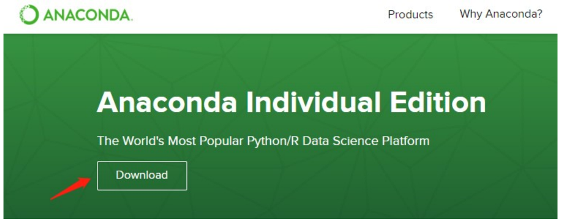
1. Go to this web site: https://www.anaconda.com/distribution/

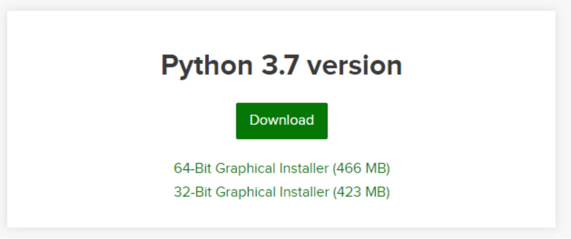
2. Click the download button on the page:



Anaconda Individual Edition

The World's Most Popular Python/R Data Science Platform

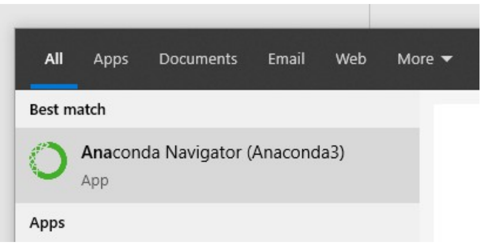
3. Download Python 3.7 version, 64-bit.



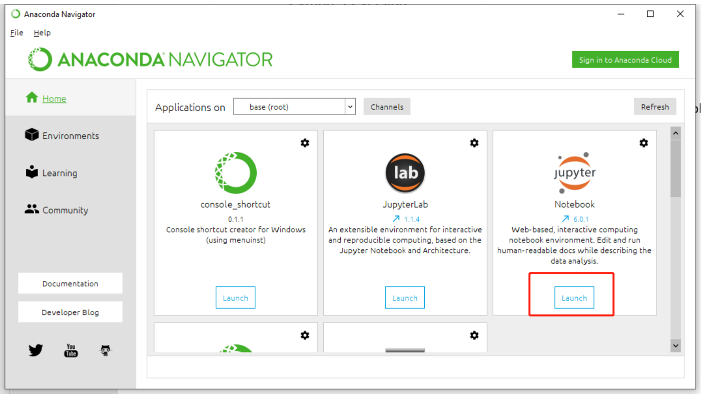
64-Bit Graphical Installer (466 MB)
32-Bit Graphical Installer (423 MB)

Note: Just install the Anaconda package, it will include all the Python 3.7 executable, libraries and tools, which means you don't need to install a standalone Python again.

4. Run Anaconda Navigator.



5. Launch Jupyter Notebook from the navigator.

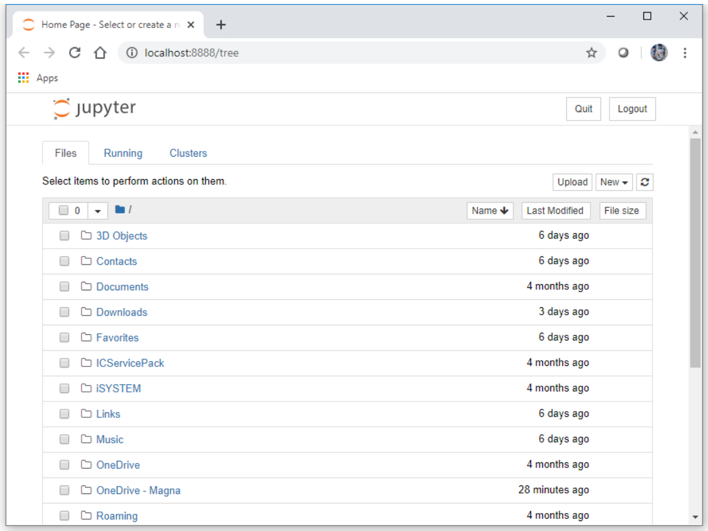


Console shortcut creator for Windows (using menuinst)

An extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture.

