life.augmented

STM32 Security Workshop

04 Experience SBSFU benefits

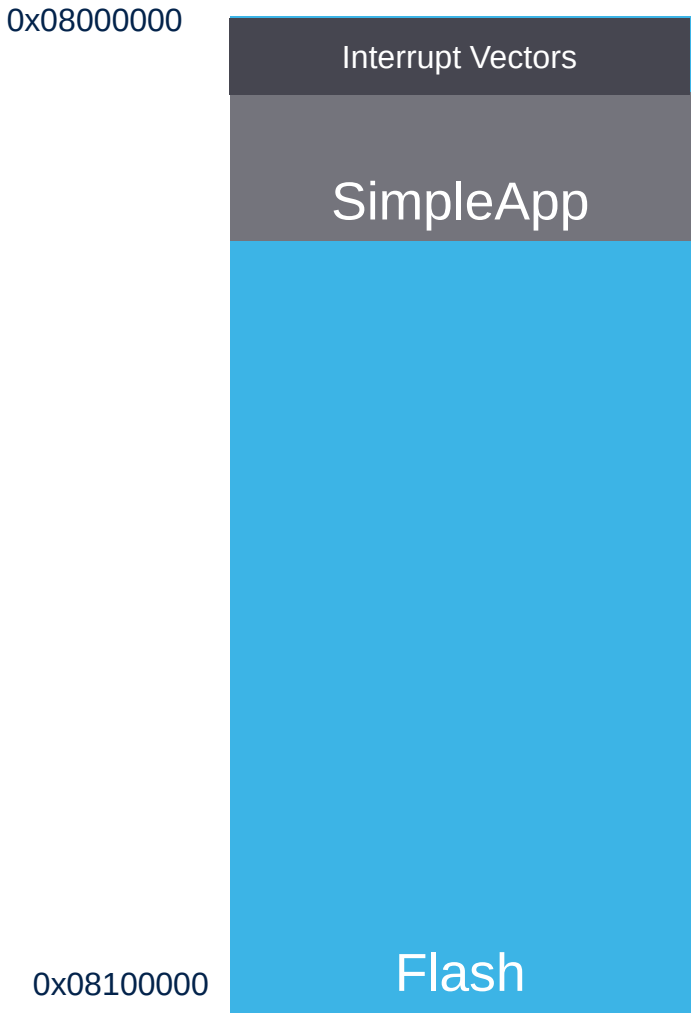
I want to use SBSFU with my application

- Starting from a simple application
- Make sure application is running standalone
- Make modification to integrate it with SBSFU
- Application is now checked and launched by SBSFU

life.augmented

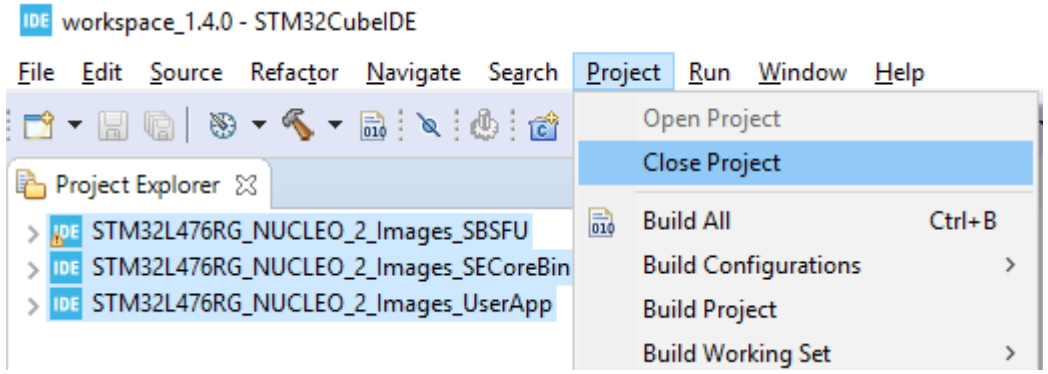
Standalone application

- Application created using CubeIDE/CubeMX
  - Simple heartbeat traces on terminal
  - Led blink
- Application located by default at beginning of FLASH



Let’s clean first our environment

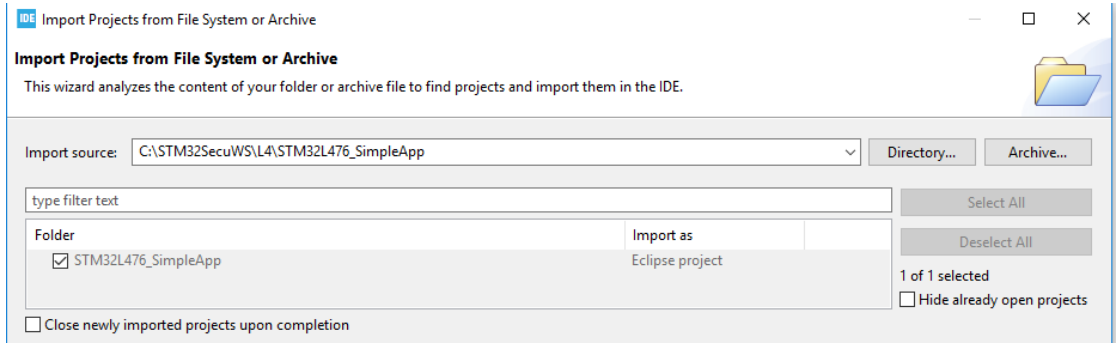
- Come back to CubeIDE environment and close previous projects
  - Don’t delete them !



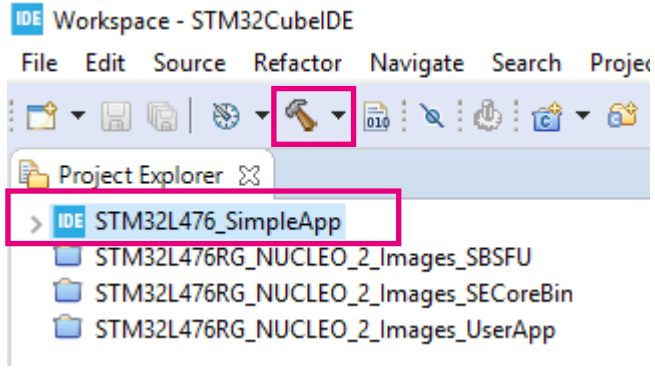
- Reset target configuration using script **00_ResetL4Target.bat**
- Restart TeraTerm (if closed previously) using script **00_StartTeraTermL4**

life.augmented

Build standalone application



- Open in CubeIDE application
  - File/Open Projects from File-System
  - Select C:\STM32SecuWS\L4\STM32L476_SimpleApp



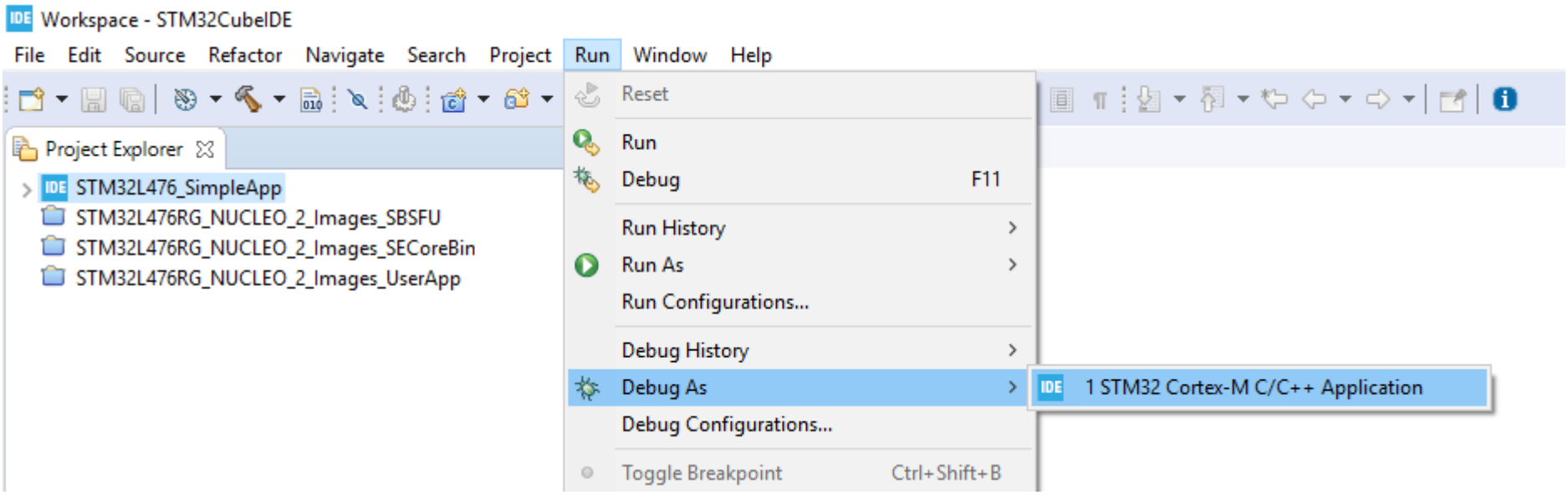
- Click on SimpleApp project and Build Application

```
CDT Build Console [STM32L476_SimpleApp]
Finished building target: STM32L476_SimpleApp.elf

arm-none-eabi-size   STM32L476_SimpleApp.elf
arm-none-eabi-objdump -h -S  STM32L476_SimpleApp.elf  > "STM32L476_SimpleApp.list"
arm-none-eabi-objcopy  -O binary  STM32L476_SimpleApp.elf  "STM32L476_SimpleApp.bin"
   text    data     bss     dec     hex filename
  14944     120    1712   16776    4188 STM32L476_SimpleApp.elf
Finished building: default.size.stdout

Finished building: STM32L476_SimpleApp.bin
Finished building: STM32L476_SimpleApp.list



17:16:56 Build Finished. 0 errors, 0 warnings. (took 6s.507ms)
```

