life.augmented

STM32 security workshop

02 Building the SBSFU

Purpose

- Starting from the SBSFU build and execution on target
- We'll exercise the secure boot which will authenticate and launch an application
- Then we will generate a version 2 of the application and use the SBSFU to update it on the target

life.augmented

Restarting from homework configuration

- During homework you have build 3 projects and generated 2 binaries
- You have flashed the binary containing both SBSFU and UserApp to the target
- Then you have been able to see the trace of execution of SBSFU and UserApp on TeraTerm
- Let’s restart from this point
  - Please plug your Nucleo L476 containing the SBSFU and UserApp to your PC
  - Open an explorer window and go to C:\STM32SecuWS\L4\Scripts
  - Launch 00_StartTeraTermL4
  - Press reset button

life.augmented

Quick view on traces after reset

COM60 - Tera Term VT

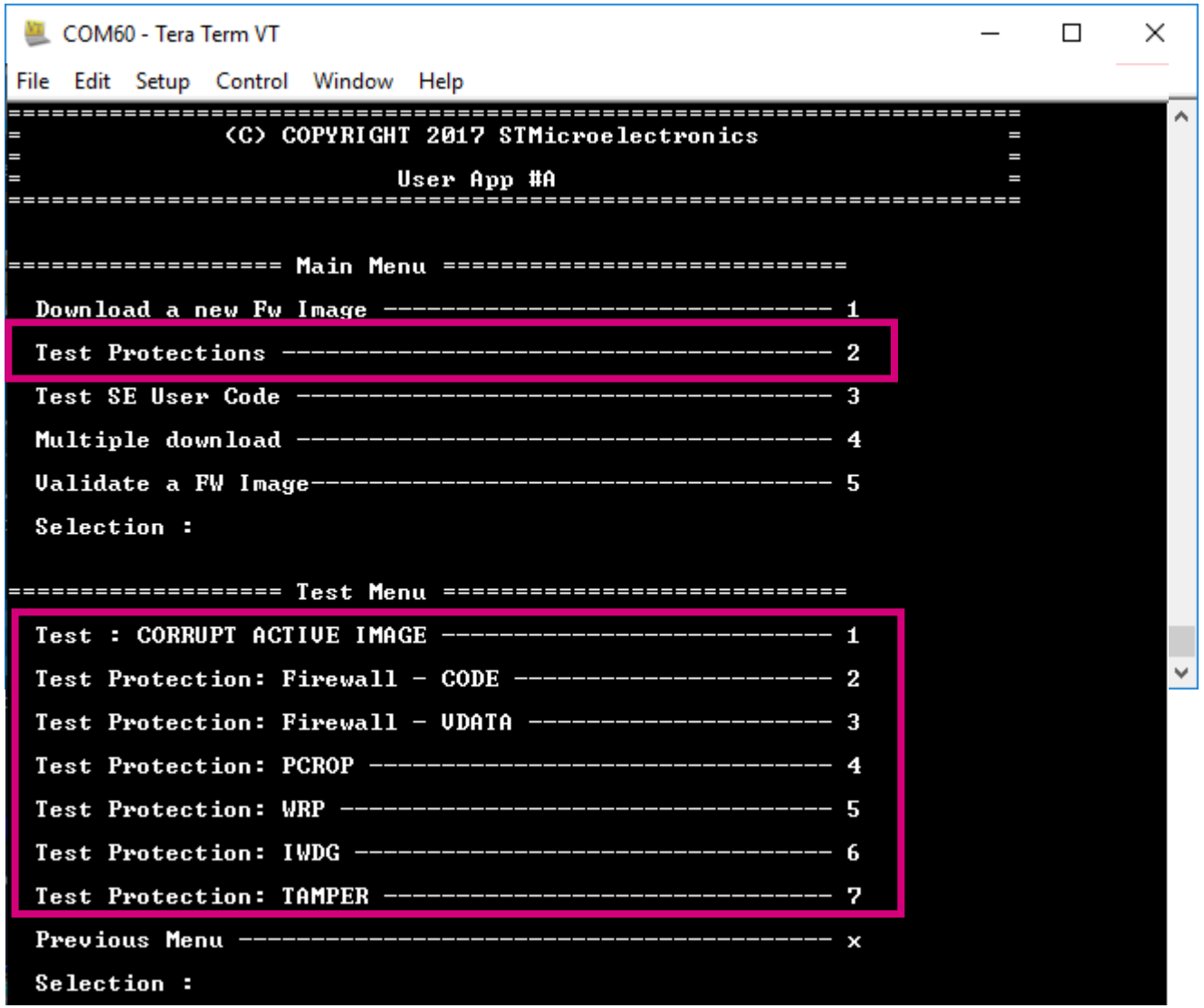
File Edit Setup Control Window Help

```
= [SBOOT] System Security Check successfully passed. Starting...


=====================================================================
=              (C) COPYRIGHT 2017 STMicroelectronics                =
=                                                                   =
=              Secure Boot and Secure Firmware Update               =
=====================================================================


= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
          INFO: A Reboot has been triggered by a Hardware reset!
          INFO: Last execution detected error was: No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: CHECK USER FW STATUS
          A FW is detected in the slot SLOT_ACTIVE_1
= [SBOOT] STATE: VERIFY USER FW SIGNATURE
= [SBOOT] 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 :
```

