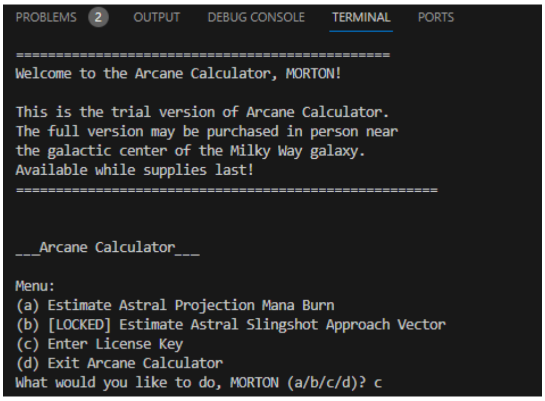
WRITE-UP TASKPHASE 2
KEYGENME-py(PicoCTF)

Apps Used: VS Code.

In this CTF problem we get a 200+ line python code, in order to run this program we had to install the following in the cmd promp using

"pip install python-cryptography-fernet-wrapper"

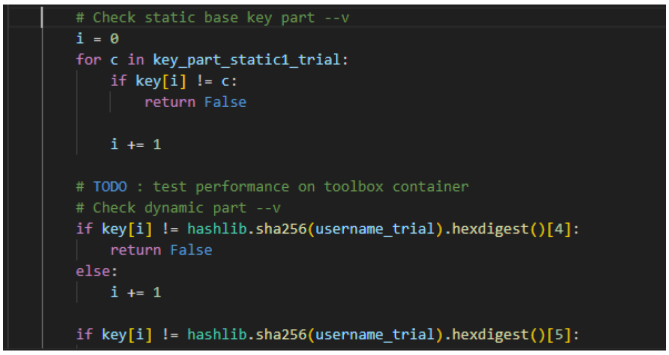
After running it we can see it gives the following output



```
===============================================
Welcome to the Arcane Calculator, MORTON!

This is the trial version of Arcane Calculator.
The full version may be purchased in person near
the galactic center of the Milky Way galaxy.
Available while supplies last!
=====================================================


___Arcane Calculator___

Menu:
(a) Estimate Astral Projection Mana Burn
(b) [LOCKED] Estimate Astral Slingshot Approach Vector
(c) Enter License Key
(d) Exit Arcane Calculator
What would you like to do, MORTON (a/b/c/d)? c
```

here we can estimate astral projection mana burn with a star of our choice etc, but in order to enter license key we had to choose option C

Now we'll check through the code what is coded inside option C

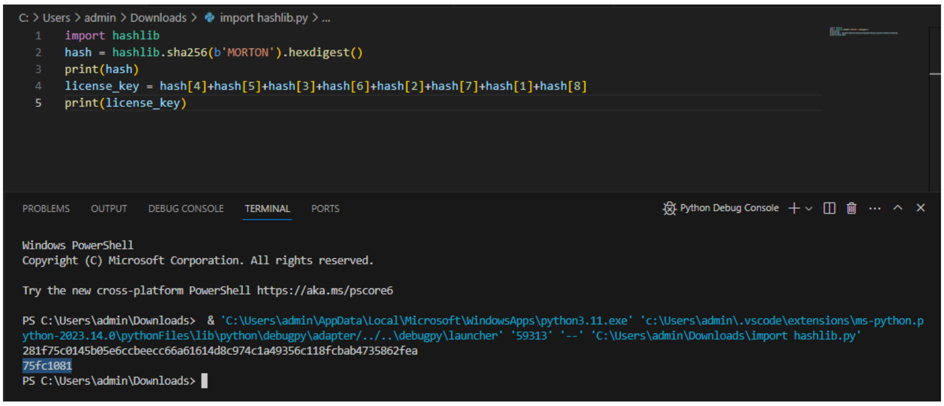


```
# Check static base key part --v
i = 0
for c in key_part_static1_trial:
    if key[i] != c:
        return False

    i += 1

# TODO : test performance on toolbox container
# Check dynamic part --v
if key[i] != hashlib.sha256(username_trial).hexdigest()[4]:
    return False
else:
    i += 1

if key[i] != hashlib.sha256(username_trial).hexdigest()[5]:
```

for inside C option we can see the route to obtain the license key of the code but first we'll get it by running the code separately, here the username_trial is "MORTON" but apparently that didn't work so we decided to go with bUsername_trial which was b"Morton".

In the code we also see below username_trial it has static and dynamic part of the password
which means our password is of the form

“picoCTF{1n_7h3_|<3y_of_xxxxxxxx}” here xxxxxxxx is the dynamic part which we’ll get after decoding the hashlib code stuff in new window which we receive as:



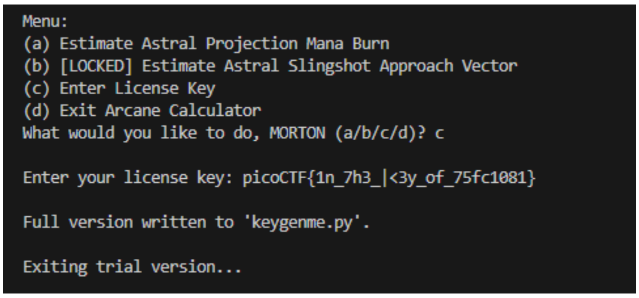
```python
import hashlib
hash = hashlib.sha256(b'MORTON').hexdigest()
print(hash)
license_key = hash[4]+hash[5]+hash[3]+hash[6]+hash[2]+hash[7]+hash[1]+hash[8]
print(license_key)
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\admin\Downloads>  & 'C:\Users\admin\AppData\Local\Microsoft\WindowsApps\python3.11.exe' 'c:\Users\admin\.vscode\extensions\ms-python.p
ython-2023.14.0\pythonFiles\lib\python\debugpy\adapter/../..\debugpy\launcher' '59313' '--' 'C:\Users\admin\Downloads\import hashlib.py'
281f75c0145b05e6ccbeecc66a61614d8c974c1a49356c118fcbab4735862fea
75fc1081
PS C:\Users\admin\Downloads>
```

here main stuff’s particular index makes up our dynamic password and our overall password is

“picoCTF{1n_7h3_|<3y_of_75fc1081}”

we can exit trial version and get full version by typing this in main program’s option c as shown



```
Menu:
(a) Estimate Astral Projection Mana Burn
(b) [LOCKED] Estimate Astral Slingshot Approach Vector
(c) Enter License Key
(d) Exit Arcane Calculator
What would you like to do, MORTON (a/b/c/d)? c

Enter your license key: picoCTF{1n_7h3_|<3y_of_75fc1081}

Full version written to 'keygenme.py'.

Exiting trial version...
```

our flag is the same as our password which is

picoCTF{1n_7h3_|<3y_of_75fc1081}

Name: Atharva Mishra

“Keygenme-py”