life.augmented

Launch Standalone application

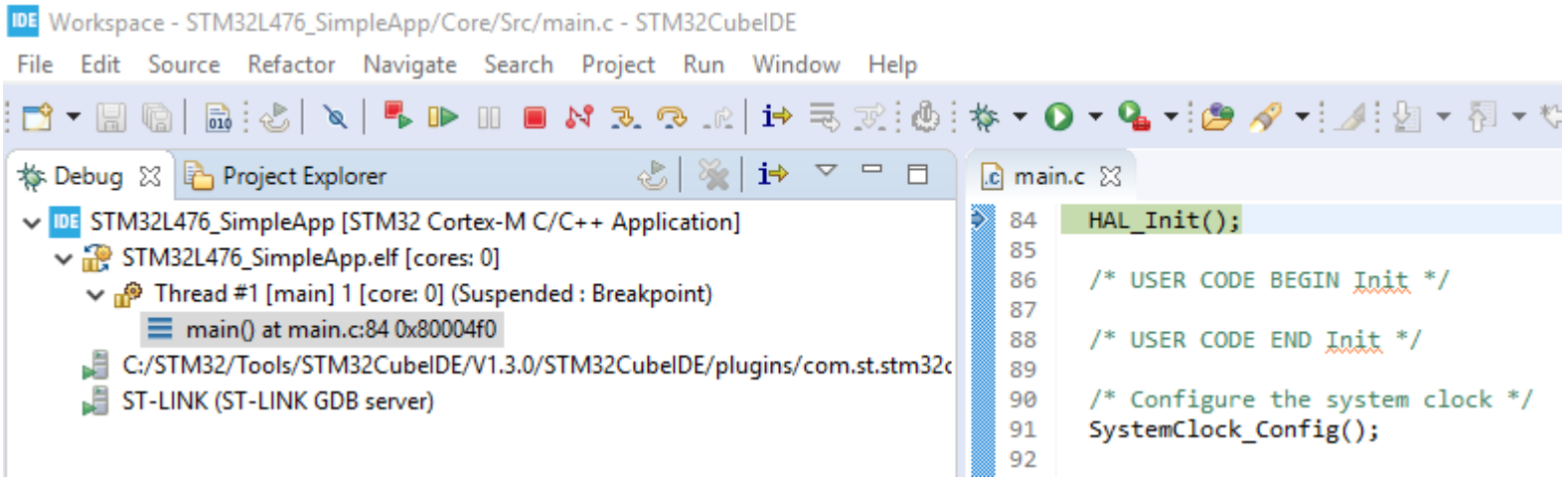
- Run application on target using debugger
  - Debug as / STM32 Cortex-M C/C++ Application



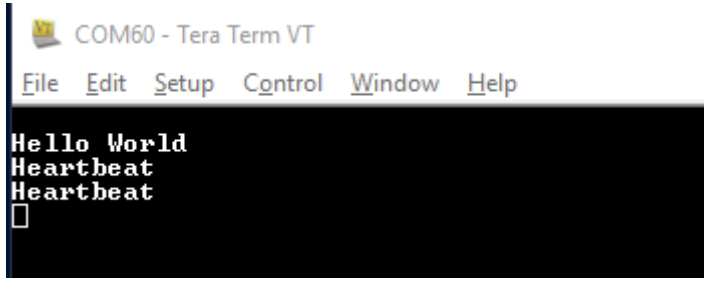
- Click OK in the debug configuration window
- Answer Switch in the pop window asking to switch to debug perspective

Run standalone application

- Run application from debugger



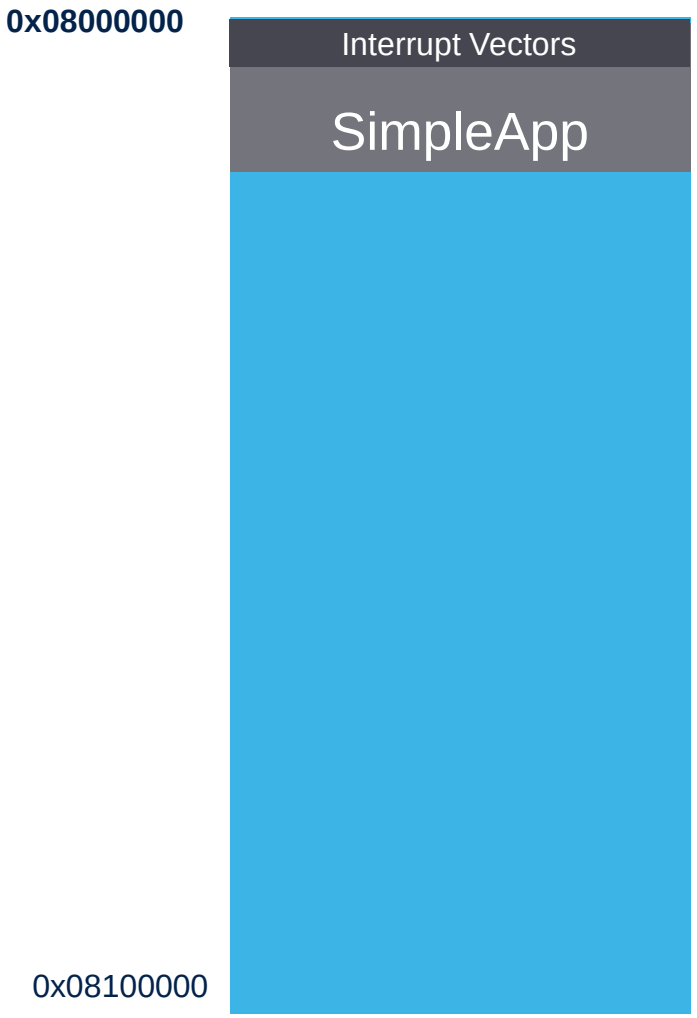
- Tera Term should display the heartbeat



