



life.augmented

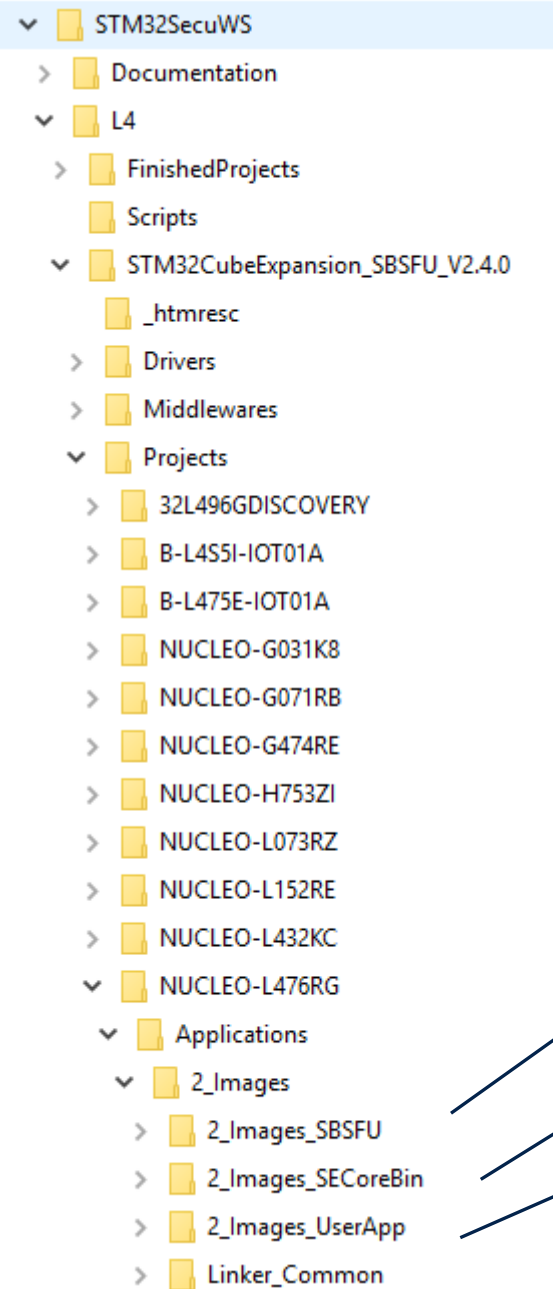
STM32 security workshop

SBSFU Homework

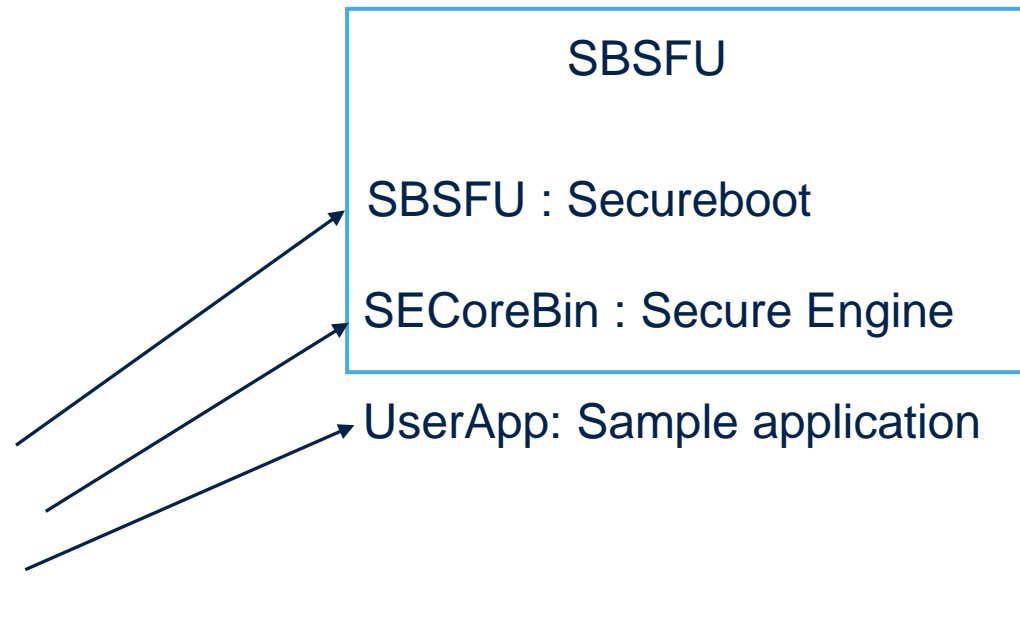
Purpose

- The purpose of this homework is to prepare your environment to be ready for the workshop hands-on related to SBSFU
- The following slides detail
 - How to build SBSFU
 - How to flash on STM32L4 target to check everything is working fine

