**Project Report - CSE 469**

Subhadarshi Samal(Task 1)

Rakeen Huq(Task 2)

**Overview**

The project is implemented using Python 3.5 and test on Windows 10 and Linux. The project goal to perform three main tasks of a forensics process - acquisition, authentication and analysis. The project is divided into three major tasks and each task is further divided into few sub tasks as per convenience. Task 1 is to implement a conversion utility which includes address conversion and mac conversion. Task 2 is to perform acquisition, authentication and analysis.

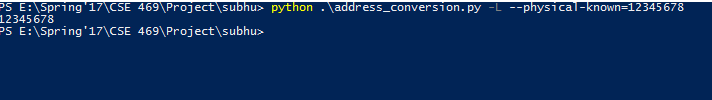
Argument handling is done using Python Argparse library.

# Argparse — Parser for command-line options, arguments and sub-commands.

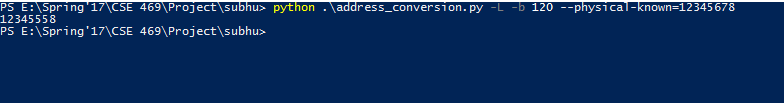
**Task 1(Part a)**

This task is to build two conversion utility. First, address conversion and second is MAC conversion. In address conversion, three type of memory addresses such as logical, physical and cluster are being derived from one another.

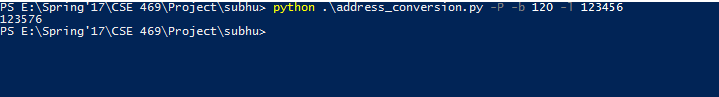
Logical address of physical sector when partition begins at sector 0.



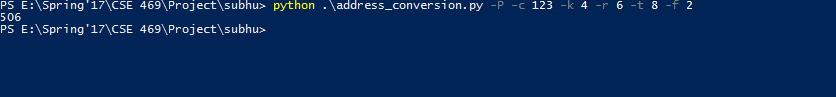
Logical address of a physical sector than begins at physical sector 120



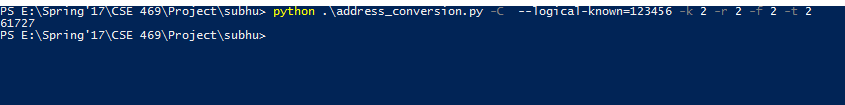
Physical address, when logical address and start sector is known.



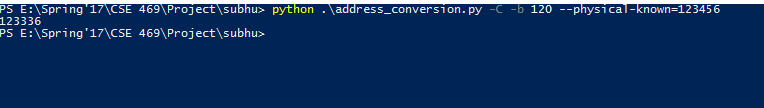
Physical address, when cluster address is known. Value of k, r, t, f must be provided.



Cluster address, when logical address is known. Value of k,r,t,f must be provided



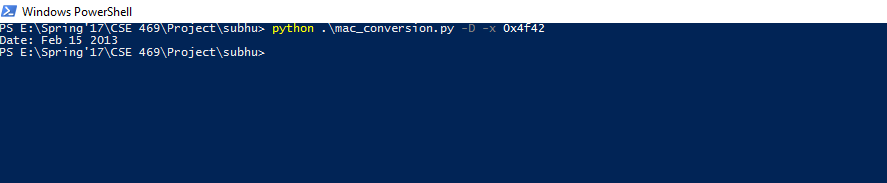
Cluster address, when physical address and start address is known.



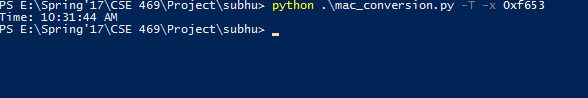
**Task 1(Part b)**

Part b is MAC conversion. The input can be provided through input file or directly as a hex value argument. We assume a little endian ordering is applied.

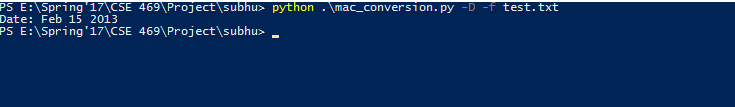
This example shows the date conversion with the hex value as an input:



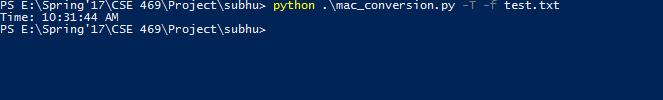
Time conversion with the hex input.