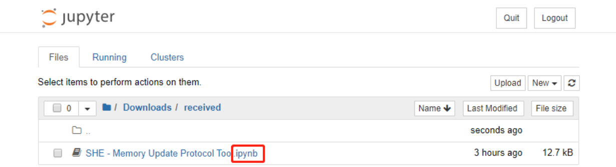
Web-based, interactive computing notebook environment. Edit and run human-readable docs while describing the data analysis.

6. Jupyter Notebook is a web-based tool, it will automatically open a web-page from your default web browser.



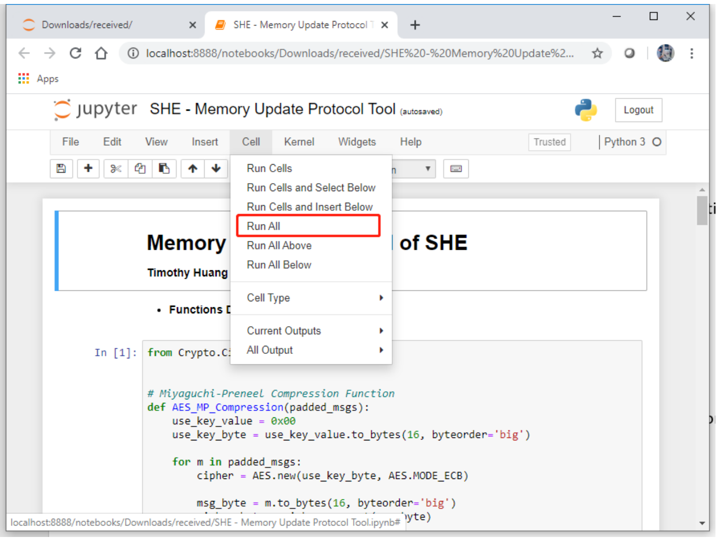
Name	Last Modified
3D Objects	6 days ago
Contacts	6 days ago
Documents	4 months ago
Downloads	3 days ago
Favorites	6 days ago
ICServicePack	4 months ago
iSYSTEM	4 months ago
Links	6 days ago
Music	6 days ago
OneDrive	4 months ago
OneDrive - Magna	28 minutes ago
Roaming	4 months ago

7. The web-page will looks like a file system, you can navigate to the location where you save the script file (a .ipynb file).



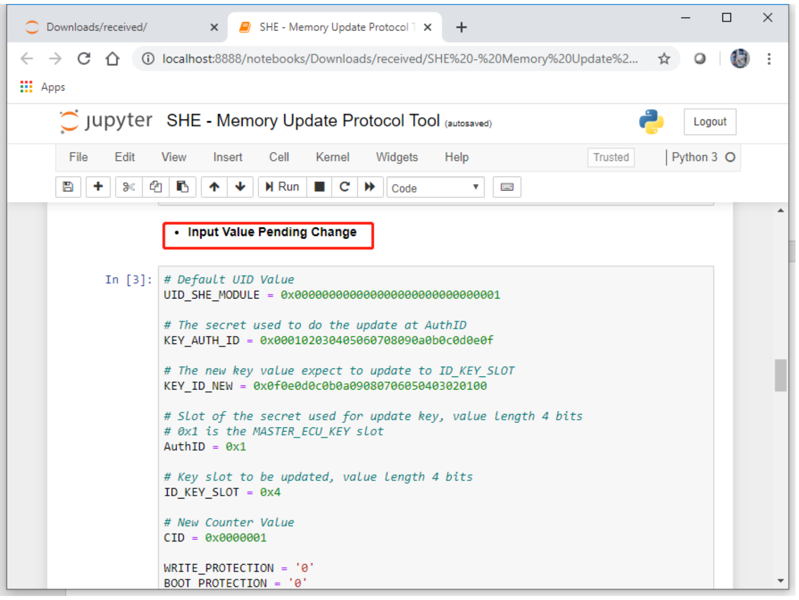
Name	Last Modified	File size
..	seconds ago	
SHE - Memory Update Protocol Tool.ipynb	3 hours ago	12.7 kB

8. Click the file name to open the script. It will open a new page that contains the script which is able to run. Click **Cell→Run All** every time when you update your input.