Setup environment

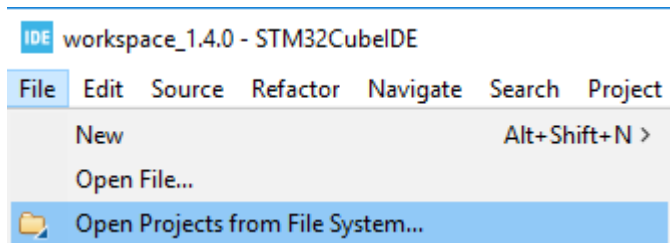
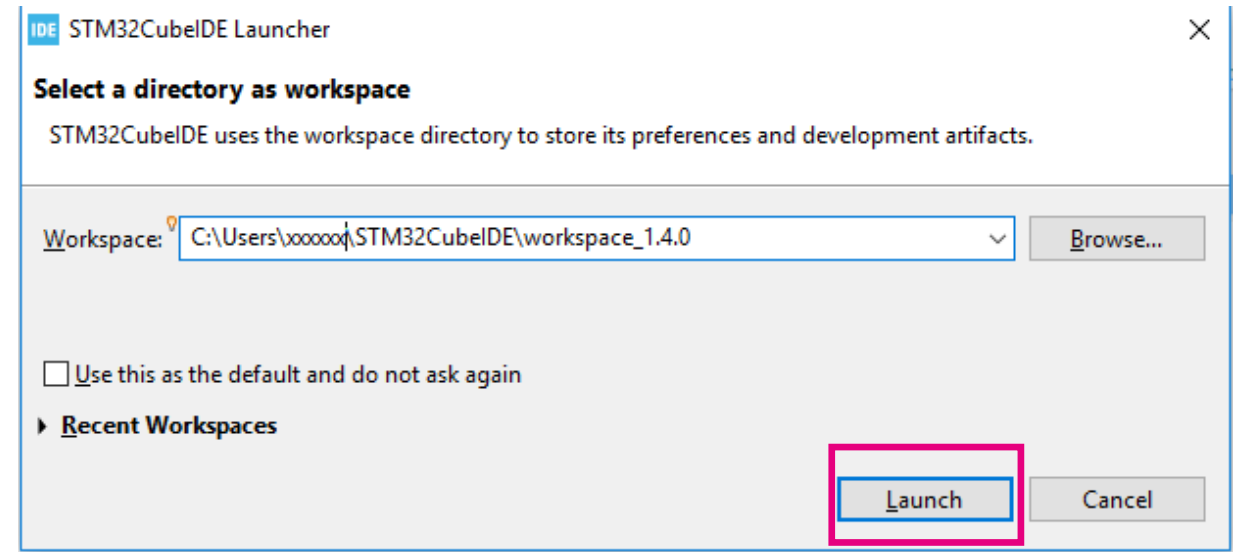


- SBSFU package in this folder : C:\STM32SecuWS\L4
- Package structure : 3 projects