- Check security protections and setup consistency
- Initialise the secure engine
- Boot status check
- Check local update request
- Check fw status: Download slot to install, interrupted installation, Active firmware presence…
- Verify Active fw signature
- Verify active fw signature (second time) and launch application

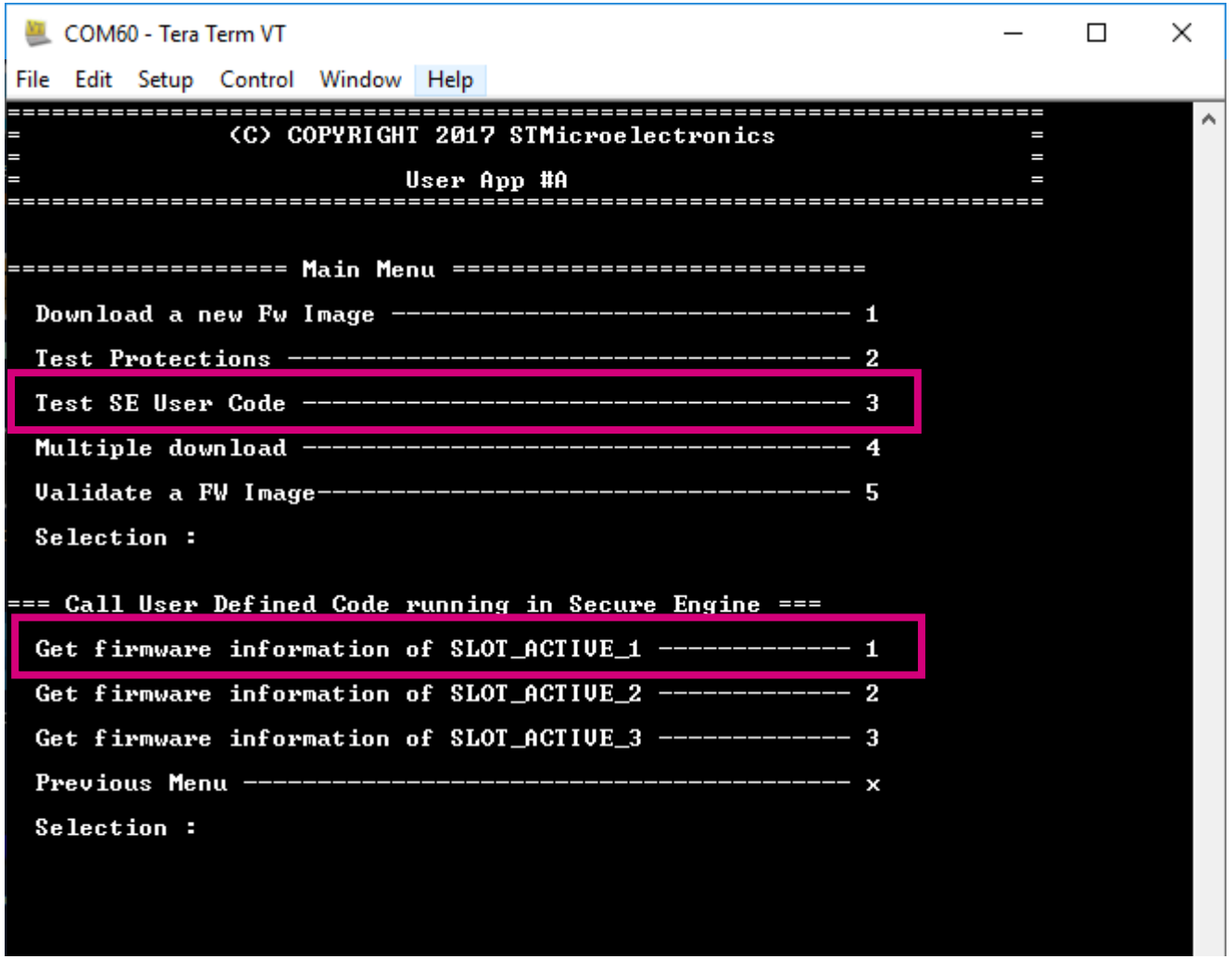
life.augmented

Test protection menu



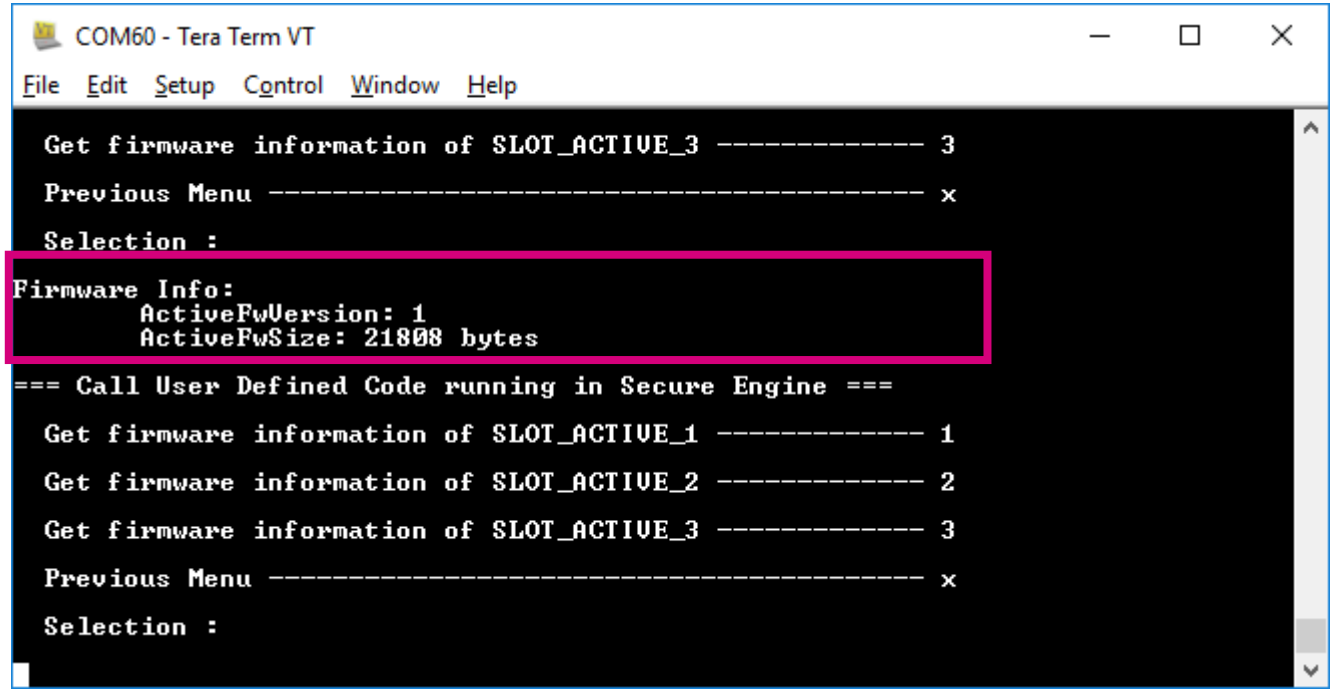
- Press 2
- Then you can play with these options to see what happens
- If you corrupt the image in SLOT_ACTIVE_1 you will have to launch the scripts **00_ResetL4Target** and **01_Flash_SBSFU_UserApp**

Test SE User Code menu



- Press 3 and then 1

Test SE User Code menu



- It shows information available from application side

Note about active slots

- Active slot is where active user firmware is located
- By opposition with download slot where new version of the firmware is downloaded
- There are 3 possible active and download slots managed by SBSFU
- The main purpose of having more than one active slot is the support of multiple cores chips with independent firmware.

life.augmented

SBSFU in a nutshell

- You should now have a first view on:
  - SBSFU directory structure
  - How to build the SBSFU : Need to be done in order
  - SBSFU generates useful files for download in UserApp/binary directory
  - SBSFU + User application are loaded at the same time on the target
  - SBSFU is activating secure protections
  - SBSFU checks the user application authenticity and launches it
  - Default User application provides some basic menu allowing
    - To check some protections
    - To call a SBSFU API
    - To perform an update
- Let’s see how update is working

