.

~Take Ownership: Allows or denies taking ownership of the file or folder.

~Synchronize: Allows or denies different threads to wait on the handle for the file or folder and synchronize with another thread that may signal it.

* 1. List the advanced permissions that affect folders.

~Traverse Folder: Allows or denies moving through a restricted folder to reach files and folders beneath the restricted folder in the folder hierarchy.

~List Folder: Allows or denies viewing file names and subfolder names within the folder. List Folder only affects the contents of that folder and does not affect whether the folder you are setting the permission on will be listed.

~Delete Subfolders and Files: Allows or denies deleting subfolders and files.

1. Read the information provided on the “Basic Permissions” page.
   1. The basic permissions are listed at the top of the columns in the table. List the 6 basic permissions.

The Basic Permissions are Basic Full Control, Basic Modify, Basic Read & Execute, Basic List Folder Contents, Basic Read and Basic Write.

* 1. What basic permissions allow a user to write data to a file?

Basic Write, Basic Modify and Basic Full Control allow a user to write data to a file.

* 1. What basic permissions allow a user to delete a folder?

Basic Full Control and Basic Modify allow a user to delete a folder.

1. Why do you think there are separate permissions for reading and writing a file? Provide an example where you might want somebody to read a file but not be able to change it.

I think that there are separate permissions for reading and writing a file because there may be people that need to see it, but shouldn’t be able to write to that file. For example, if a teacher shares an assignment file that has instructions and important information on it, they would want their students to be able to read the file, but not make any modifications, because they could mess up the assignment and give false information. There are many cases where people will need to view a file but shouldn’t be able to edit it.

1. Why do you think there are separate permissions for listing folders and reading files? Provide an example where you might want somebody to be able to list a folder but not be able to read a file in the folder.

I think that there are separate permissions for listing folders and reading files because there may be cases where someone should be able to view the files in the folder, but not be able to read what’s in those files. For example, a teacher could be showing what’s in each of their folders to their students as an example on how to organize them, but not give their students access to opening their files.

**Level 3: Windows Share Permissions**

Refer to the following document when answering the questions for Level 3.

<https://blog.netwrix.com/2018/05/03/differences-between-share-and-ntfs-permissions/>

1. What are share permissions?
   1. Who do share permissions affect?

Share permissions manage access to folders shared over a network; they don’t apply to users who log on locally. Share permissions apply to all files and folders in the share; you cannot granularly control access to subfolders or objects on a share.

* 1. Who do share permissions not affect?

Share permissions don’t affect users that log on locally; they only affect users over a particular network.

* 1. Summarize the 3 types of share permissions.

Read — Users can view file and subfolder names, read data in files, and run programs. Everyone gets this by default.

Change — Users can do everything allowed by the “Read” permission, as well as add files and subfolders, change data in files, and delete subfolders and files. Nobody gets this by default.

Full Control — Users can do everything allowed by the “Read” and “Change” permissions, and they can also change permissions for NTFS files and folders only. By default, the “Administrators” group is granted “Full Control” permissions.

1. Summarize the main difference between NTFS and Share Permissions.

~Share permissions are easy to apply and manage, while NTFS allows more control and more control options.

~When share and NTFS permissions are used simultaneously, the most restrictive permission always wins. For example, when the shared folder permission is set to “Everyone Read Allow” and the NTFS permission is set to “Everyone Modify Allow”, the share permission applies because it is most restrictive; the user is not allowed to change the files on the shared drive.

~Share permissions can be used when sharing folders in FAT and FAT32 file systems; NTFS permissions can’t.

~NTFS permissions apply to users who are logged on to the server locally; share permissions don’t.

~Share permissions allow you to restrict the number of concurrent connections to a shared folder. NTFS doesn’t.

~Share permissions are configured in the “Advanced Sharing” properties in the “Permissions” settings. NTFS permissions are configured on the Security tab in the file or folder properties.

1. Summarize how to view and change share permissions.

In order to change share permissions, you must;

~Right-click the shared folder.

~Click “Properties”.

~Open the “Sharing” tab.

~Click “Advanced Sharing”.

~Click “Permissions”.

~Select a user or group from the list.

~Select either “Allow” or “Deny” for each of the settings.

**Level 4: Your Files and Folders**

1. Organized your files and folders on your network drive to match your GitHub repository.
   1. Create a folder on your student drive for Computer Science Work
   2. Create sub-folders (e.g. Topic A, etc.) to match the folders on your GitHub repository
   3. Move your answer files and other work you have done for this course into the proper sub-folders.
   4. Show your organized folders/files to Mr. Nestor.