**Challenge #5**

**Mid Term Capture the Flag**

**Cyber 262**

Please write a Python program to analyze all of the three given log files and print to console the following outputs:

* The Attack Description, which is given to you as part of this challenge, contains six blue color text boxes;
* Each blue color text box represents a malicious event; the red color edges between the blue color text boxes represent the time order between the malicious events;
* Among the three log files, only one log file contains these malicious events;
* After you identify the log file that contains these malicious event, for each blue color text box you detect in the log, please output the following:
  + The timestamp of the corresponding event;
  + The pid;
  + The command line command, if any, which was executed by the attacker when this event happened;

**What to submit**:

* Your Python program
* The outputs you get (in a txt file)

Please put all these items in a folder and compress the folder into a single ZIP archive file. Include your team name in the file name of the ZIP archive.