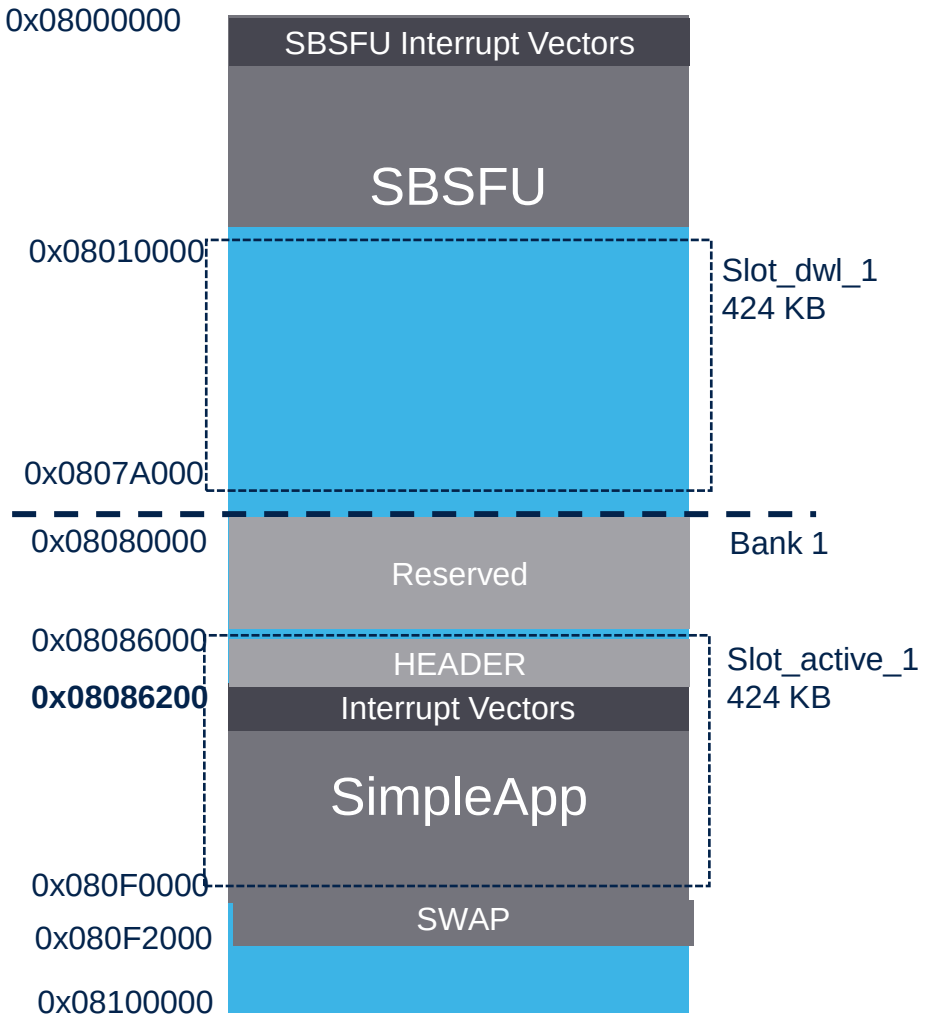
- Stop debugging session

life.augmented

Adapt simple application to SBSFU



FLASH MAPPING for SBSFU on STM32L4



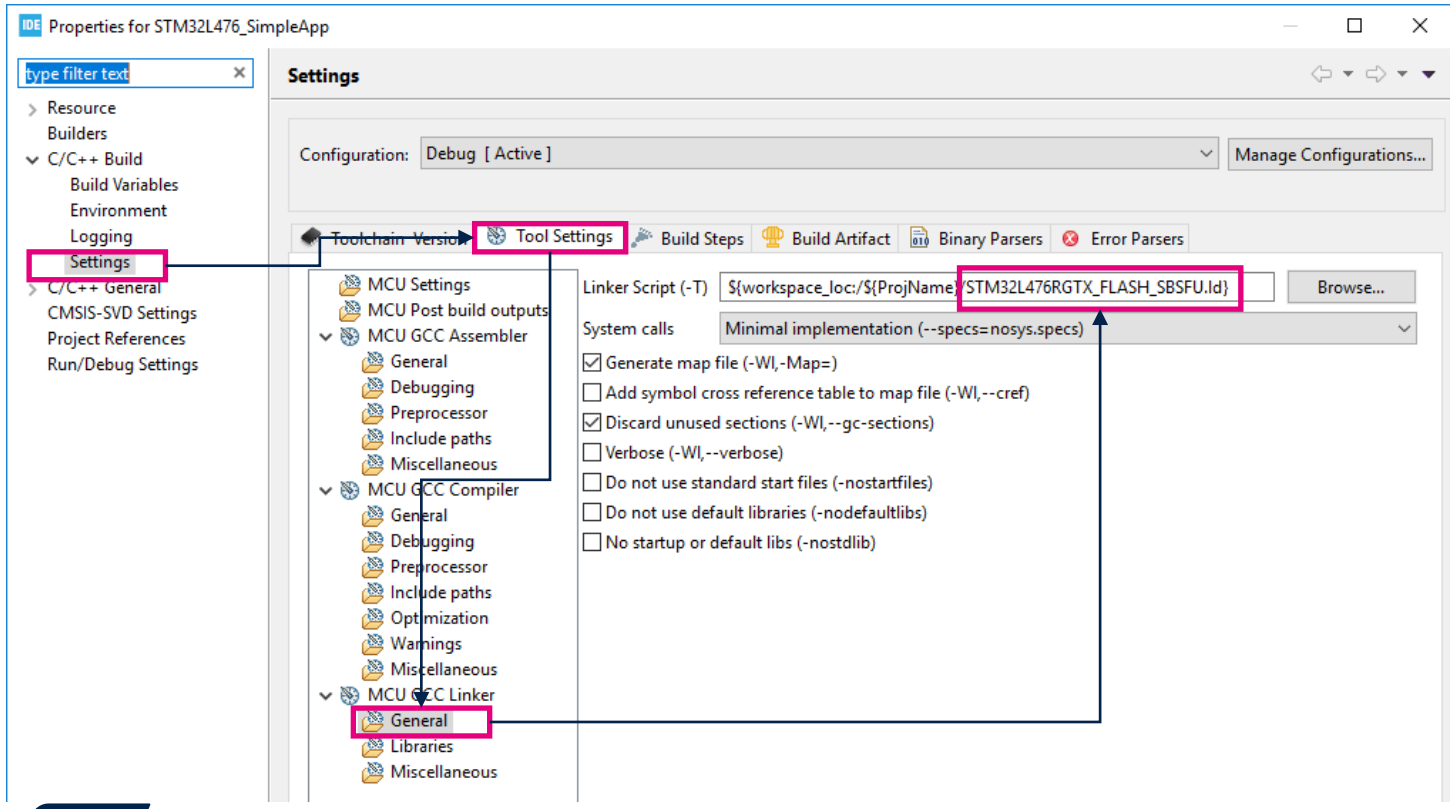
Adapt simple application to SBSFU

- Steps
  - Memory mapping : Impact on **STM32L476RGTX_FLASH.ld** file
    - Application should run from SBSFU SLOT_ACTIVE_1 address : **0x08086200** / Size to **424** KB
    - Secure Engine reserves the first 4KB RAM: Appli starts from **0x20001000** / Reduce size to 92KB
  - Flash alignment: Firmware size should be aligned on 16 bytes: Add specific section in .ld file
  - Firmware is shifted => Reset vector are shifted: Impact in system_stm32l4xx.c
    - #define VECT_TAB_OFFSET **0x08086200**
  - => Check application is still working standalone with debugger with these modifications
  - Use builder script

life.augmented

Change linker script

- Change the linker file to move the application in SLOT_ACTIVE_1
  - Project -> Properties -> C/C++ Build/ Settings/Tool Settings Tab/MCU GCC Linker/General



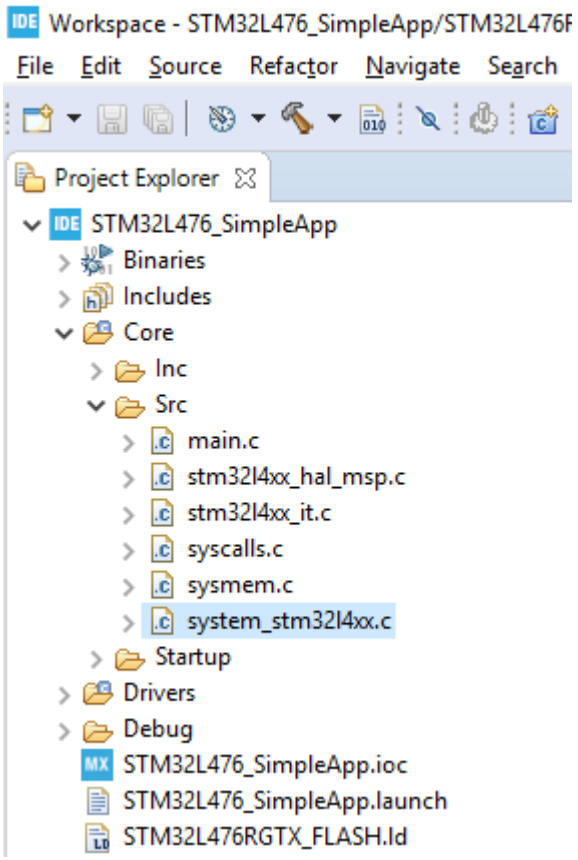
Click on Browse and select:
STM32L476RGTX_FLASH_SBSFU.ld

