

CS 365: Digital Forensics

Spring 2020

Assignment #5

Arun Dunna
adunna@cs.umass.edu

Revision 1.0 - March 28, 2020

Due: April 3, 11:55pm

Submission Instructions

1. The assignment will be graded out of 100 points, such that up to 35 points are available for extra credit.
2. Your programming solutions for this assignment are to be written in **Python 3.6**.
3. Your programming solutions are to be submitted to the corresponding Gradescope programming assignment. These should be submitted in a **ZIP file** containing your Python code files, in the following format:

```
submission.zip
└─ parse.py
```

This will match the format of the assignment code distributable.

Alternatively, you can upload each Python file individually in Gradescope instead of using a ZIP file.

Prerequisites

1. Ensure that you are enrolled in the course on Gradescope. The assignment submission will open a few days before the deadline. If you have not been automatically enrolled, you can use the following enrollment code: **9DZ53K**
2. Setup and test your own environment for executing **Python 3.6** code. For example, this can be in an IDE such as PyCharm, or in a terminal with the **python3.6** command.
3. Obtain the assignment distributable from the course website: **asgn05distrib.zip**

1 Programming

The assignment distributable contains skeleton code in one file: `parse.py`. Edit the `parse.py` Python file to complete following functions, further described in the docstrings of each function in the skeleton code. You may assume that any files you are reading (passed into your functions as strings) exist.

1.1 FAT16 Parsing [100 points]

(40 points) `boot_sector_info(inputFile)`: extract information from the boot sector of a FAT16 FS

(25 points) `read_chain(fatTableBytes, startCluster)`: extract a given cluster chain from the FAT

(35 points) `directory_info(directoryBytes)`: given a bytes object, extract directory entries

1.2 Bonus: FAT16 Parsing, Level Two [35 points]

(20 points) `fat16_parse(inputFile)`: recursively parse all directory entries in a FAT16 FS

(15 points) `fragmented_score(inputFile, cost=5)`: generate a fragmented score to represent the fragmentation of a FAT16 FS