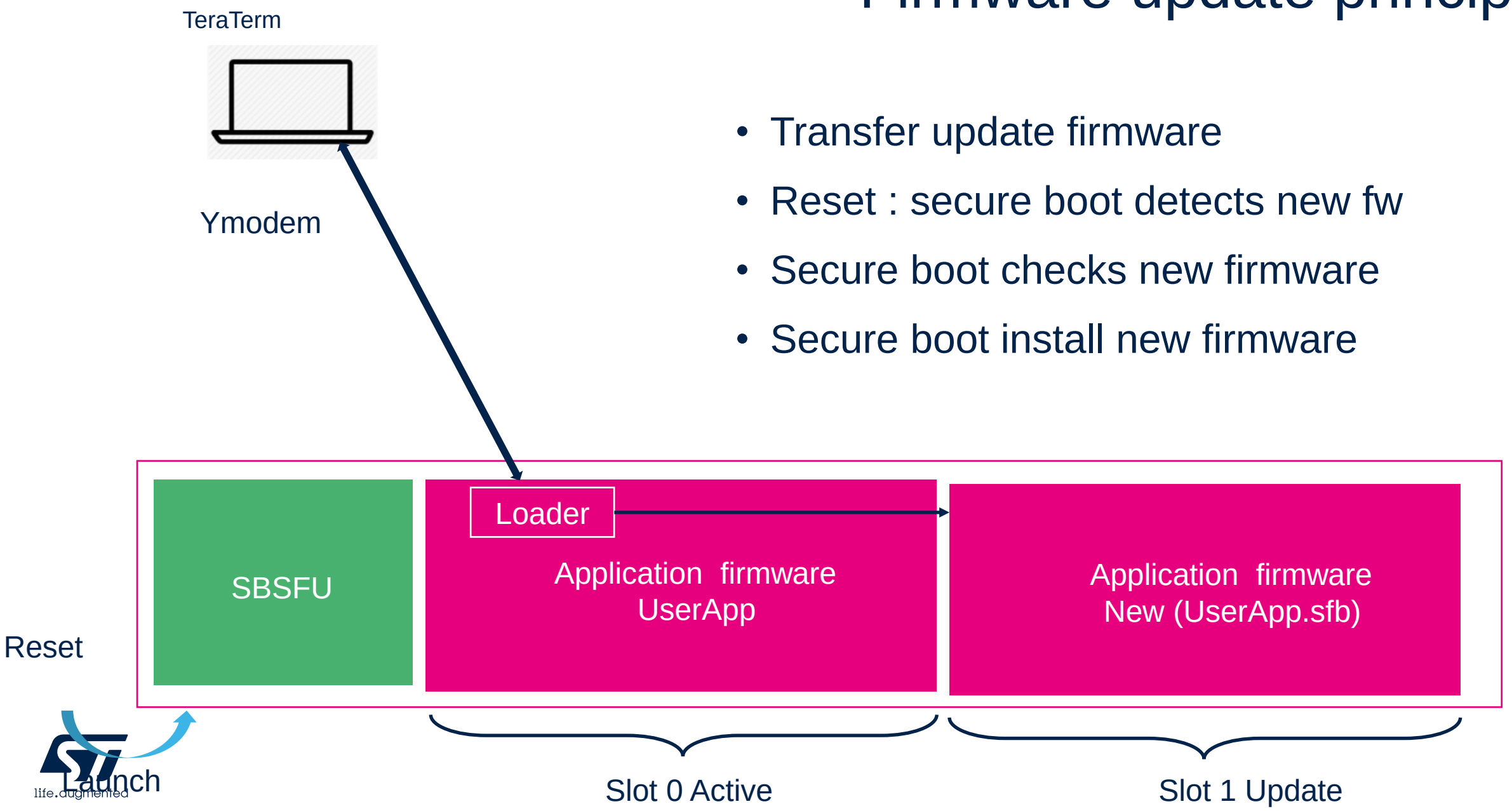
life.augmented

Firmware update

- First menu launches a firmware update
- This update is managed inside the application
- Application will receive the firmware through Ymodem protocol
- Then it will write each chunk in a spare part of the flash.
- At the end, the application should reset the chip to launch the secure boot
- Secure boot will detect this new firmware an install it