Apply and Close

Change vector table address

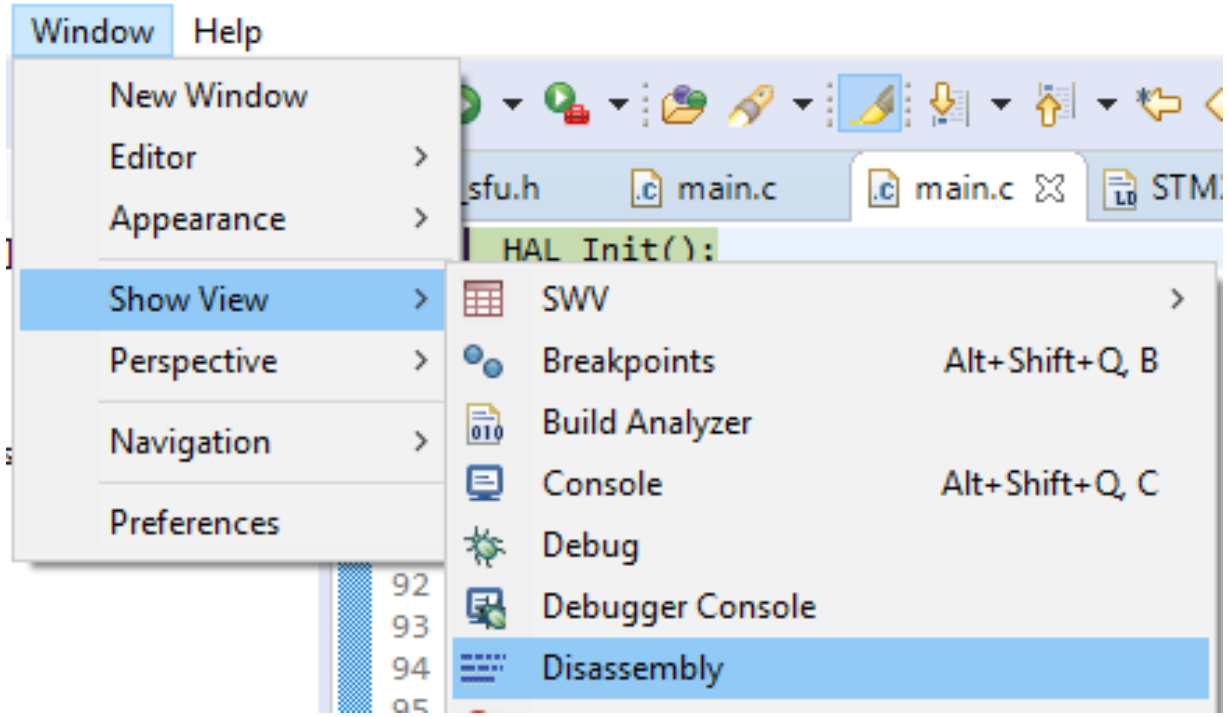
- Code system_stm32l4xx.c line 126

```
/************************* Miscellaneous Configuration ************************/
/*!< Uncomment the following line if you need to relocate your vector Table in
     Internal SRAM. */
/* #define VECT_TAB_SRAM */
#define VECT_TAB_OFFSET  0x08086200 /*!< Vector Table base offset field.
                                         This value must be a multiple of 0x200. */
/******************************************************************************/
```



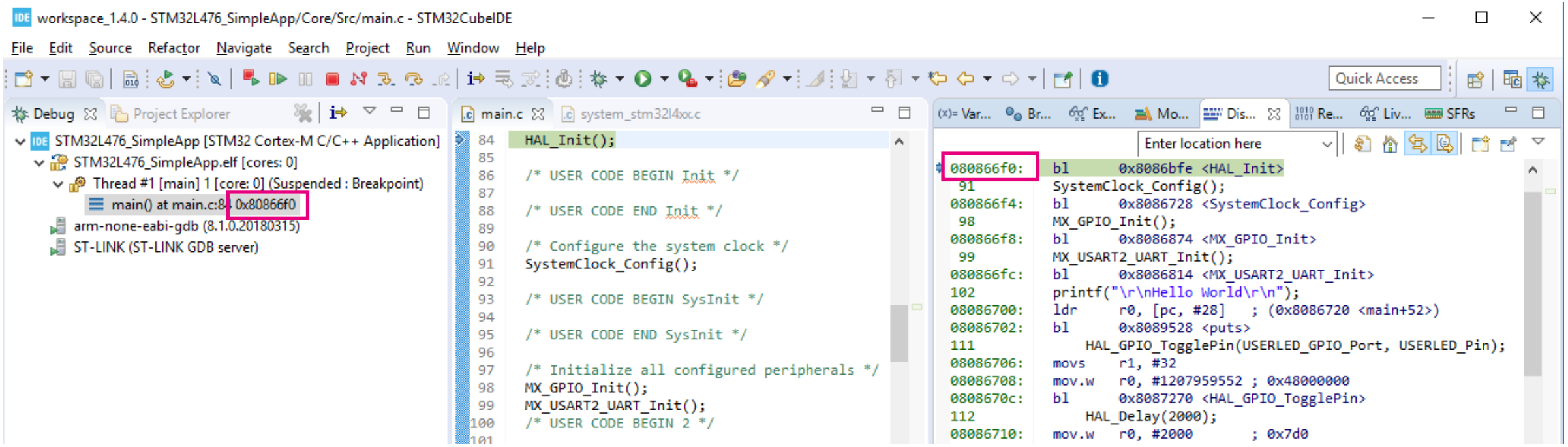
Check application is still working

- Rebuild Application
- Run script **00_ResetL4Target.bat** script
- Run Application on target using debugger and add disassembly view



Check application location

- Check Addresses : In left part main is at 0x080866F0 : in SBSFU slot 0



- Run and check application is still working
- Now, please press RESET button (black button on Nucleo), it stops working. Why?

Explanation

- After a system reset, the ARM Cortex reads reset handler address at flash base address
- When application is linked at flash base address, it works fine
- When application is linked anywhere else, it cannot work any more
- Then why it worked the first time ?
- Reason is because you used the debugger
  - Debugger reads the content of the downloaded image
  - It reads the reset handler address and updates the program counter with this value
  - Then application can start from where it was linked from

Actual integration with SBSFU

- We changed the SimpleApp mapping to adapt to SBSFU mapping
- Now, the SimpleApp should be launched by the SBSFU
- We need to create the SimpleApp meta data, so that SBSFU can check it
- SBSFU provides a “postbuild” script that handles this automatically at the end of the Sample UserApp building

Postbuild script used in SBSFU

- In first hands on, at the end of UserApp compilation, a postbuild was automatically launched:

```
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-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

18:36:47 Build Finished. 0 errors, 0 warnings. (took 14s.937ms)
```

life.augmented

Building the metadata for SimpleApp

- SBSFU postbuild script generates 2 main files
  - A firmware update binary composed of the header and the encrypted firmware (.sfb)
  - A full binary containing SBSFU + header validated + firmware in clear : Ready to be flashed
- For this workshop we reused same script and made few changes
  - Hardcode the parameters
  - Change the directory relation between SBSFU and UserApp
  - Add traces for each step
  - Produce file name with version
- Such script is called *Postbuild* in the scripts directory

Build the update file

- Launch script **02_01_Postbuild_SimpleAppV1.bat**
  - V1 is for version = 1
- Output should look like:

C:\windows\system32\cmd.exe

```
Generating secure binaries executing in c:\STM32SecuWS\L4\STM32L476_SimpleApp
Postbuild with windows executable
Encrypt debug\STM32L476_SimpleApp.bin into .\\Binary\\\STM32L476_SimpleApp.sfu using AES key from SecureEngine binary
Compute signature (sha256) of debug\STM32L476_SimpleApp.bin in .\\Binary\\\STM32L476_SimpleApp.sign
Generate update firmware : Header (version, iv, sha256 and own signature) + encrypted firmware in .\\Binary\\\STM32L476_
SimpleAppV1.sfb
Generate header to be included in big image in .\\Binary\\\STM32L476_SimpleAppsfuh.bin
Generate big image composed of SBSFU + Header + appp firmware in clear in .\\Binary\\\SBSFU_STM32L476_SimpleAppV1.bin
Press any key to continue . . .
```

- You can see it generates the Full image to be flashed (.bin) and the update file (.sfb)

life.augmented

Checking script output

- Please check content of C:\STM32SecuWS\L4\STM32L476_SimpleApp\Binary
  - STM32L476_SimpleAppV1.sfb
    - Secure Firmware Binary that is the update file containing header and encrypted firmware encrypted
  - SBSFU_STM32L476_SimpleAppV1.bin
    - Full binary (SBSFU + header validated + firmware in clear)
    - This is the file we are going to flash

life.augmented

Check SimpleApp on target

- Launch scripts
  - **00_ResetL4Target.bat**
  - **02_02_Flash_SBSFU_SimpleApp.bat**
- Do a power on reset of the board
- Press reset button
- Check traces
  - Why is it resetting ?
  - Look at SBSFU status on 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
          WARNING: A Reboot has been triggered by a Watchdog reset!
          INFO: Last execution detected error was: Watchdog error.
= [EXCPT] WATCHDOG RESET FAULT!
= [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
Hello World
Heartbeat
Heartbeat

= [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
          WARNING: A Reboot has been triggered by a Watchdog reset!
          INFO: Last execution detected error was: Watchdog error.
= [EXCPT] WATCHDOG RESET FAULT!
= [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
Hello World
Heartbeat
Heartbeat
```

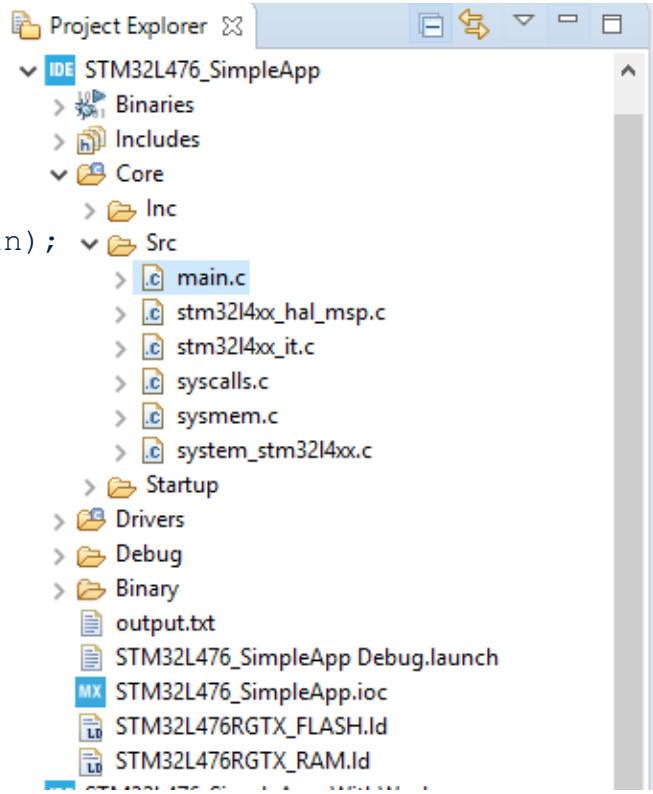
life.augmented

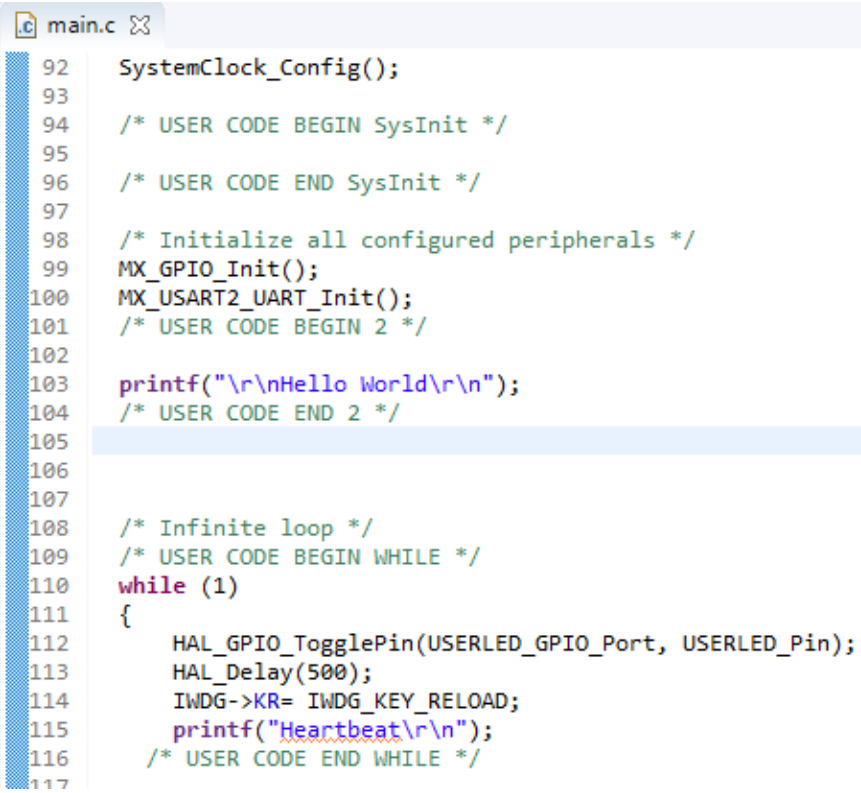
Update SimpleApp on target

- Make a change in the application
  - change frequency of blinking from 2s to 0,5 second and add watchdog refresh:

```
/* USER CODE BEGIN PD */
#define IWDG_KEY_RELOAD  0x0000AAAAu
/* USER CODE END PD */
…
while (1)
  {
  HAL_GPIO_TogglePin(USERLED_GPIO_Port, USERLED_Pin);
  HAL_Delay(500);
  IWDG->KR= IWDG_KEY_RELOAD;
  printf("Heartbeat\r\n");
```

Code snippet





Generate the new update file

- Rebuild application 
- Launch script : **02_03_Postbuild_SimpleAppV2.bat**
- It will set version 2 in the update image

life.augmented

Update SimpleApp V2 on target

- SimpleApp does not contain code to manage update (as provided in UserApp) but SBSFU has a local loader via YMODEM . To activate it :
- Press blue button and then RESET button. Release RESET button first

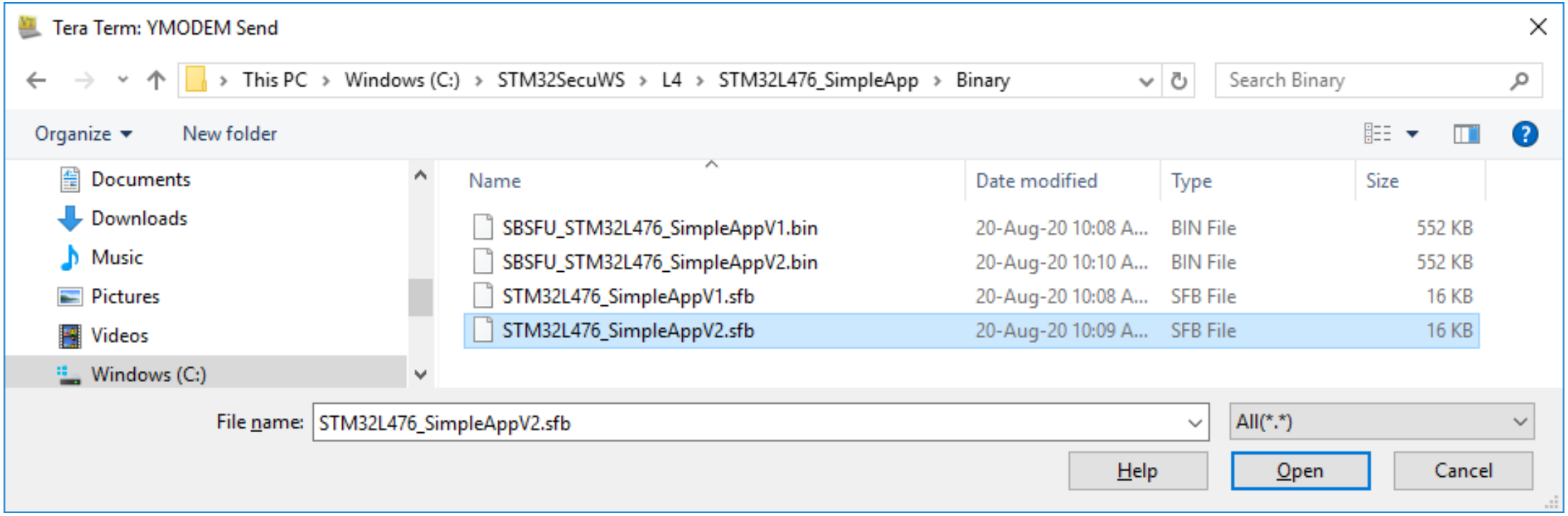
```
=====================================================================
=              (C) COPYRIGHT 2017 STMicroelectronics                =
=                                                                   =
=              Secure Boot and Secure Firmware Update               =
=====================================================================


= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
          WARNING: A Reboot has been triggered by a Watchdog reset!
          INFO: Last execution detected error was: Watchdog error.
= [EXCPT] WATCHDOG RESET FAULT!
= [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
Hello World
Heartbeat
Heartbeat

= [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: DOWNLOAD NEW USER FIRMWARE
          File> Transfer> YMODEM> Send .
```

Press reset button (black) while user button already pressed

Detect the user button pressed and launch the loader

Update SimpleApp V2 on target

- Open File/Transfer/Ymodem/Send and select
  - C:\STM32SecuWS\L4\STM32L476_SimpleApp\Binary\STM32L476_SimpleAppV2.sfb



Update SimpleApp V2 on target

- Traces on terminal

```
          INFO: Last execution detected error was: No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: DOWNLOAD NEW USER FIRMWARE
          File> Transfer> YMODEM> Send .
= [SBOOT] STATE: REBOOT STATE MACHINE
========= End of Execution ==========


= [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. Success.
= [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
```

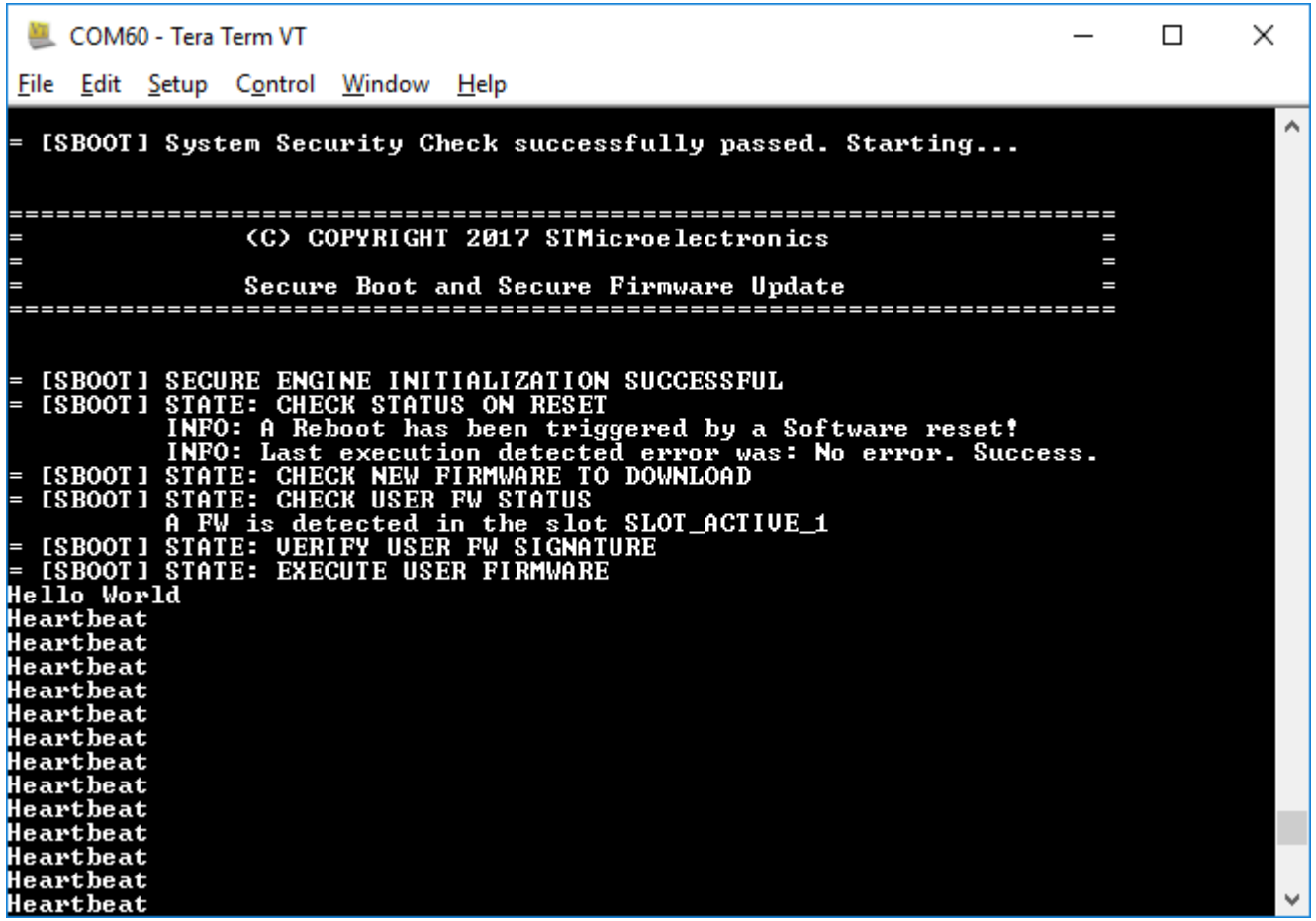
New firmware is downloaded using SBSFU embedded loader in SLOT_DWL_1 Then Reset is performed to trigger installation

New firmware detected in SLOT1 to be installed. Verify new header signature

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

Reset

SimpleAppV2 now working fine



- HeartBeat is faster
- No more watchdog reset

life.augmented

Antirollback

- Antirollback prevents updating application with old version
- Try update with SimpleAppV1
  - Press Blue button + Reset to enter in update mode
  - Select Ymodem Send menu
  - Select SimpleAppV1
  - SBSFU will reject the update

COM60 - Tera Term VT

File Edit Setup Control Window Help

```
          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: DOWNLOAD NEW USER FIRMWARE
          File> Transfer> YMODEM> Send
= [SBOOT] STATE: HANDLE CRITICAL FAILURE
= [EXCPT] INSTALLATION CANCELLED: FORBIDDEN VERSION!
= [SBOOT] STATE: REBOOT STATE MACHINE
========= End of Execution ==========