Import projects in CubeIDE

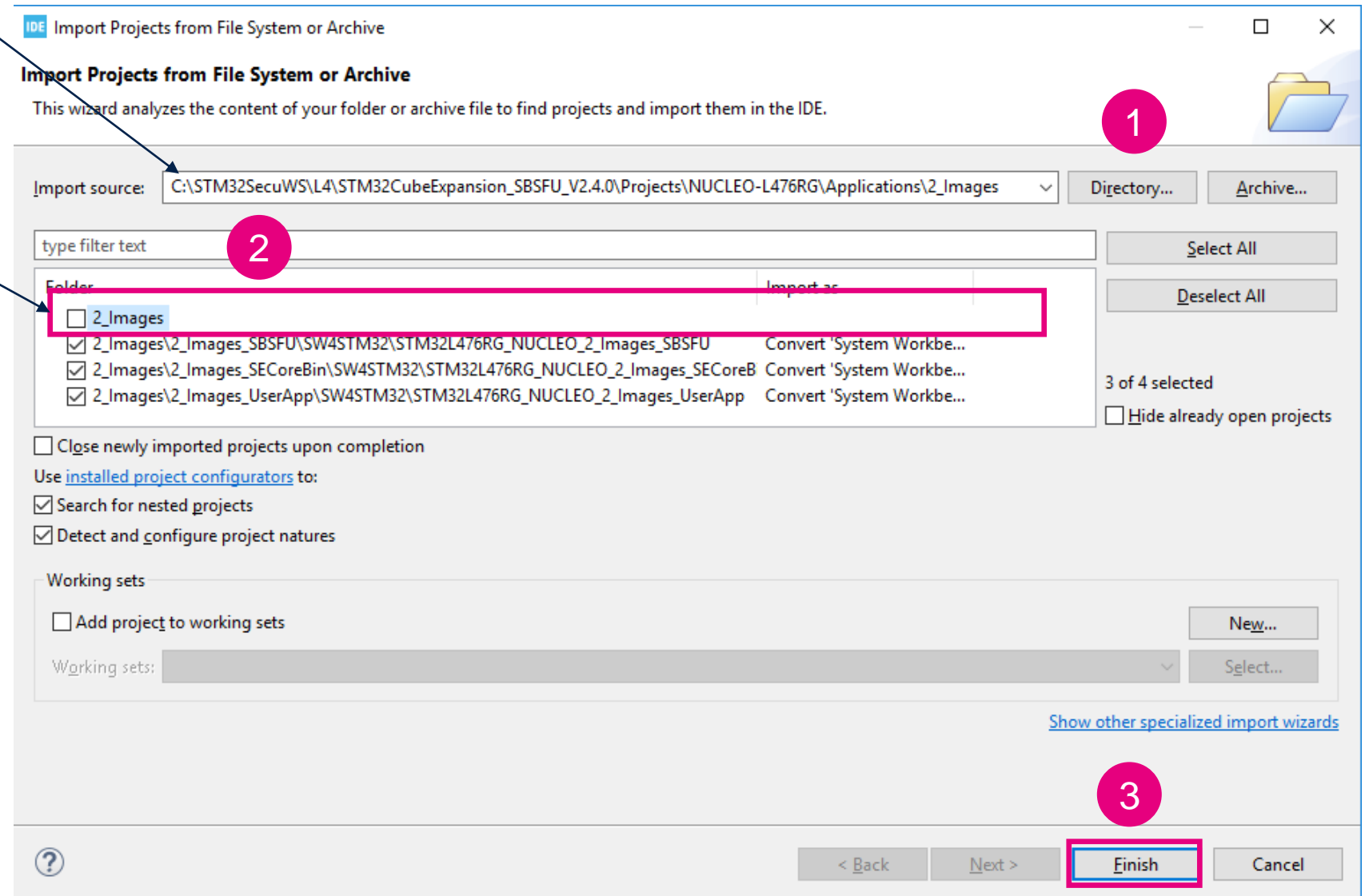
- Launch CubeIDE
- Select a workspace, click on Launch
- Open a project






Import SBSFU in CubeIDE

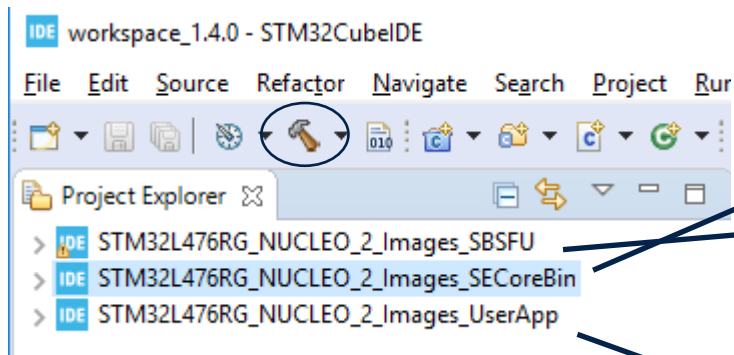
C:\STM32SecuWS\L4\STM32CubeExpansion_SBSFU_V2.4.0\Projects\NUCLEO-L476RG\Applications\2_Images