life.augmented

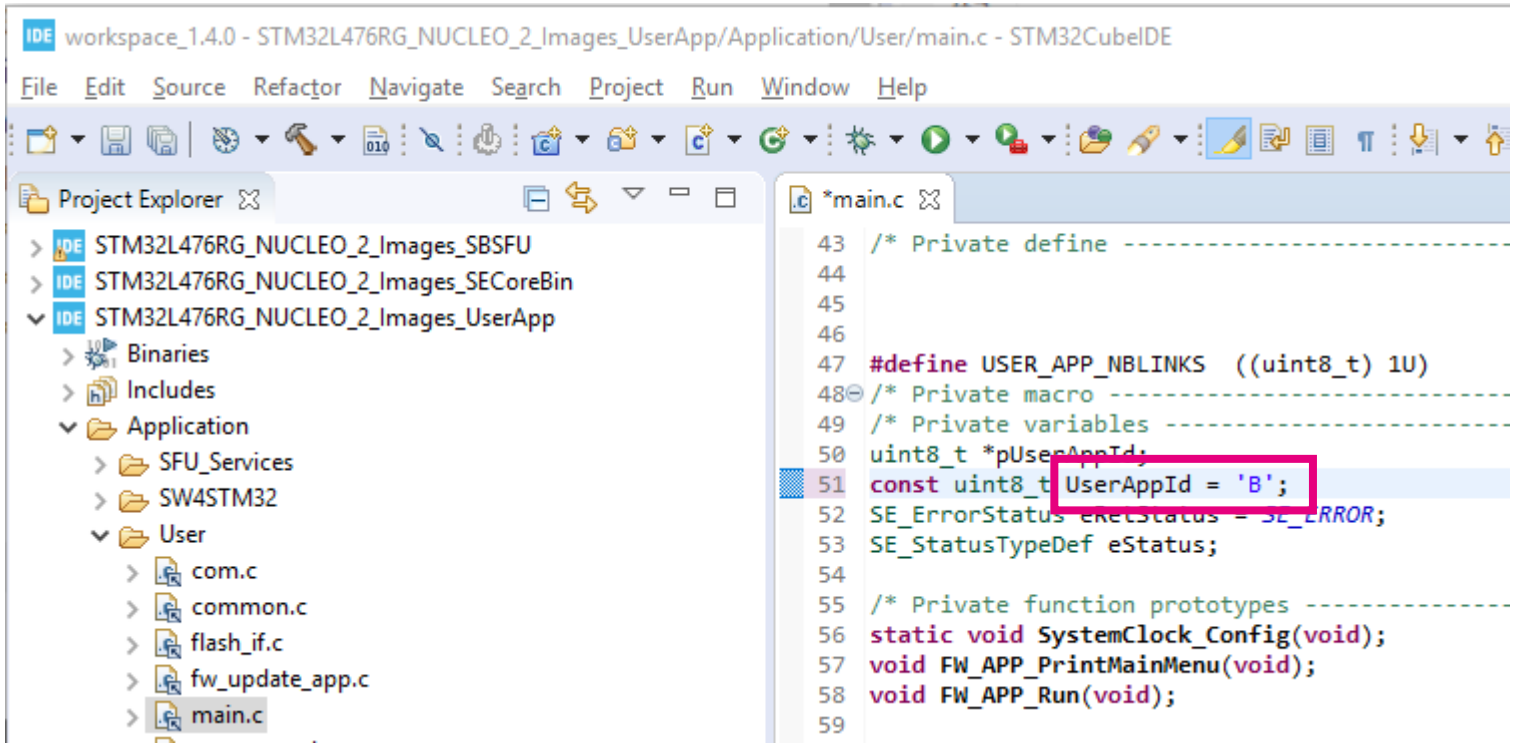
Firmware update principle



- Transfer update firmware
- Reset : secure boot detects new fw
- Secure boot checks new firmware
- Secure boot install new firmware

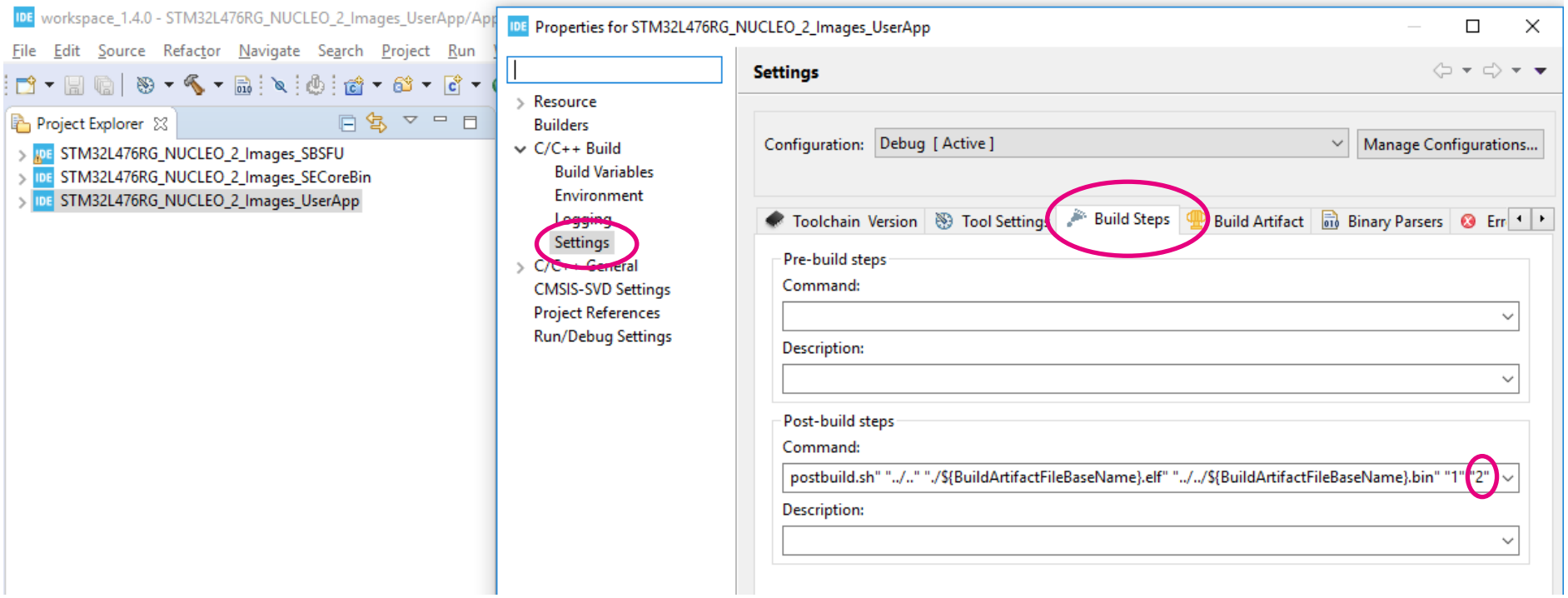
Prepare an update image

- Open same workspace in STM32CubeIDE you've used for the homework
- Change the application identifier in the code :



Update: prepare image

- Change the version of the UserApp
  - Click on STM32L476RG_NUCLEO_2_Images_UserApp, click on menu Project/Properties
  - Goto C++Build/Settings/BuildSteps
  - Edit post build steps replace the last “1” by “2”, apply and close