= [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: Firmware version rejected by
anti-rollback.
= [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
Hello World
Heartbeat
```

life.augmented

Conclusion

- The integration of the application in SBSFU is very simple:
  - Few changes in code and mapping file
  - One script required to generate the needed files for update (Can be adapted from original script to fit your directory structure)
- Not addressed in this hands-on
  - Firmware loader in the application: this needs the integration of the code to manage the update file download. This is just reuse of few functions provided in SBSFU example

life.augmented

Optional 2nd hands-on

- Starting from previous STM32L476_SimpleApp
- Check what happens when trying to corrupt the update image

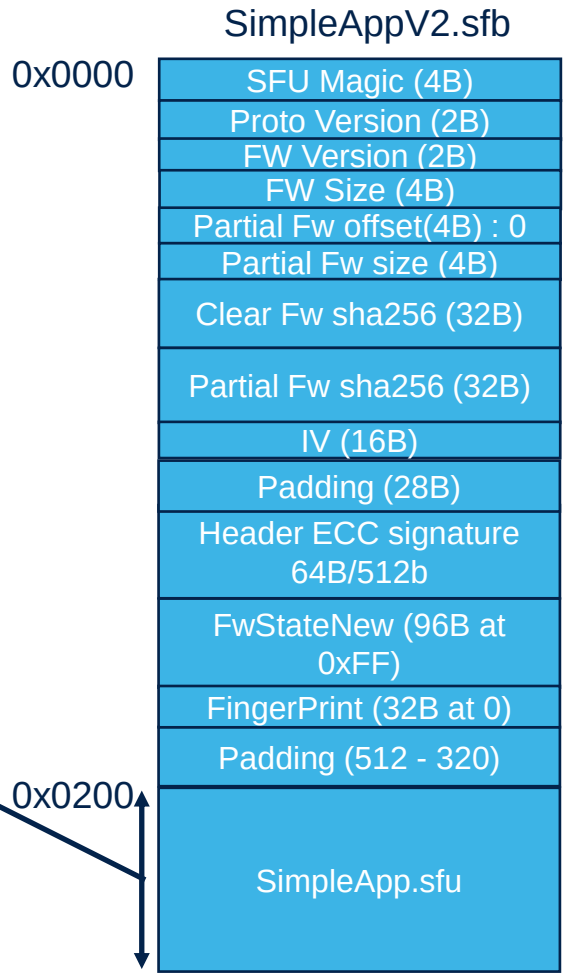
life.augmented

Tampering the firmware update file

- Process :
  - Edit the update binary file and change one bit in the firmware part
  - Try to update the device using this tampered file
  - Analyze what happens

Tampering the firmware update file

- Go to C:\STM32SecuWS\L4\STM32L476_SimpleApp\Binary\
- Duplicate STM32L476_SimpleAppV2.sfb to create
  - STM32L476_SimpleAppV2_FWCorrupt.sfb
- Edit the file using C:\STM32Secu\Tools\HxD\HxD.exe
- Change one bit in the encrypted firmware (0x200 to end)
- Save
- Launch the update and use this corrupted file



Trace

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 Software reset!
          INFO: Last execution detected error was: No error. Success.
= [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
= [SBOOT] STATE: HANDLE CRITICAL FAILURE
= [EXCPT] FIRMWARE SIGNATURE CHECK FAILED!
= [SBOOT] STATE: REBOOT STATE MACHINE
========= End of Execution ==========


= [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: Firmware signature check fail
ure.
= [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
Hello World
Heartbeat
Heartbeat
Heartbeat
```

Firmware integrity check failed

Stay with old version

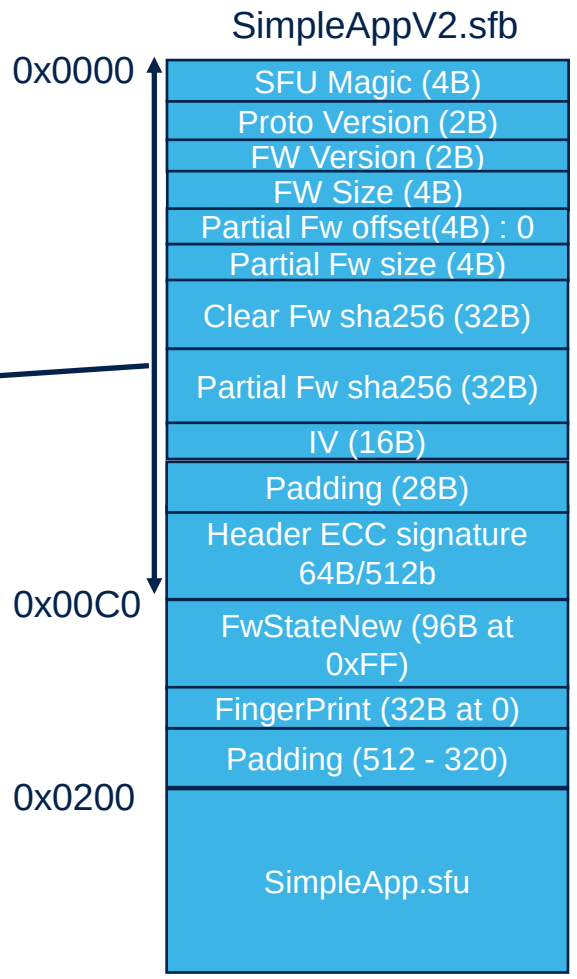
life.augmented

Tampering the header part

- Change one bit in the header
- The header is protected thanks to an ECDSA signature (asymmetric)
- Any change in the header is detected immediately thanks to this signature check

Tampering the firmware update file

- Go to c:\STM32SecuWS\L4\STM32L476_SimpleApp\Binary\
- Duplicate STM32L476_SimpleAppV2.sfb to create
  - STM32L476_SimpleAppV2_HeaderCorrupt.sfb
- Edit the file using C:\STM32Secu\Tools\HxD\HxD.exe
- Change one bit in the metadata (0x0 to 0xC0)
- Save
- Launch the update and use this corrupted file



life.augmented

Trace

COM60 - Tera Term VT

File Edit Setup Control Window Help

```
Heartbeat
Heartbeat

= [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: DOWNLOAD NEW USER FIRMWARE
          File> Transfer> YMODEM> Send
= [SBOOT] STATE: HANDLE CRITICAL FAILURE
= [EXCPT] HEADER AUTHENTICATION FAILURE!
= [SBOOT] STATE: REBOOT STATE MACHINE
========= End of Execution ==========


= [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: Header authentication failed.
= [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
Hello World
Heartbeat
Heartbeat
```

Header corruption detected.

life.augmented

Conclusion

- The SBSFU is robust to any possible hack on the downloaded firmware image
- There will be no installation of any corrupted/hacked firmware
- This is the main purpose of a secure firmware update !

