Extracting images from the formatted disk has been an important issue for forensics analysts as well as the people who accidentally deleted their images from their disks. When the jpeg images are recently deleted, it is easy to recover them from the disk by programs such as Autopsy and Sleuthkit. These programs search through disks and finds many files from the disks, however, in many cases they are too complex for learners to use. Alternatively, there is PhotoRec, which is a very handy tool that can effectively recover images and other filetypes from the disks. However, when the disks are used for long time, there is a high chance that to have orphan image fragments whose header is erased from the disk and they just wait in the disk to be overwritten.

The main goal in this project is to recover those possible fragments from the disks which can be used for forensics analysts when those bytes can be re-constructed without header information. Although it is not possible to reconstruct images without knowing the Exif header of the image, there is a research which brute-forces to a byte-stream to determine Huffman, Quantization, Chroma subsampling values of it. To close the gap between reconstruction of image fragments and finding them in a disk, I have implemented this c++ project, which can be helpful for forensics analyst in the future.

The pseudocode for the project is as follows:

1) find the length of the disk image divide into 4KB blocks

2) iterate through the blocks

3) find empty block (blocks that has less than 100 not 0x00 bytes)

4) find possible image signatures

5) for each image signature found in the disk

6) read it and make sure it is real image

7) if real image

8) write it as img\_disk\_position.jpg

9) for each block which is not empty and no images found in it

10 find possible image fragment that are more than 64KB

11) if a continuous byte series doesn't have non-image characteristics

12) write it to the out\_folder/frag/ as frag\_position.frag

While testing the project, I found out that the program is finding the images embedded in .pdf, .ppt and other file types which stores the images as they are. This characteristic and extracting possible image fragments separates Jpeg Image & Fragment Extractor from other programs.