Update: compile new version

- Launch build on UserApp project to generate version 2

```
CDT Build Console [STM32L476RG_NUCLEO_2_Images_UserApp]
arm-none-eabi-gcc -z max-page-size=1 -o "UserApp.elf" @"objects.list"  -l:se_interface_app.o -mcpu=cortex-m4 -T"../STM3
Finished building target: UserApp.elf

arm-none-eabi-size   UserApp.elf
   text    data     bss     dec     hex filename
  21632     176    6000   27808    6ca0 UserApp.elf
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" "2"
prepareimage with windows executable


17:39:10 Build Finished. 0 errors, 0 warnings. (took 15s.896ms)
```

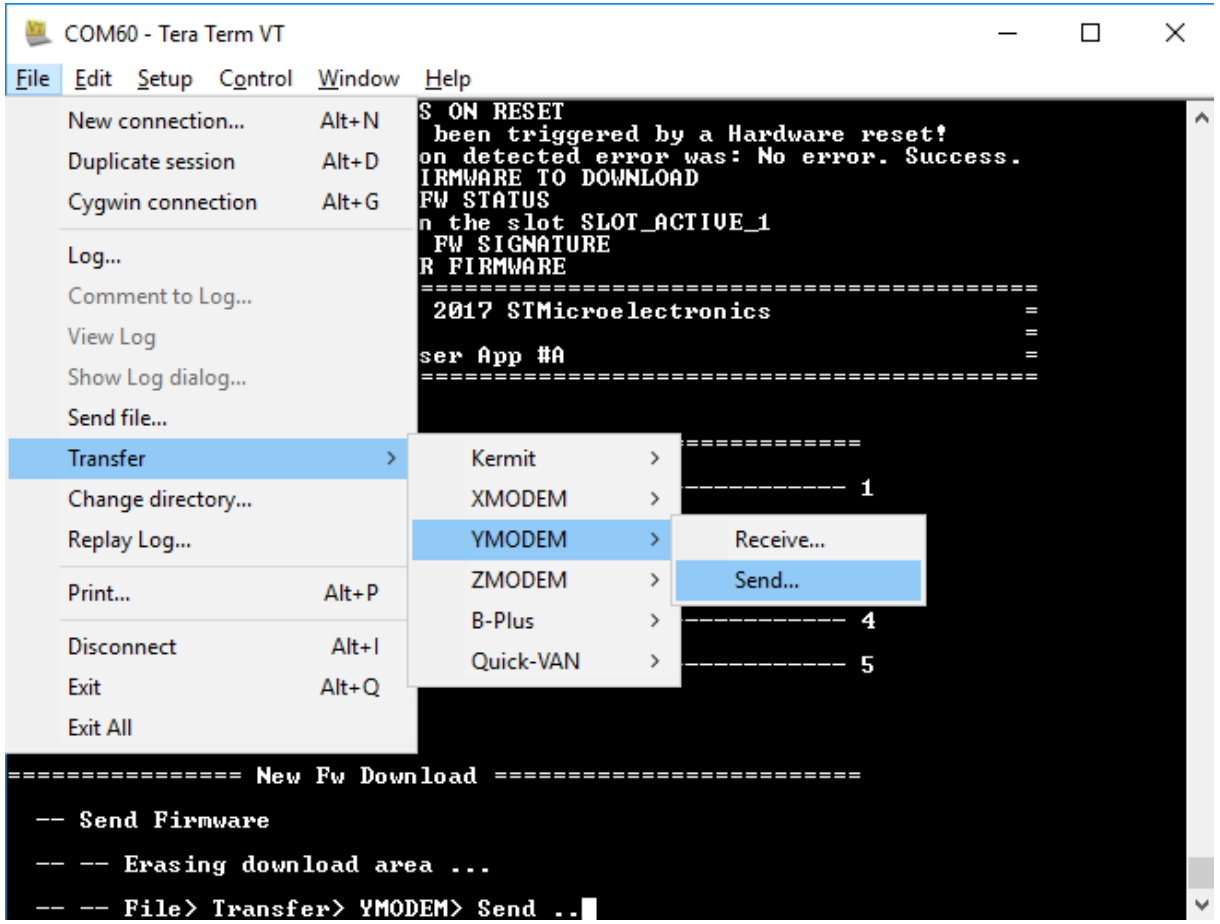
life.augmented

Update: trigger update on target

In TeraTerm Press 1 to select the Download of a new Fw Image

```
================== Main Menu ============================
 Download a new Fw Image ------------------------------- 1
 Test Protections ------------------------------------- 2
 Test SE User Code ------------------------------------- 3
 Selection :

=============== New Fw Download ========================
 -- Send Firmware
 -- -- Erasing download area ...
 -- -- File> Transfer> YMODEM> Send .......................
```