Downloads/received/
SHE - Memory Update Protocol T
localhost:8888/notebooks/Downloads/received/SHE%20-%20Memory%20Update%2...
Apps
jupyter SHE - Memory Update Protocol Tool (autosaved)
Logout
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Trusted
Python 3
Run Cells
Run Cells and Select Below
Run Cells and Insert Below
Run All
Run All Above
Run All Below
Cell Type
Current Outputs
All Output
Memory
of SHE
Timothy Huang
Functions D
localhost:8888/notebooks/Downloads/received/SHE - Memory Update Protocol Tool.ipynb#

```
In [1]: from Crypto.Ci


        # Miyaguchi-Preneel Compression Function
        def AES_MP_Compression(padded_msgs):
            use_key_value = 0x00
            use_key_byte = use_key_value.to_bytes(16, byteorder='big')

            for m in padded_msgs:
                cipher = AES.new(use_key_byte, AES.MODE_ECB)

                msg_byte = m.to_bytes(16, byteorder='big')
                                                     yte)
```

9. To modify your input, go to cell 3 with the title – Input Value Pending Change.

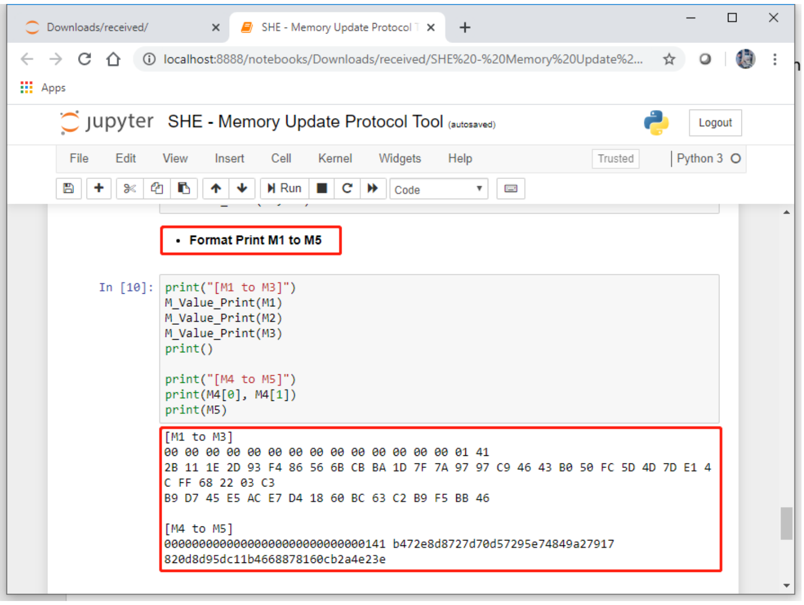

Downloads/received/
SHE - Memory Update Protocol T
localhost:8888/notebooks/Downloads/received/SHE%20-%20Memory%20Update%2...
Apps
jupyter SHE - Memory Update Protocol Tool (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3
Run
Code

- **Input Value Pending Change**

In [3]:

```
# Default UID Value
UID_SHE_MODULE = 0x00000000000000000000000000000001

# The secret used to do the update at AuthID
KEY_AUTH_ID = 0x000102030405060708090a0b0c0d0e0f

# The new key value expect to update to ID_KEY_SLOT
KEY_ID_NEW = 0x0f0e0d0c0b0a09080706050403020100

# Slot of the secret used for update key, value length 4 bits
# 0x1 is the MASTER_ECU_KEY slot
AuthID = 0x1

# Key slot to be updated, value length 4 bits
ID_KEY_SLOT = 0x4

# New Counter Value
CID = 0x0000001

WRITE_PROTECTION = '0'
BOOT_PROTECTION = '0'
```

10. To view your M1 to M5 result, go to cell 10 with the title – Format Print M1 to M5.
    1) Copy paste the M1 to M3 values line by line to CANoe for target ***RID*** and start the routine.
    2) Run request result to get M4 and M5 from the ECU and compare if the values are the same as the output from the script.


