Assignment 1: File Carving

Total Points: 40

Due: October 04, 2017 (Wednesday) at 11:55 PM

Hello Detective Genius! Today, you are examining a memory stick we seized from a crime scene. There is one file inside this memory stick. Try opening it. Did it open? No?! It looks like the file is corrupted. Bummer! What do we do now? Well, let us try extracting what we can from it by writing a program in Python 2.7.

MD5 hash value of the source file: 906461e9d0a2716fa16b2420af1e8d53

Some investigative leads:

- There are four files you need to extract from this single corrupted file.
- The content of the file you received may have been *base64* encoded.
- I suggest looking for *JPEG*, *PDF*, *GIF*, and *PNG* files sequentially.
- A hex-editor may come in handy for this assignment.
- If you know your **Magic Numbers**, you are already halfway there.

The following are the MD5 hash values of the files you will be looking for:

File 1**:** c3a04e65e43b4a862b010927fae9aab1
File 2**:** 3b2f3b12ee4b04d4d0384adeee21e4d4
File 3**:** 06d08f17d7b2efbc0dc0d303398196d0
File 4**:** aec49002f8b02c2099152df1ec18b6c1

Bonus: There is an extra file, in addition to the first four files, within this file. If you extract it, you will be rewarded with five bonus points on this assignment.

Submission Guideline

1. Save all the files you extract with their proper extension.
2. Save your program (file_carving.py) you write to aid you in extracting these files.
3. Create a "*Read Me.pdf*" file containing:
    a. Your name
    b. A paragraph explaining how you successfully extracted the files (basically, all the steps you went through.)
    c. Short descriptions on how you used your program, how it works, and how to run it.
4. Compress all these files into a single *ZIP* file. Name your *ZIP* file "*LastName_Assignment_1.zip*" and upload it on Moodle before the deadline.

Good luck!