IMPORTANT !
Uncheck the first line



Build the SBSFU for NucleoL476RG

- Use the hammer to build in following order
 - Click on SECorebin project then  and wait completion
 - Click on SBSFU project then  and wait completion
 - Click on UserApp project then  and wait completion



```
arm-none-eabi-gcc -mcpu=cortex-m4 -g3 -c -x assembler-with-cpp -MMD -MP -MFApp1
arm-none-eabi-gcc -o "SECoreBin.elf" @objects.list -l:libSTM32CryptographicV3
Finished building target: SECoreBin.elf

arm-none-eabi-size SECoreBin.elf
text data bss dec hex filename
20424 88 2616 23128 5a58 SECoreBin.elf
Finished building: default.size.stdout

arm-none-eabi-objdump -h -S SECoreBin.elf > "SECoreBin.list"
Finished building: SECoreBin.list

arm-none-eabi-objcopy -O binary SECoreBin.elf "SECoreBin.bin"
Finished building: SECoreBin.bin

14:02:51 Build Finished. 0 errors, 0 warnings. (took 28s.519ms)
```

```
arm-none-eabi-objcopy -O binary "SBSFU.elf" "SBSFU.bin"
Finished building: SBSFU.bin

arm-none-eabi-objcopy -O binary "SBSFU.elf" "SBSFU.bin"
arm-none-eabi-size "SBSFU.elf"
text data bss dec hex filename
59578 296 10584 70458 1133a SBSFU.elf
arm-none-eabi-objcopy -j .SE_IF_Code "SBSFU.elf" se_inter.elf > /dev/null 2>>1
arm-none-eabi-objcopy --extract-symbol se_inter.elf se_interface_app.elf
arm-none-eabi-objcopy -S --keep-symbols=../se_interface.txt se_interface_app.elf se_interface_app.o

14:09:52 Build Finished. 0 errors, 0 warnings. (took 1m:10s.608ms)
```

```
arm-none-eabi-size
text data
21632 176
Finished building: default.size.stdout

arm-none-eabi-objdump -h -S UserApp.elf > "UserApp.list"
Finished building: UserApp.list

arm-none-eabi-objcopy -O binary UserApp.elf "UserApp.bin"
Finished building: UserApp.bin

arm-none-eabi-objcopy -O binary "UserApp.elf" "../UserApp.bin"
arm-none-eabi-size "UserApp.elf"
text data bss dec hex filename
21632 176 6000 27808 6ca0 UserApp.elf
"../../../../2_Images_SECoreBin/SW4STM32/postbuild.sh" "../" "../UserApp.elf" "../UserApp.bin" "1" "1"
prepareimage with windows executable

14:13:03 Build Finished. 0 errors, 0 warnings. (took 50s.309ms)
```

What was actually done

- The SBSFU build process makes things simple
- It generates automatically 2 binaries.

File Explorer window showing the directory structure for the SBSFU build process. The path is C:\STM32SecuWS\L4\STM32CubeExpansion_SBSFU_V2.4.0\Projects\NUCLEO-L476RG\Applications\2_Images\2_Images_UserApp\Binary.

The left pane shows the folder hierarchy:

- NUCLEO-L476RG
 - Applications
 - 2_Images
 - 2_Images_SBSFU
 - 2_Images_SECoreBin
 - 2_Images_UserApp
 - Binary
 - EWARM
 - Inc
 - MDK-ARM
 - Src
 - SW4STM32
 - Linker_Common

The right pane shows the files in the Binary folder:

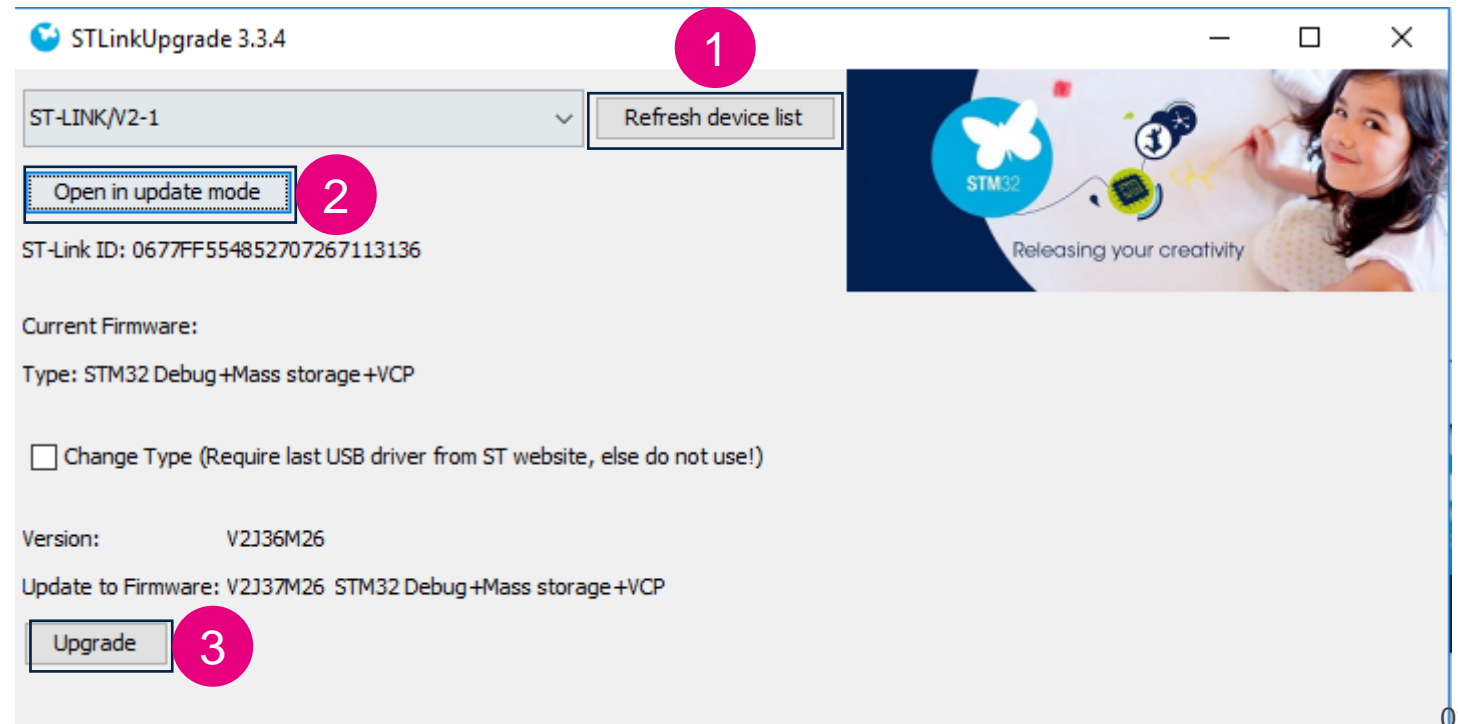
Name	Date modified	Type	Size
SBSFU_UserApp.bin	28-Jul-20 2:13 PM	BIN File	558 KB
UserApp.sfb	28-Jul-20 2:13 PM	SFB File	22 KB

Arrows point from the files to callout boxes:

- SBSFU_UserApp.bin points to a box labeled **SBSFU bootloader + User Application**.
- UserApp.sfb points to a box labeled **User Application update file**.