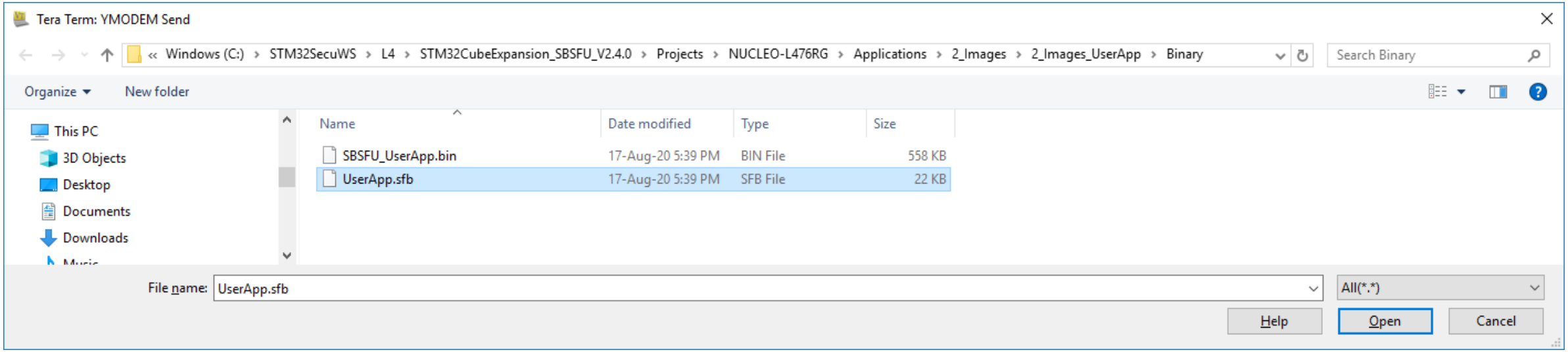
Wait for Ymodem request on the screen, and select File/Transfer/YMODEM/Send



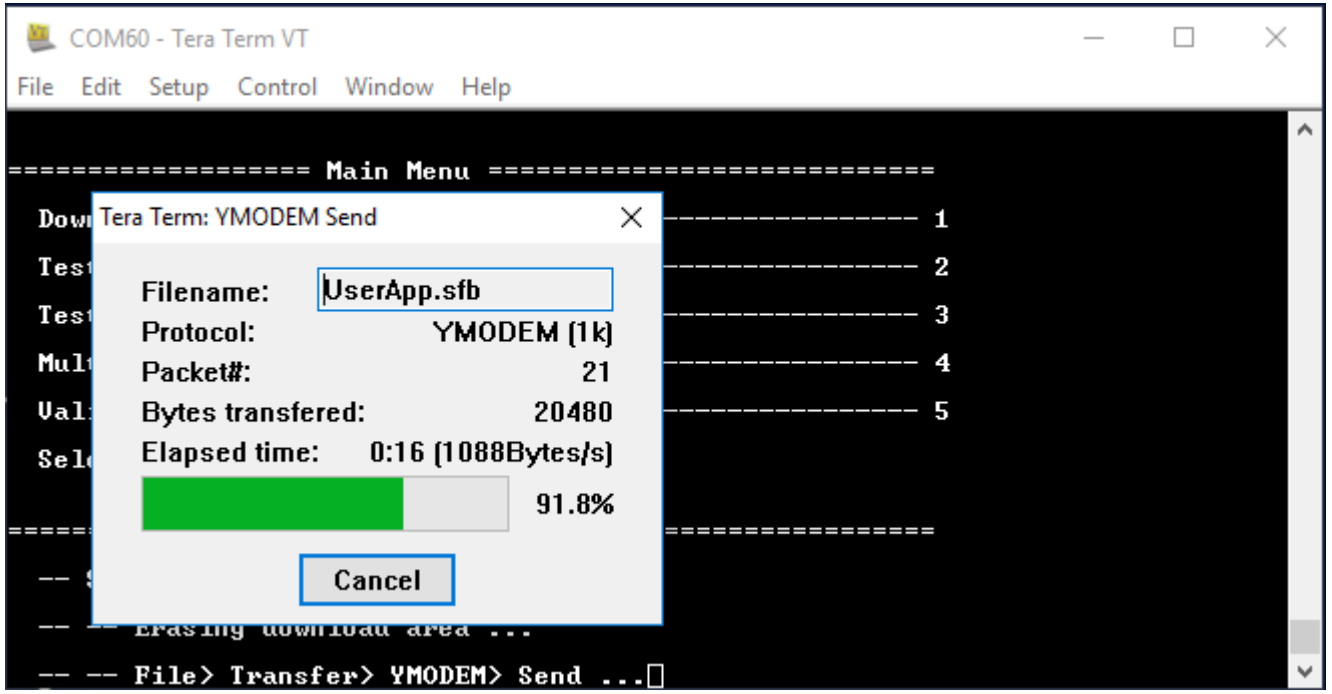
Update: select update file

Popup window should display by default the directory in SBSFU C:\STM32SecuWS\L4\STM32CubeExpansion_SBSFU_V2.4.0\Projects\NUCLEO-L476RG\Applications\2_Images\2_Images_UserApp\Binary

