For a forensics analysis, every information on disk might be crucial to decide whether a person is guilty. One important information that can reveal a lot a person is images in their disks. Obtaining them is a crucial step for forensics analysis which requires knowledge of the where they are on the disk.

Although it is valuable to obtain all images, it is sometimes difficult to find them on the disks because many images are deleted or fragmented or overwritten by another file which might lead researchers/analyst lose very essential data about some criminals. There are programs that can find deleted images but when the image headers are deleted or corrupted the analysts can't reveal any information from those pieces and even not able to determine those pieces are images.

In this synopsis, I propose a new tool to help solve this problem which is to find the offsets of each image in a disk including fragmented and partially overwritten ones. The proposed method will apply multiple techniques to find all jpeg pieces on the disk. This tool will return users the beginning and end offset of jpeg images/fragments.

The aim of this tool is just to obtain the position of pieces, how these pieces can be combined or reconstructed is another problem to be solved. My goal is to find all possible image pieces with minimum the false positives and false negatives. I will test my program in both hard disk drive (HDD) and solid state drive (SSD or USB), however, it is expected to get better performance for HDD as HDD is more likely to keep the related pieces of images together.

For this project, I will use file signature information to find the Jpeg files and some heuristics to find the jpeg fragments in the disk. To decrease the false positive, I will set a threshold for the fragment size that the byte streams which are less than this threshold will be eliminated.