Date conversion with the file input. File contains the hex value.



Time conversion with the file as input.



**Task 2. Acquisition, Authentication, and Analysis**

In Task 2 we must provide a raw image file as input to be parsed by our program. This Task has a total of 3 parts: Obtain MD5 and SHA1 values from the image file and output them as text files with the name being the same as the input imae file. Output Partition type as well as start sector address and partition size in sectors, and finally if the partition is of type FAT16/FAT32 output extra information.

**How to run Code:**

The code was written to be compatible with python 3.6, and was tested on linux mint using python 3.5.2

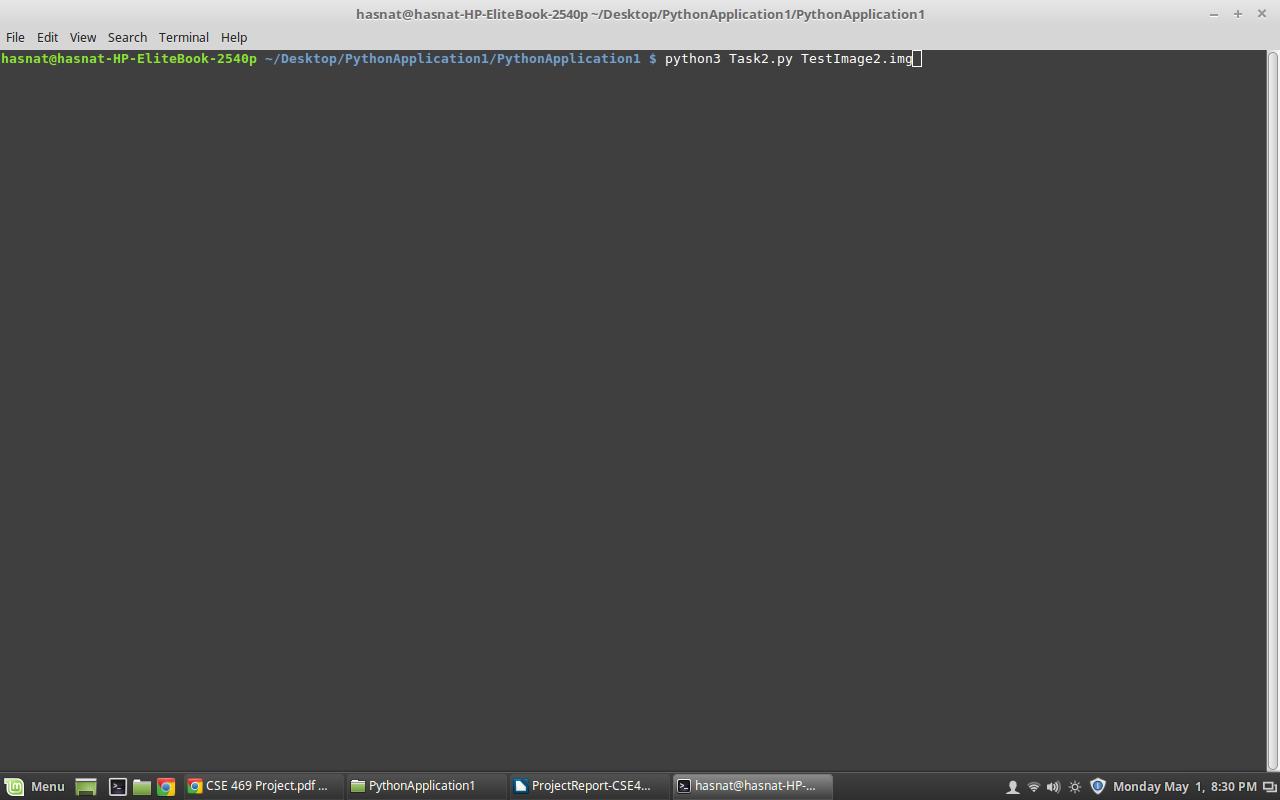
The name of the python file is **Task2.py**

When executing the code, the terminal should be opened **in the directory containing the python file(Task2.py).**

