

CMSY 156 – Final Project

Copyright ©2022 – Howard Community College All rights reserved; Unauthorized duplication prohibited.

You have been hired as a threat detection analyst for a bank. Part of your job is inspecting IP logs to try to find any potential security threats.

An IP version 4 address contains 4 octets of numbers between 0 and 255. They are in a format such as:

192.116.234.122

For purposes of this lab, all the IPv4 addresses have the full octet, even if the number starts with 0. As such, 78.82.123.145 would be stored as 078.082.123.145.

Professor Offenbergs teaches an excellent Ethical Hacking class here at HCC. Unfortunately, his evil twin brother, Darth Offenbergs, is the head of the international crime group Offenbergs's Unethical Computer Hackers (OUCH). Hackers from OUCH are trying to penetrate your system. OUCH always uses one of three IP address ranges:

1. 168.193
2. 224.174
3. 233.012

You have been forwarded a file called "ipfile.txt". This file contains an unknown number of IP addresses and the data and time that the IP address accessed your system. Your job is to read the file, find all the suspect IP addresses that might have been used by OUCH, and produce an output report to both the screen and to an output file.

1. The program must allow the user to enter in the name of the input file:
 - a. The program must call a function that receives the input filename as a parameter
 - b. The program must use a try..except block to test that the file exists; if it does not exist, the program must display the appropriate error message and allow the reentry of the filename
 - c. Once the program determines that the file exists, the function must return the file handle
2. The program must allow the user to enter in the name of the output file:
 - a. The program must call the same function as above that receives the output filename as a parameter
 - b. The program must use a try..except block to test that the file can be created; if it cannot be created, the program must display the appropriate error message and allow the reentry of the filename
 - c. Once the program determines that the file can be created, the function must return the file handle

CMSY 156 – Final Project

Copyright ©2022 – Howard Community College All rights reserved; Unauthorized duplication prohibited.

3. The program must read all the data in the input file as strings:
 - a. The program must keep a count of the total number of records in the file
 - b. The program must create a list of strings that contains all the suspect IP Addresses; these are IP addresses that start with the values listed above
 - c. Once the entire file is read, the program must close the file
4. The program must create and call a function to create the output report:
 - a. The function must take the total number of records in the file, the list of suspect IP addresses and the output file handle as parameters
 - b. The function must create the output report as displayed in the screen shot below; the output report MUST match the screen shot exactly
 - c. The function must create the output file with the exact format as shown in the screen shot below; again, the output format must match the screen shot exactly
 - d. The output report must contain the following:
 - i. The number of records in the file
 - ii. The number of suspect IP addresses (the number must be determined using a list function)
 - iii. The percentage of IP addresses that are suspect (formatted to display to 3 decimal places)
 - iv. The list of suspect IP addresses sorted by the IP address (the code must use a list function to perform this sort and string slicing to separate the IP address from the data and time stamp)
 - e. The function must close the output file once the output report is complete
5. The code must display an end of program message

CMSY 156 – Final Project

Copyright ©2022 – Howard Community College All rights reserved; Unauthorized duplication prohibited.

Here is the screen shot. Note: This uses a test file and is not the file that you will be downloading from Canvas.

```
===== RESTART: C:\Users\bnb21\Downloads\final_project.py =====
Enter the input file name: c:\\test\\iperror.txt

ERROR -- There is an issue with file c:\\test\\iperror.txt. Please reenter:

Enter the input file name: c:\\test\\ipfile_test.txt
Enter the output file name: s:\\test\\badip.txt

ERROR -- There is an issue with file s:\\test\\badip.txt. Please reenter:

Enter the output file name: c:\\test\\badip.txt

Output Report
-----
The total number of records in the file is: 100000

The number of suspect IP addresses is: 2

The percentage of suspect IP addresses is: 0.002

Suspect IP Addresses
-----
IP Address = 233.012.063.200   Date and Time = Wed Jul  6 08:25:46 2022
IP Address = 233.012.196.049   Date and Time = Wed Jul  6 08:25:48 2022

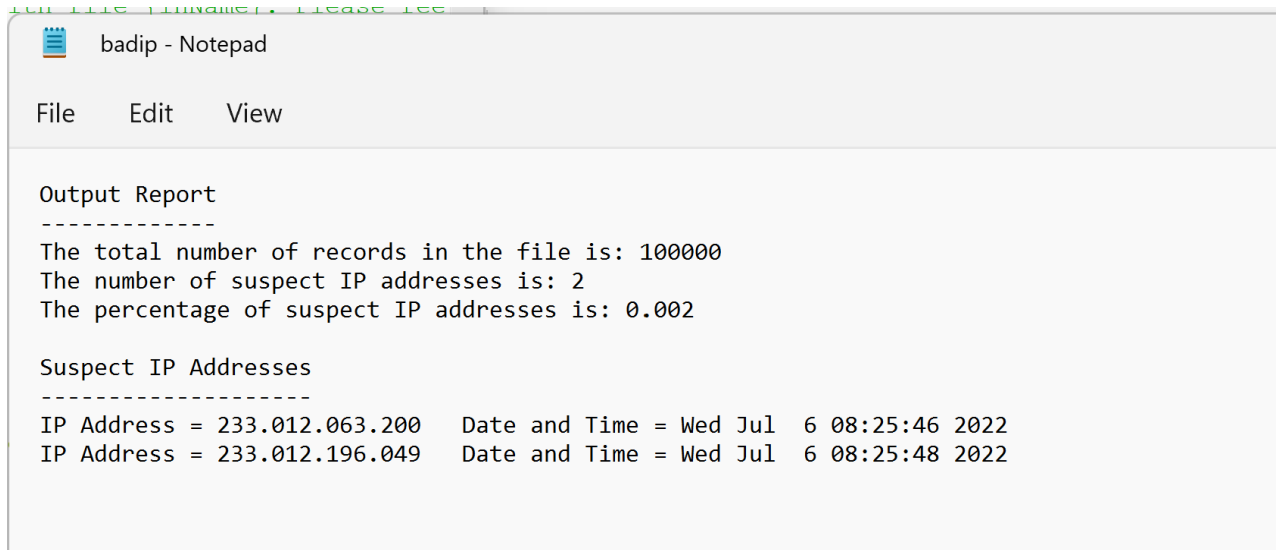
Program complete!
>>>
```

CMSY 156 – Final Project

Copyright ©2022 – Howard Community College All rights reserved; Unauthorized duplication prohibited.

Notes:

1. Submit the .py file and the “badip.txt” output file in Canvas.
2. Any actions involving the list must use list functions; the code MUST create a list of the suspect IP addresses
3. The output file must look exactly like this:



```
badip - Notepad

File Edit View

Output Report
-----
The total number of records in the file is: 100000
The number of suspect IP addresses is: 2
The percentage of suspect IP addresses is: 0.002

Suspect IP Addresses
-----
IP Address = 233.012.063.200    Date and Time = Wed Jul  6 08:25:46 2022
IP Address = 233.012.196.049    Date and Time = Wed Jul  6 08:25:48 2022
```