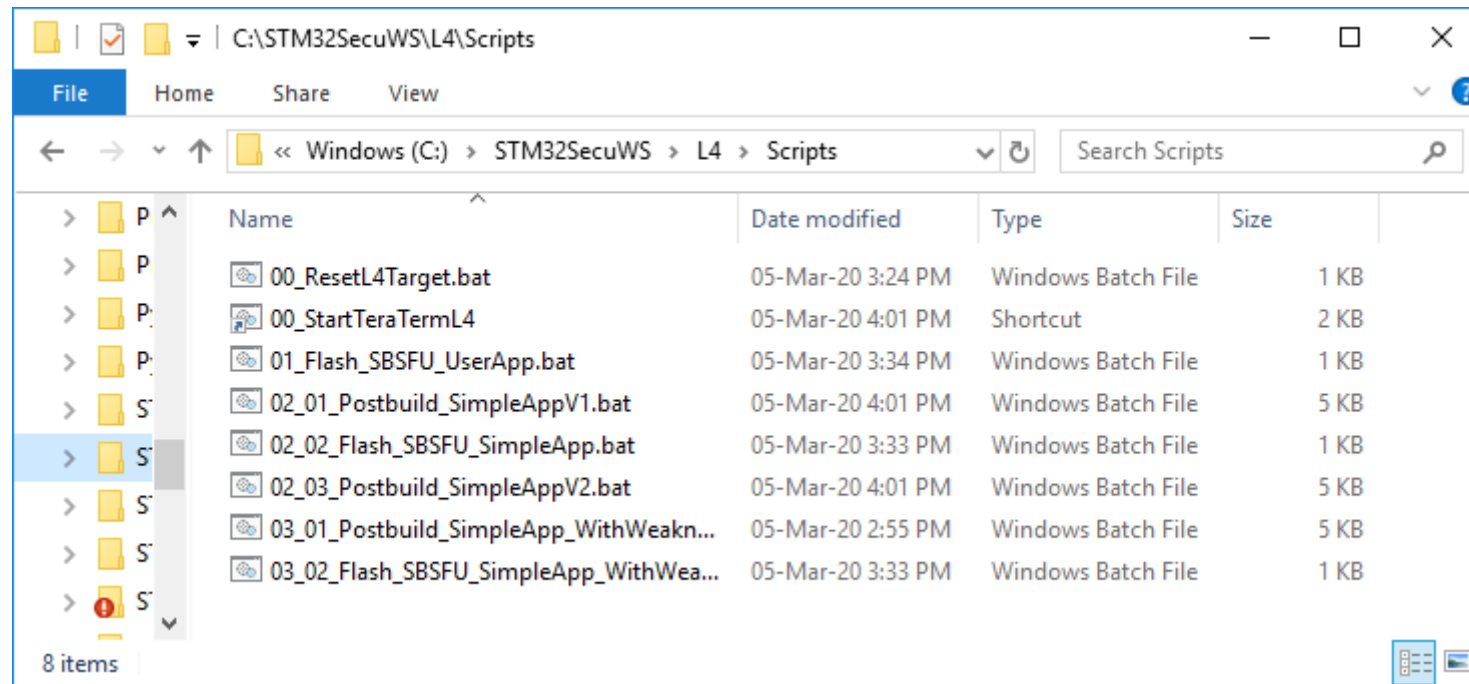
Update the ST-Link firmware

- In CubeIDE select Help/ST-Link Upgrade
- Connect the Nucleo board to the PC
- Click refresh device list
- Click Open in update mode
- Click Upgrade
- Once finished unplug and plug board again



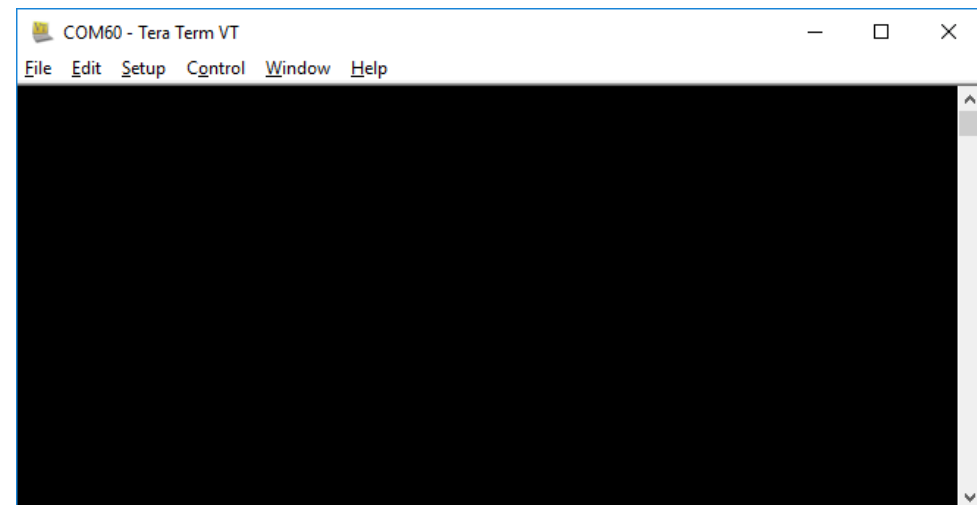
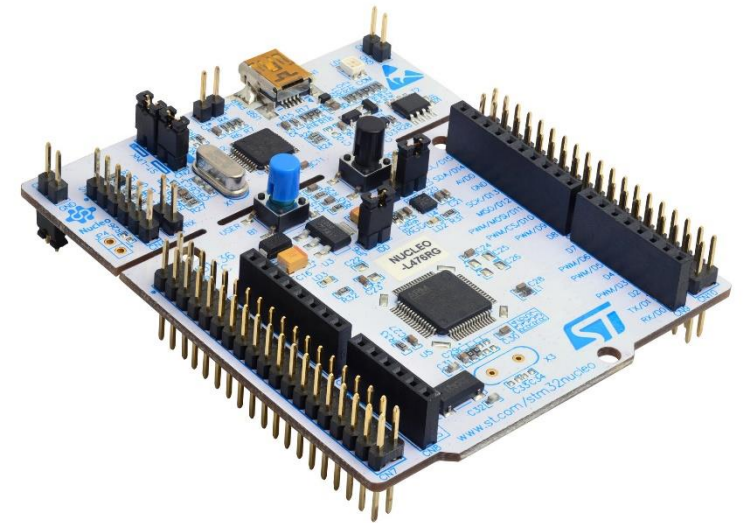
Open an explorer dedicated to scripts

