Assignment 1

Task 1

Using a hex editor of your choice, view the headers of a variety of files and file types. Complete the table below to create your own list of “Magic Numbers”

> A lot of file types are already given in the document, so i will include some of the lesser known/not included file types. Sources: https://en.wikipedia.org/wiki/List_of_file_signatures https://file.org/extension/pgp

File	Extension	Header HEX	Other Details
parquet	-	`50 41 52 31`	Starts with `PAR1` ends with `PAR1`
ISO (CD/Disk Image)	.iso	`43 44 30 30 31`	
Script	-	`23 21`	File starting with `#!`
SQLite DB	.db, .sqlite .sqlitedb	`53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00`	
OpenSSH private Key File	-	`2D 2D 2D 2D 2D 42 45 47 49 4E 20 4F 50 45 4E 53 53 48 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D`	`-----BEGIN OPENSSH PRIVATE KEY-----`
OpenSSH public Key File	.pub	`2D 2D 2D 2D 2D 42 45 47 49 4E 20 53 53 48 32 20 4B 45 59 2D 2D 2D 2D 2D`	`-----BEGIN SSH2 PUBLIC KEY-----`
MicroSoft Tape Format	-	`54 41 50 45`	Microsoft Tape Format for Tape Backup of different Windows Systems
PGP	-	`85 XX XX 03`	File Format for Storing Public Keys, used in keyrings and widely adopted in Linux Communities

Task 2

Using a hex editor of your choice,
- Open ‘file carving’
- Consult the ‘Files Headers List.docx’ and check file signature for ‘file carving’,
- Add the correct extension to the ‘file carving’ filename and open it,

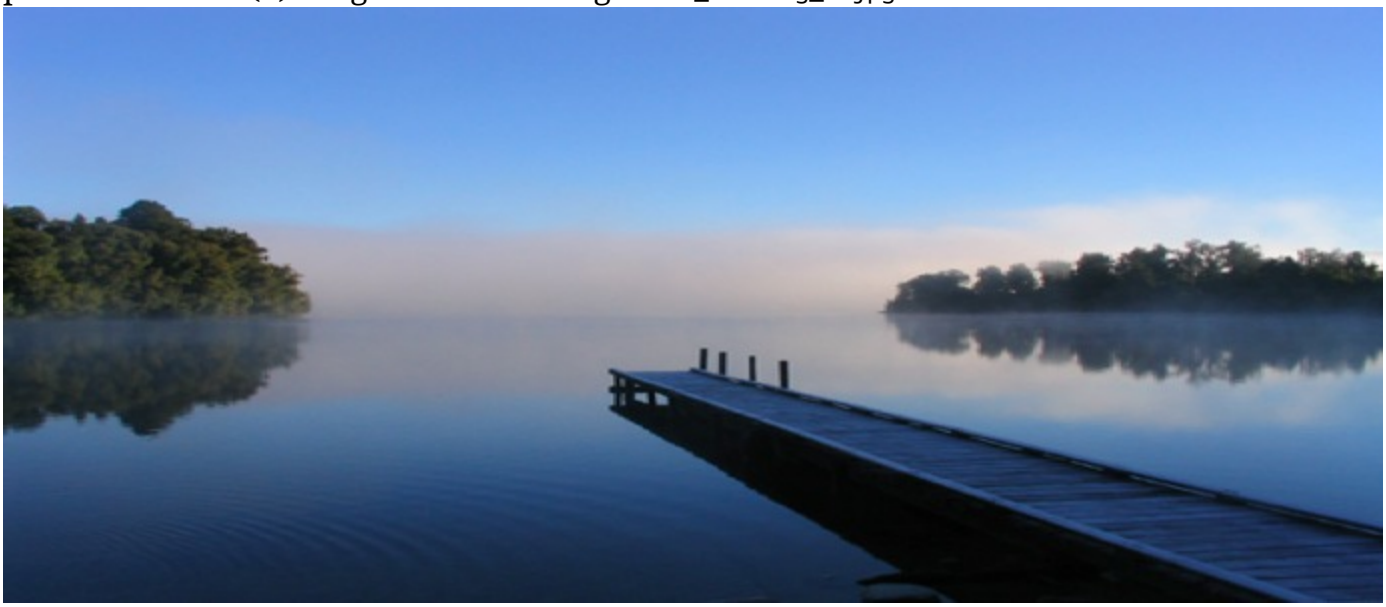
- Extract All hidden files in the ‘file carving’,
- Save each extracted file with a separate name and with the correct extension.
- Open each extracted file —

`File Carving` has the Signature `FF D8 FF E0 00 10 4A 46 49 46 00 01` Which is a jpeg/jpg file, but is it only that?

From Wiki: https://en.wikipedia.org/wiki/JPEG; The End of Image JPEG Marker is `0xFFD9` At the last Offset `0001FDF6 + 5 Bytes` the marker is `0x0D` So this file is not just a JPEG Image.

1: Searching for `0xFFD9` we extract the real jpg image under the file name `File_Carving_1.jpg`

2: Right after this signature there is another jpg Header starting with `FF D8`, Doing same procedure as in (1) we get another Image `File_Carving_2.jpg`:



3: Again, immediately after the pier image we find another JPG signature, same procedure as previous we get `File_Carving_3.jpg`:

4: Right After that image we find a PDF file Signature `25 50 44 46 2D`, We need to know a PDF EoF marker to correctly extract it. From: https://stackoverflow.com/questions/11896858/does-the-eof-in-a-pdf-have-to-appear-within-the-last-1024-bytes-of-the-file

We know that the PDF EoF is `%%EOF` First `%%EOF` marker yields a corrupt PDF `File_Carving_4.pdf`, a second `%%EOF` Marker is found yielding an intact pdf `File_Carving_5.pdf`. To make sure this is correct I try to find another `%PDF-` Marker to see if there is another PDF present, which is not the case.

To make sure there are no files left, some common file formats signatures were searched, yet received no results:

```
ID3      mp3
WEBP     webp images
rtf      Rich Text
ftyp     mp4 file formats begin with ftyp
Rar!     rar archives
```

all found media is given with assignment submission