Exercise 11

09/11/2021

File carving

File carving is the process of reassembling computer files from fragments in the absence of file system metadata. All file systems contain some metadata that describes the actual file system. At a minimum, the following is stored: the hierarchy of folders and files, with names for each. For each file is also kept the physical address on the hard disk where the file is stored. A file might be scattered in fragments at different physical addresses.

File carving is the process of trying to recover files without the metadata. This is done by analysing the raw data and identifying what it is (text, executable, png, mp3, etc.). This can be done in different ways, but the simplest is to look for headers. For instance, every Java class file has as its first four bytes, the hexadecimal value CA FE BA BE. Some files such as pdfs contain footers as well, making it just as simple to identify the ending of the file. Refer the lab exercise on file signature analysis.

File carving can be used to recover data from a hard disk where the metadata is missing or damaged, especially by professional data recovery companies. When a file is deleted, only the entry in the file system metadata is removed, while the actual data is still on the disk. After a format and even a repartitioning it might be that most of raw data is untouched and can be recovered using file carving. Many carving schemes have been developed. File carving should be done on a disk image, rather than on the original disk. The majority of file carving programs will only recover files that are contiguous on the media (in other words files that are not fragmented).

For more details about file carving, refer

https://en.wikipedia.org/wiki/File_carving

https://forensicswiki.xyz/wiki/index.php?title=File_Carving

A number of carving tools are available. See the following link

https://forensicswiki.xyz/wiki/index.php?title=Tools:Data_Recovery#Carving

Many test images are available for performing file carving. For example, see http://dftt.sourceforge.net/

Hexadecimal editors such as WinHex also help in file carving.

For this exercise. take two images from a site such as http://dftt.sourceforge.net/ and perform file carving.

Include screenshots in your submission.