- Please open an explorer window to be able to launch the scripts:



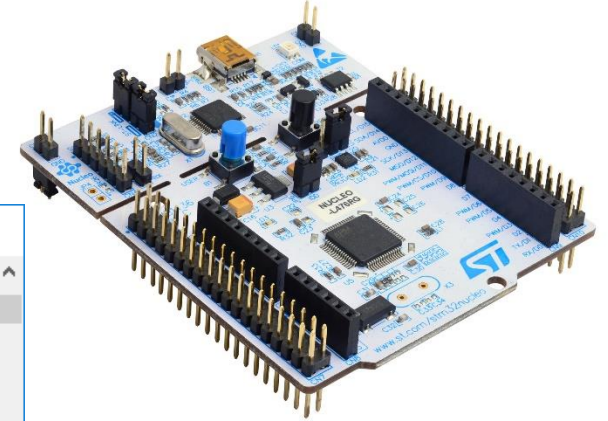
Launch TeraTerm

- Please ensure NucleoL476RG is still connected to your computer with a USB cable
- No other board should be connected
- Launch script **00_StartTeraTermL4.Ink**
 - It should automatically find the good com port.
 - Com port configuration is already done



Prepare Nucleo target

- Launch script **00_ResetL4Target.bat**
 - This will set the board to good initial state



```
C:\windows\system32\cmd.exe

SRAM2_RST      : 0x1 (SRAM2 is not erased when a system reset occurs)

PCROP Protection (Bank 1):

  PCROP1_STRT   : 0xFFFF (0x807FFF8)
  PCROP1_END    : 0x0  (0x8000000)
  PCROP_RDP     : 0x0  (PCROP zone is kept when RDP is decreased)

Write Protection (Bank 1):

  WRP1A_STRT    : 0xFF  (0x807F800)
  WRP1A_END     : 0x0  (0x8000000)
  WRP1B_STRT    : 0xFF  (0x807F800)
  WRP1B_END     : 0x0  (0x8000000)
OPTION BYTES BANK: 1

PCROP Protection (Bank 2):

  PCROP2_STRT   : 0xFFFF (0x80FFF8)
  PCROP2_END    : 0x0  (0x8080000)

Write Protection (Bank 2):

  WRP2A_STRT    : 0xFF  (0x80FF800)
  WRP2A_END     : 0x0  (0x8080000)
  WRP2B_STRT    : 0xFF  (0x80FF800)
  WRP2B_END     : 0x0  (0x8080000)

C:\STM32SecuWS\L4\Scripts>pause
Press any key to continue . . .
```

Stm32cubeprogrammer location

- The script above can fail with following message:

```
*****ERROR*****
```

```
STM32CubeProgrammer not found
```

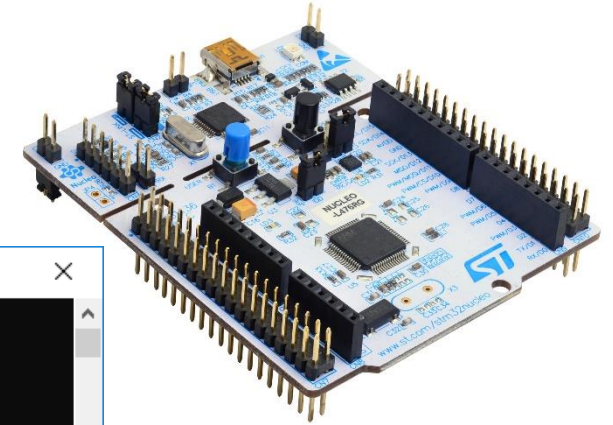
```
Please update STM32CubeProgrammer path in C:\STM32SecuWS\Tools\Other\SetEnv.bat
```

```
*****
```

