##

Assignment - 6

(16SN602 -Memory Forensics)

By:- Pratyush and Sreelakshmi

Department Of Cyber Security Systems and Networks

##

***Deadline* -** Friday 23/02/2018 11.55 pm.
Submission is on AUMS

Brother Trouble!!!
I had left my computer open and had gone away for a while when my brother, who takes pride in his ability to use the command prompt, did something with the system. I managed to get a memory dump of the system. Can you find out what he actually did ?

1.) Given the Memory Dump you are required to:
   - Find the profile using the tool/commands mentioned in the class.
   - Find out the commands executed in cmd before the Memory Dump has been taken.
   - Find the "Flag", which is in the format inctfj{<md5 hash of the full command executed>}

2.) Write a write-up stating:
   - Your name and roll no.
   - Tools used.
   - Complete walkthrough of how you approached.
   - Commands you use to find out the necessary results and why?

**Read about ways you can execute commands in cmd.

Code of Conduct:

- ***Plagiarism*** will result in direct ***zero*** for the assignment.
- Deadline should be followed ***strictly***. Submission after the deadline without prior information of any valid reason could result into losing marks.