Downloads/received/
SHE - Memory Update Protocol T
localhost:8888/notebooks/Downloads/received/SHE%20-%20Memory%20Update%2...
Apps
jupyter SHE - Memory Update Protocol Tool (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3
Run
Code

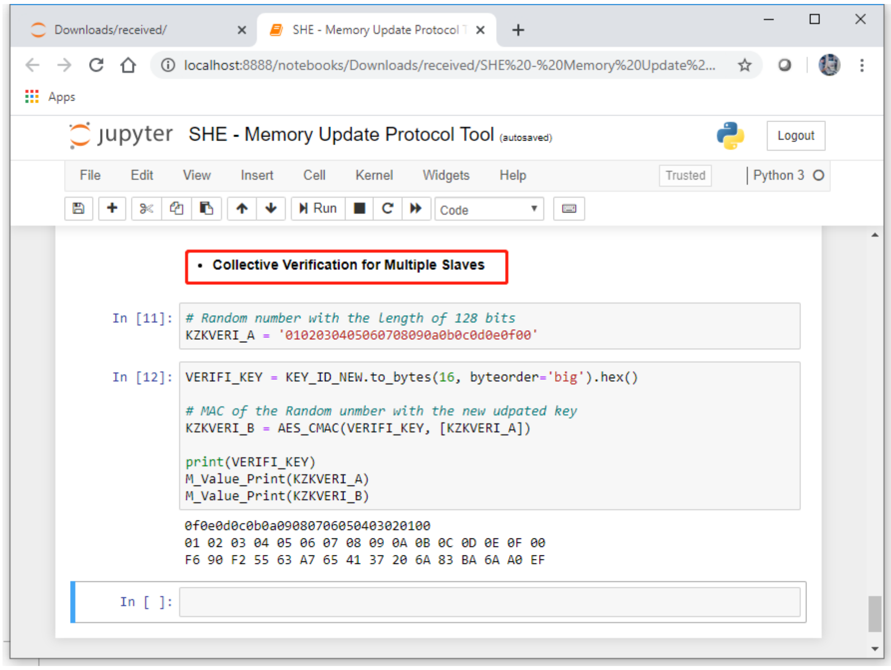
- **Format Print M1 to M5**

In [10]:

```
print("[M1 to M3]")
M_Value_Print(M1)
M_Value_Print(M2)
M_Value_Print(M3)
print()

print("[M4 to M5]")
print(M4[0], M4[1])
print(M5)
```

```
[M1 to M3]
00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 41
2B 11 1E 2D 93 F4 86 56 6B CB BA 1D 7F 7A 97 97 C9 46 43 B0 50 FC 5D 4D 7D E1 4
C FF 68 22 03 C3
B9 D7 45 E5 AC E7 D4 18 60 BC 63 C2 B9 F5 BB 46

[M4 to M5]
00000000000000000000000000000141 b472e8d8727d70d57295e74849a27917
820d8d95dc11b4668878160cb2a4e23e
```

11. The script under title – Collective Verification for Multiple Slaves, is for target ***RID***. You are only allowed to modify cell 11 for the random number.



Downloads/received/
SHE - Memory Update Protocol
localhost:8888/notebooks/Downloads/received/SHE%20-%20Memory%20Update%2...
Apps
jupyter SHE - Memory Update Protocol Tool (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3
Run
Code

- **Collective Verification for Multiple Slaves**

```
In [11]: # Random number with the length of 128 bits
         KZKVERI_A = '0102030405060708090a0b0c0d0e0f00'
```

```
In [12]: VERIFI_KEY = KEY_ID_NEW.to_bytes(16, byteorder='big').hex()

         # MAC of the Random unmber with the new udpated key
         KZKVERI_B = AES_CMAC(VERIFI_KEY, [KZKVERI_A])

         print(VERIFI_KEY)
         M_Value_Print(KZKVERI_A)
         M_Value_Print(KZKVERI_B)

         0f0e0d0c0b0a09080706050403020100
         01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00
         F6 90 F2 55 63 A7 65 41 37 20 6A 83 BA 6A A0 EF
```

```
In [ ]:
```