Select UserApp.sfb



Update: download



New firmware transfer

Update process

COM60 - Tera Term VT

File Edit Setup Control Window Help

```
================ New Fw Download ========================

  -- Send Firmware

  -- -- Erasing download area ...

  -- -- File> Transfer> YMODEM> Send ...

  -- -- Programming Completed Successfully!

  -- -- Bytes: 22320

  -- Image correctly downloaded - reboot

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

=====================================================================
=               (C) COPYRIGHT 2017 STMicroelectronics               =
=                                                                   =
=               Secure Boot and Secure Firmware Update              =
=====================================================================

= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
          INFO: A Reboot has been triggered by a Software reset!
          INFO: Last execution detected error was: No error [illegible]ess.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: CHECK USER FW STATUS
          New Fw to be installed from slot SLOT_DWL_1
= [SBOOT] STATE: INSTALL NEW USER FIRMWARE
          Image preparation done.
          Swapping the firmware images.........................................
...........
========= End of Execution ==========


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

=====================================================================
=               (C) COPYRIGHT 2017 STMicroelectronics               =
=                                                                   =
=               Secure Boot and Secure Firmware Update              =
=====================================================================
```

Application manages the full download and then reset to activate the secureboot

New firmware detected in SLOT_DWL_1 to be installed. Verify new header signature

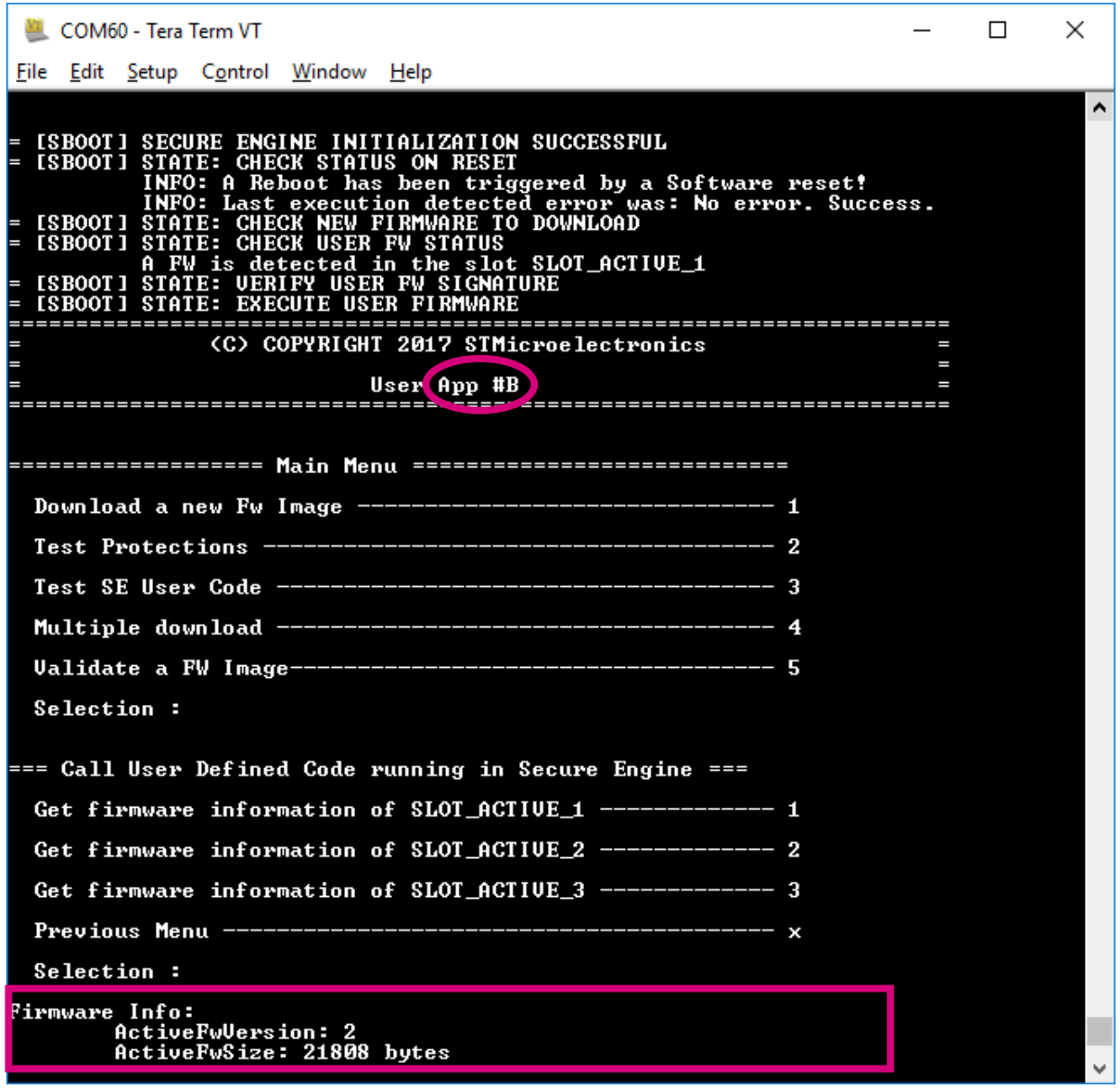
Firmware installation: Check version, Decryption in place, check fw signature, SWAP

Reset.

life.augmented

Update: check version

- Check new version using the Test SE User Code menu



Conclusion

- SBSFU build is simple
- SBSFU is a secure bootloader that checks integrity and authenticity of the application
- SBSFU is able to securely update the application, checking integrity and authenticity at each step
- Update application transfer uses Ymodem protocol

Thank you

life.augmented