**CSE 469 Project Manual**

**Contributions:**

Ellery Leung:

address4forensics.py (Task 1a)

AAA.py (Task 2-1)

Brandon Nydam:

mac\_conversion.py (Task 1b)

AAA.py (Req. A & B)

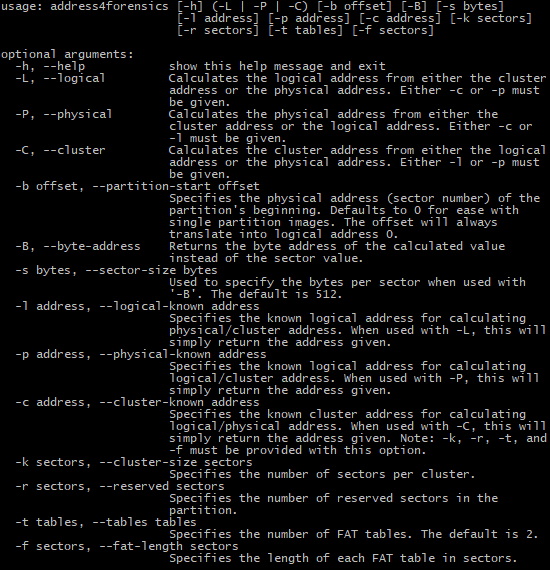
AAA.py (Task 2-2)

**Usage Instructions:**

\*\*RUN WITH PYTHON 3\*\*

We used Python 3 because it supports the function .hex(), which allowed us to conveniently convert byte strings to hex values.

python address4forensics.py {parameters here}



python mac\_conversion.py -T | -D [-f filename | -h hex value]

-T Use time conversion module. Either –f or –h must be given.  
-D Use date conversion module. Either –f or –h must be given.  
-f filename

This specifies the path to a filename that includes a hex value  
of time or date. Note that the hex value should follow this  
notation: 0x1234. For the multiple hex values in either a file  
or a command line input, we consider only one hex value so the  
recursive mode for MAC conversion is optional.

-h hexval

This specifies the hex value for converting to either date or  
time value. Note that the hex value should follow this notation:  
0x1234. For the multiple hex values in either a file or a  
command line input, we consider only one hex value so the  
recursive mode for MAC conversion is optional.

python AAA.py [image file]

AAA stands for Acquisition, Authentication, Analysis (aka Part 2).

Input the path to an image file in [image file].

The program will create a MD5-filename.txt and SHA1-filename.txt in the same directory before opening the image file.

Then, the program will extract the partition tables from the MBR.

Following this, the program will read each partition’s VBR, and if it is either FAT12/16 or FAT32, it will retrieve the geometric data of the file system.

**Screenshots:**

address4forensics:



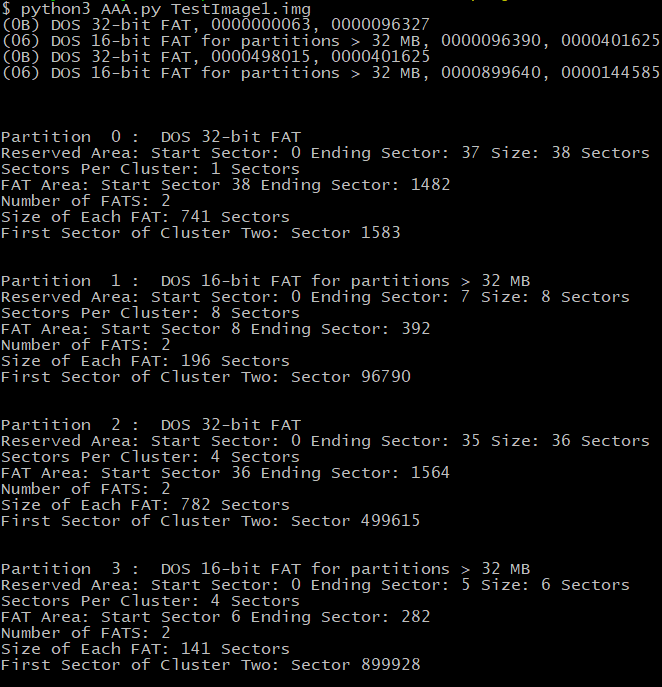
mac\_conversion with hex value:



mac\_conversion with text file (bad input discarded):



AAA with TestImage1.img:



AAA generating SHA-1 & MD5 to local directory text file:

