Forensics

Who Framed Roger Rab-bit?

Files and the File System

A File System is a like an index for all the files in your computer system! You can find a reference to all the files in your computer.

File Systems have a lot of different parts but the main ones include ‘Files’, ‘Directories/Folders’ and ‘Metadata’. Files are used to store data and have two parts - ‘Filename’ or the name used to refer to the file and ‘type’ or the kind of data that is stored in the file. Directories are collections of files grouped together in some way. Metadata is the data about the file itself like its length, time created and author etc.

When a file is created, the data is stored at some position in memory and the filename is the reference to that data. It is like the address of your friends house. The address of your friends house has nothing to do with your friends house but it is a simple way that we have come up with to remember where certain places are located. If you forget the address, your friends house doesn’t get removed. Similarly, sometimes when you delete a file, all that is happening is that your computer just doesn’t remember where that file is stored. It probably still exists at that same memory location until you write something there again.

A file consists of Blocks, which is the smallest part of the data that is stored in memory. The header block contains the starting point of the file whereas the footer block contains the end point of the file.

File Carving

“*File carving* refers to the technique to extract data from a disk drive without having the normal file system to easily recover the files.” It is a method of recovering files when there is not reference to them in the computer. It is mostly used to recover deleted files by criminal detectives.

From our previous conversation about deleting files, we know that when a file gets deleted, the data doesn't get deleted but just the reference to that data. Another important change that happens when you delete is file is that the disk location where the file is stored gets marked as unallocated and can thus be overwritten. However, it is possible to use techniques to recover most, if not all, of the data.