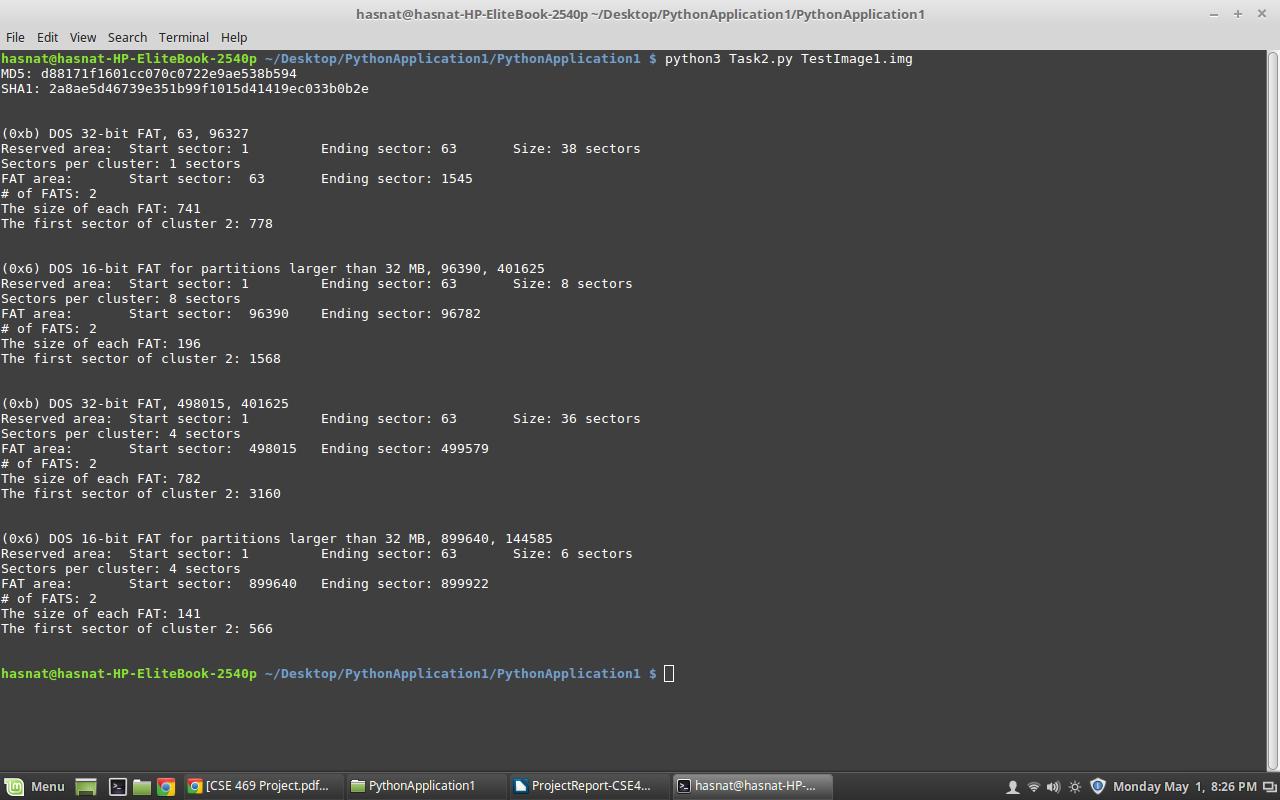
The code takes in an image filename as argument. Format: *imageName.img*