- In that case, please edit the file and replace the location of STM32CubeProgrammer by your own specific location
- Relaunch the script to check everything is ok

Download SBSFU binary

- Launch script **01_FlashSBSFU_UserApp.bat**
 - This will flash the SBSFU binary: SBSFU_UserApp.bin

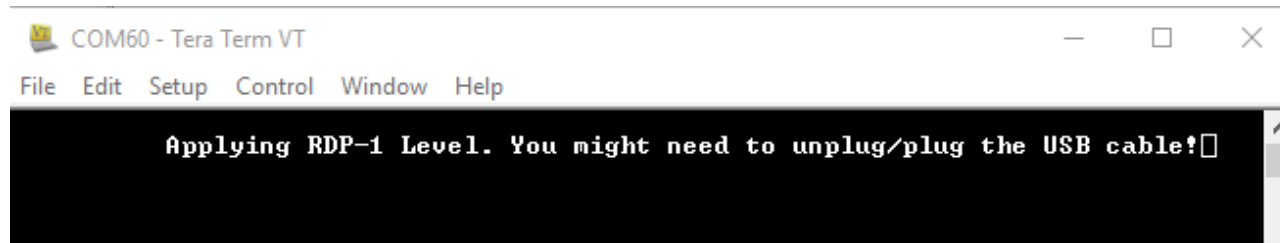


```
C:\windows\system32\cmd.exe
```

```
Connect mode: Under Reset  
Reset mode : Hardware reset  
Device ID   : 0x415  
Revision ID : Rev 4  
Device name : STM32L4x1/STM32L475xx/STM32L476xx/STM32L486xx  
Flash size  : 1 MBytes  
Device type  : MCU  
Device CPU   : Cortex-M4  
  
Mass erase ...  
  
Mass erase successfully achieved  
  
Memory Programming ...  
Opening and parsing file: SBSFU_UserApp.bin  
File      : SBSFU_UserApp.bin  
Size     : 571184 Bytes  
Address  : 0x08000000  
  
Download in Progress:  
██████████ 100%  
  
File download complete  
Time elapsed during download operation: 00:00:10.611  
  
C:\STM32SecuWS\L4\Scripts>pause  
Press any key to continue . . .
```

First start

- Just after flashing is finished you should see in the Tera Term console:



- SBSFU has activated RDP1: This requires a power on reset (POR)
- Unplug and plug the board to perform this POR
- After plugging again, you may miss some messages, the time the terminal reconnects. You can press RESET BUTTON on the board to see the full log
- You also may have no message. In that case close and relaunch TeraTerm
- You may also see some strange characters. In that case click on Control/Reset Terminal to get back normal ASCII characters

Quick view on traces after reset

```
COM60 - Tera Term VT
File Edit Setup Control Window Help

= [ISBOOT] System Security Check successfully passed. Starting...

=====
=                <C> COPYRIGHT 2017 STMicroelectronics                =
=                Secure Boot and Secure Firmware Update                =
=====

= [ISBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [ISBOOT] STATE: CHECK STATUS ON RESET
=                INFO: A Reboot has been triggered by a Hardware reset!
=                INFO: Last execution detected error was: No error. Success.
= [ISBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [ISBOOT] STATE: CHECK USER FW STATUS
=                A FW is detected in the slot SLOT_ACTIVE_1
= [ISBOOT] STATE: VERIFY USER FW SIGNATURE
= [ISBOOT] STATE: EXECUTE USER FIRMWARE
=====
=                <C> COPYRIGHT 2017 STMicroelectronics                =
=                User App #A                =
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Multiple download ----- 4
Validate a FW Image----- 5
Selection :
```

Conclusion

- If you could obtain the same traces as in the previous screen, you are ready for the SBSFU hands-on of the workshop!
- You have already a secure boot running on your target.
- **Please keep this board in this configuration for the workshop**
- If you face any issue during the setup, check following link: <https://community.st.com/stm32-security-workshop>
- If you don't find the solution in previous posts, please describe your issue

Thank you

© STMicroelectronics - All rights reserved.

The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.



life.augmented