life.augmented

Thank you

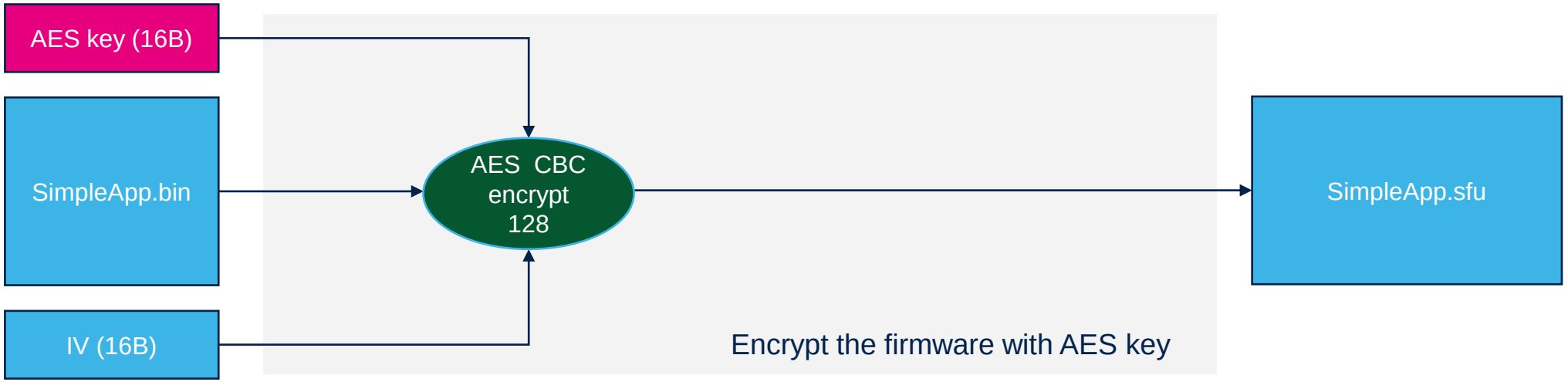
life.augmented

Appendix
Detail of postbuild scripts

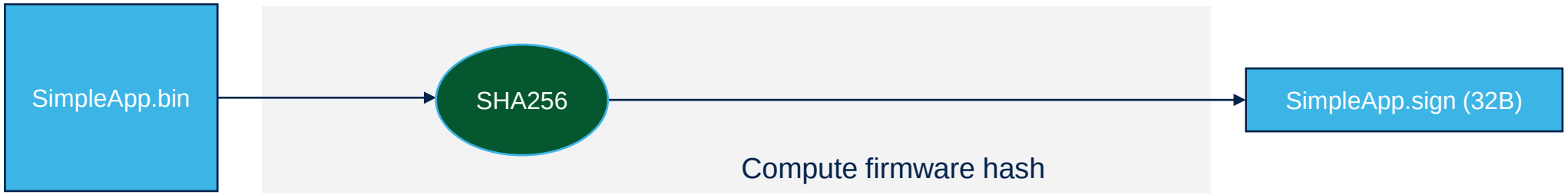
life.augmented

Firmware update binary generation

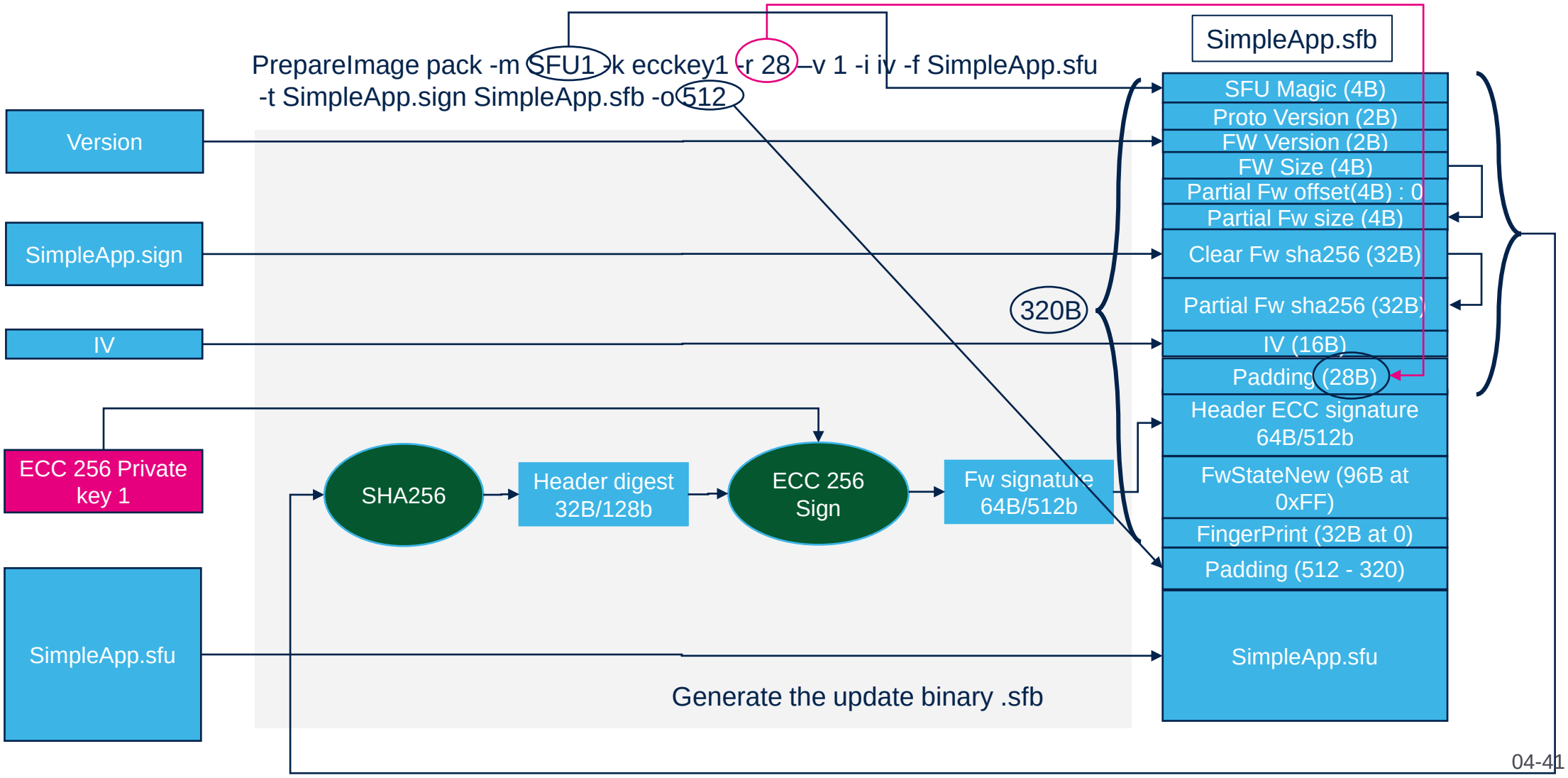
PrepareImage enc -k key -i iv SimpleApp.bin SimpleApp.sfu



PrepareImage sha256 SimpleApp.bin SimpleApp.sign

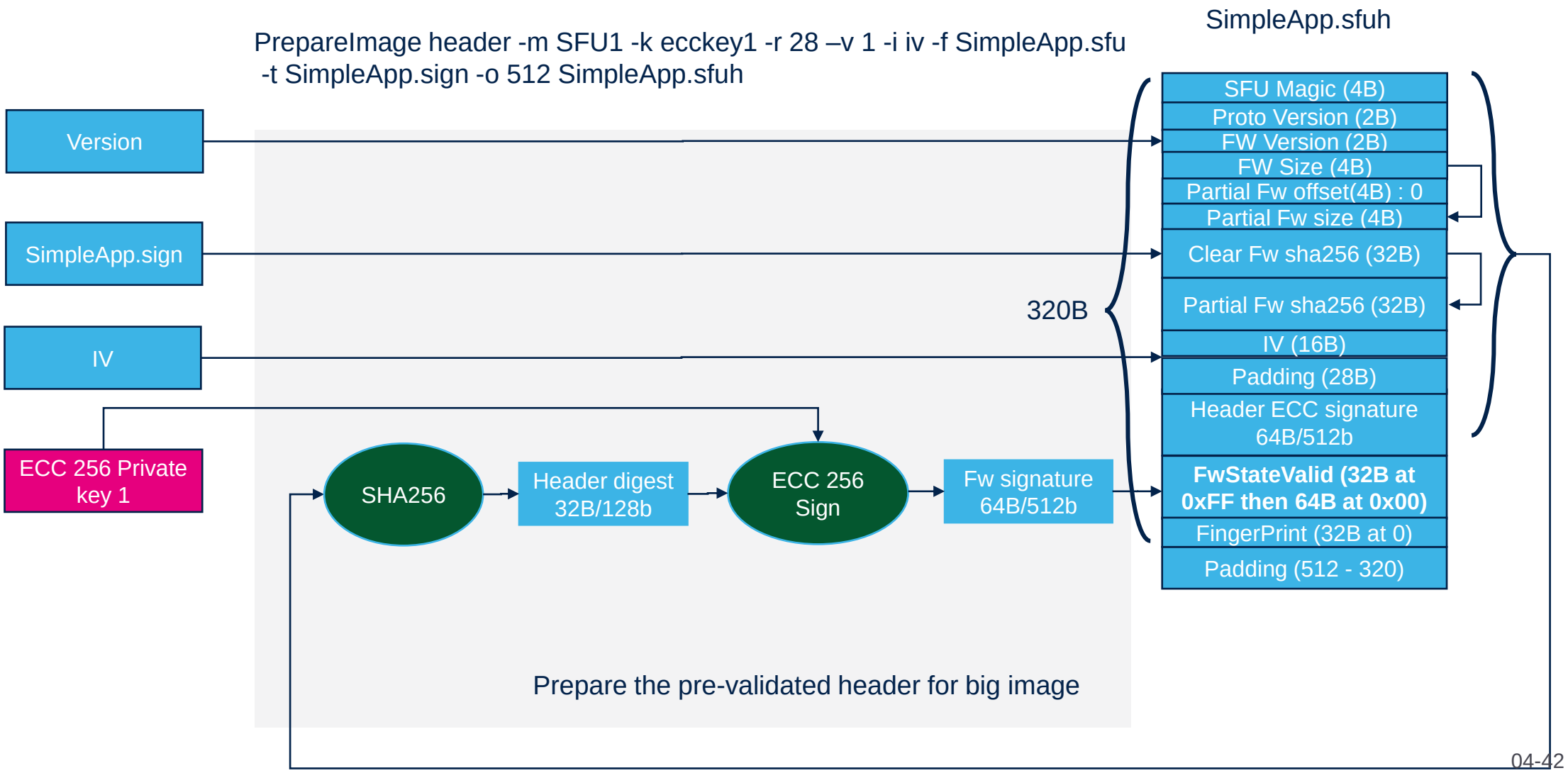


Firmware update binary generation



life.augmented

SBSFU pre-validated Header generation



life.augmented

SBSFU + SimpleApp generation