**Execute:** python3 Task2.py TestImage1.img

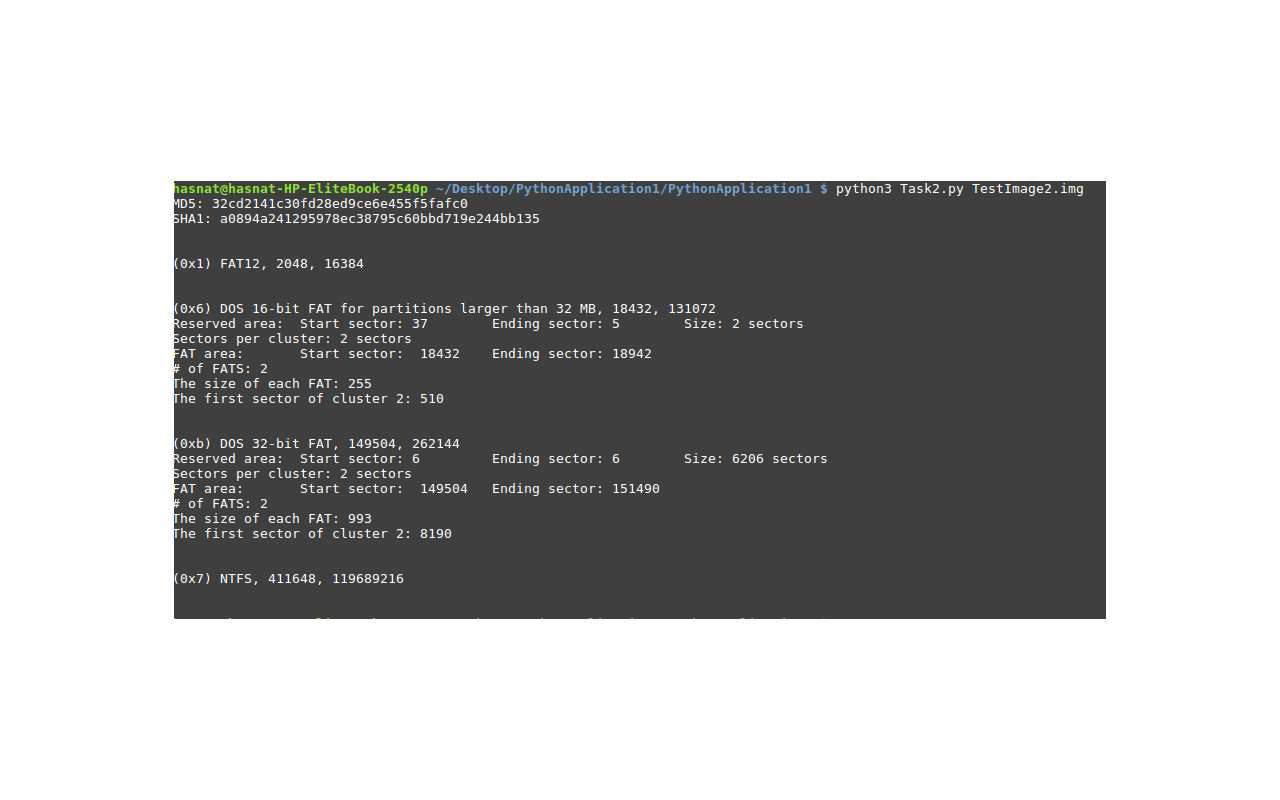
**Here is a sample image on how to execute:**



Here is a sample output of TestImage1.img when you run the above code:



And here is the output of TestImage2.img:



**References:**

<https://www.youtube.com/watch?v=rnatu3xxVQE>

<https://martin-thoma.com/how-to-parse-command-line-arguments-in-python/>

<http://www.bogotobogo.com/python/python_argparse.php>

<https://mkaz.tech/code/python-argparse-cookbook/>

<http://bioportal.weizmann.ac.il/course/python/PyMOTW/PyMOTW/docs/argparse/index.html>

<https://github.com/brutalhonesty/cse469-project1/blob/master/mac_conversion.py>

<https://github.com/Landreth/2012-Spring-CSE494-598_G-Project/blob/master/CSE494Project/address4forensics/address4forensics.py>

<http://stackoverflow.com/questions/9210525/how-do-i-convert-hex-to-decimal-in-python>

<http://stackoverflow.com/questions/10411085/converting-integer-to-binary-in-python>

<https://www.quora.com/How-can-I-convert-hex-to-decimal-in-Python>

<http://stackoverflow.com/questions/311627/how-to-print-date-in-a-regular-format-in-python>

<https://pymotw.com/2/datetime/>

<http://stackoverflow.com/questions/13855111/how-can-i-convert-24-hour-time-to-12-hour-time>

<http://stackoverflow.com/questions/1759455/how-can-i-account-for-period-am-pm-with-datetime-strptime>

<http://stackoverflow.com/questions/25541703/date-string-to-time-tuple-python>