## Practical Exercise - Image Carving

Note :- Download a Hex editor application

There are a couple of approaches to carving and recovering files from file systems.

Firstly is the "File System" approach. That is, we use the fileystem's knowledge of where the deleted file was to begin our journey of recovery.

For example, when a file is deleted in a FAT32 filesystem, the directory entry has the first byte of the entry overwritten with 'E5'. The directory entry still contains; the filename (minus the first character), the file size and the first cluster number. These can be vital to assist in the recovery process.

For a valid file we could look up the cluster number in the FAT table and find all the fragments as each FAT entry points to the next cluster number. However when a file is deleted the FAT table entries are zeroed so we cannot trace the file fragments.

The second technique for file recovery is to ignore the filesystem and treat the disk as one big block of data. We can either do this on the whole disk image or we can just export the unallocated portion of the disk. We can then use our knowledge of what type of file we are trying to recover to attempt

to find the file/s in question.

So let's start with three simple image carves.

1. JPEG: Deleted, no thumbnails, not overwritten, unfragmented in free unallocated space.

2. JPEG: Deleted, no thumbnails, not overwritten, unfragmented in full unallocated space.

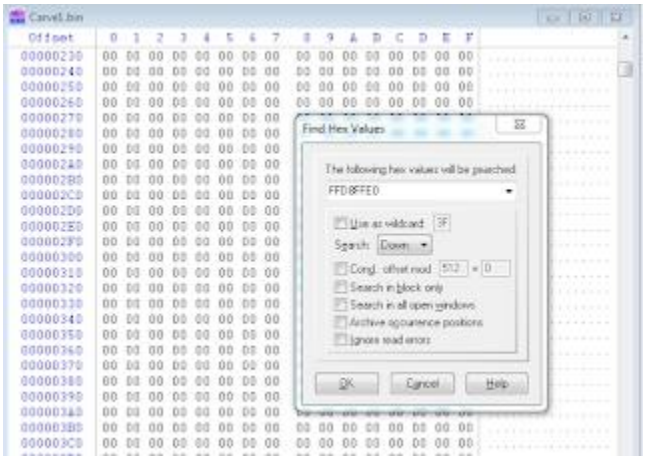
3. JPEG: Deleted, no thumbnails not overwritten, fragmented in unallocated space.

**Carve 01**

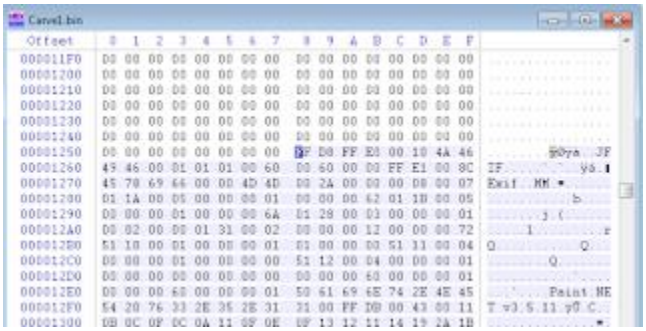
Download the bin file from the GitHub

https://github.com/thehexninja/BlogDownloads/blob/master/Carve1.bin

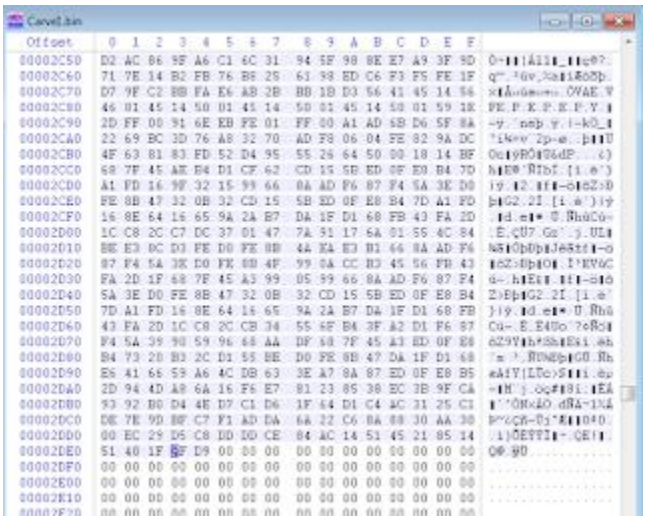
In a hex editor search for FFD8FFE0.




We find a search hit at 0x1258



Select the beginning of block at the the start of the JPEG at 0x1258. Now we search for the end of the file with the hex FFD9.




The D9 of FFD9 is at end of the file is at offset 0x2DE4. We select this as the end of the block. Copy the block out to a new file. In the filename I like to include 3 things, the file I am carving from, the start and end offset. So lets call it Carve1_1258_2DE4.jpg and wallah...

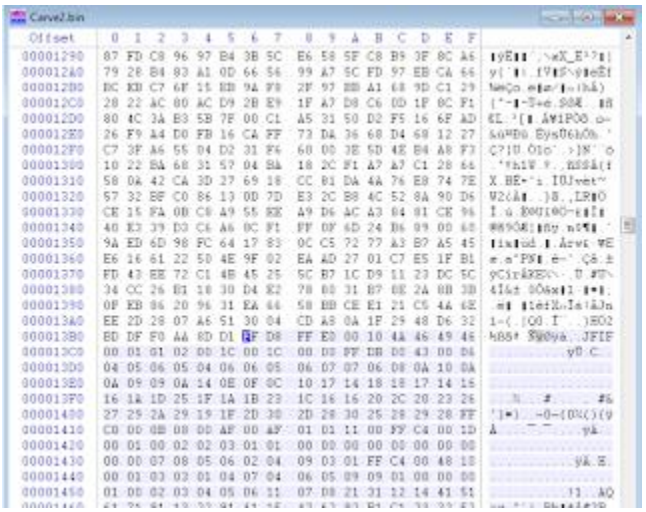


**Carve 2**

Download the bin file from the GitHub

https://github.com/thehexninja/BlogDownloads/blob/master/Carve2.bin

Again we search for FFD8FFE0.



We find it at offset 13B6. In this second example we see that it is embedded in other data (other deleted or allocated files), this is more typical of what we might see.

Again we search for FFD9 for the end of file marker. It is at 0x2360. We select the block and copy it out into a new file. Carve2_13B6_2360.jpg.



This seems simple enough, just a search from the start and end and we a have carved two deleted files of the Hex Ninja.

## Tasks

1. **Find the information relate to below file system and explain does the file system work.**

    - **NTFS**
    - **FAT32**
    - **Ext4**