Instruction Rewriting

Prepared by: Shane Reilly

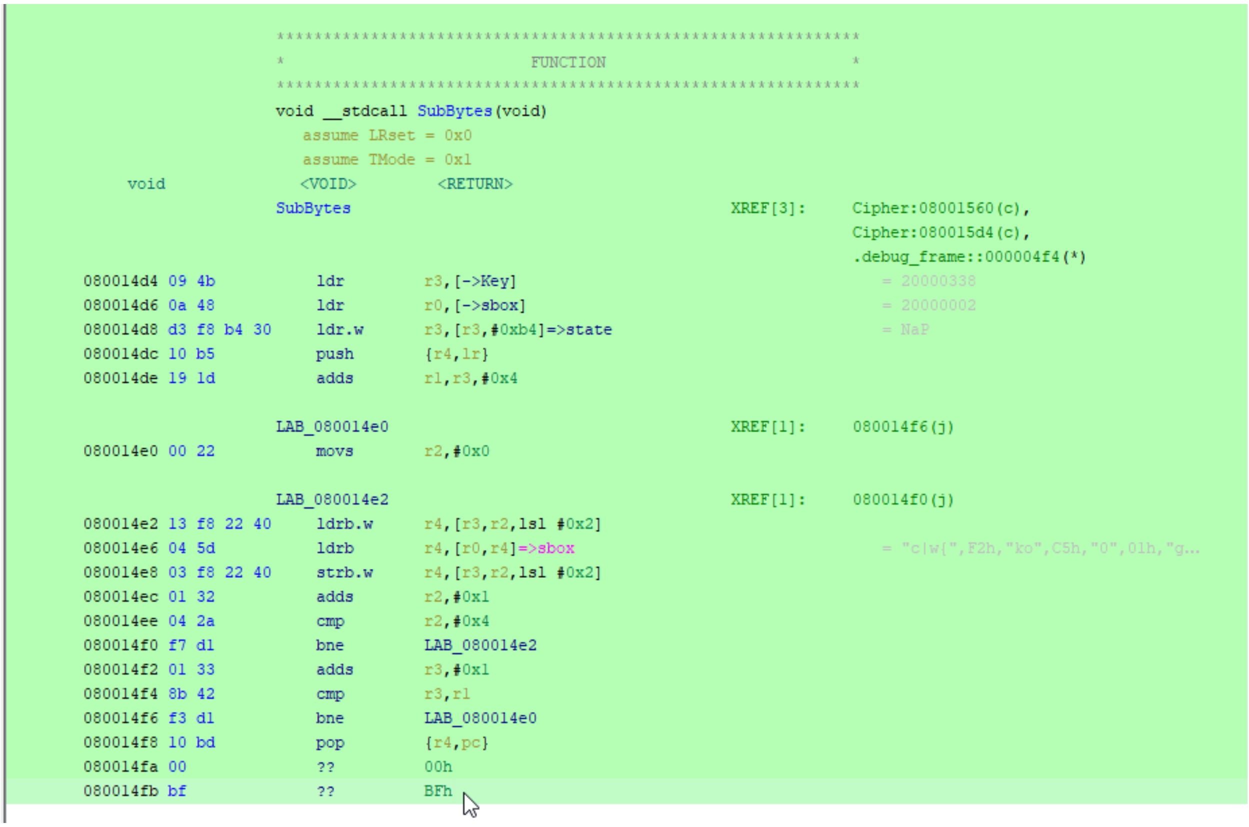
Email: reillysp@mail.uc.edu

Class of 2023, University of Cincinnati, Computer Science

This document explains how to add additional instructions to an STM32 binary without altering the behavior. The binary used here will be the ELF file. The sample file used in this document was compiled with arm-non-eabi-gcc version 8.3.1.

1. Build the firmware normally. Take the simpleserial-aes-CW308_STM32F3.elf file and load it inside of Ghidra (https://ghidra-sre.org/). A copy is featured in the `samples` folder of this repository with the name of **`before_simpleserial-aes-CW308_STM32F3`**. The format and language should automatically populate. Select the file and allow Ghidra to auto-analyze.

2. Navigate to the **`SubBytes`** function. Note that the last two bytes occur after the return.

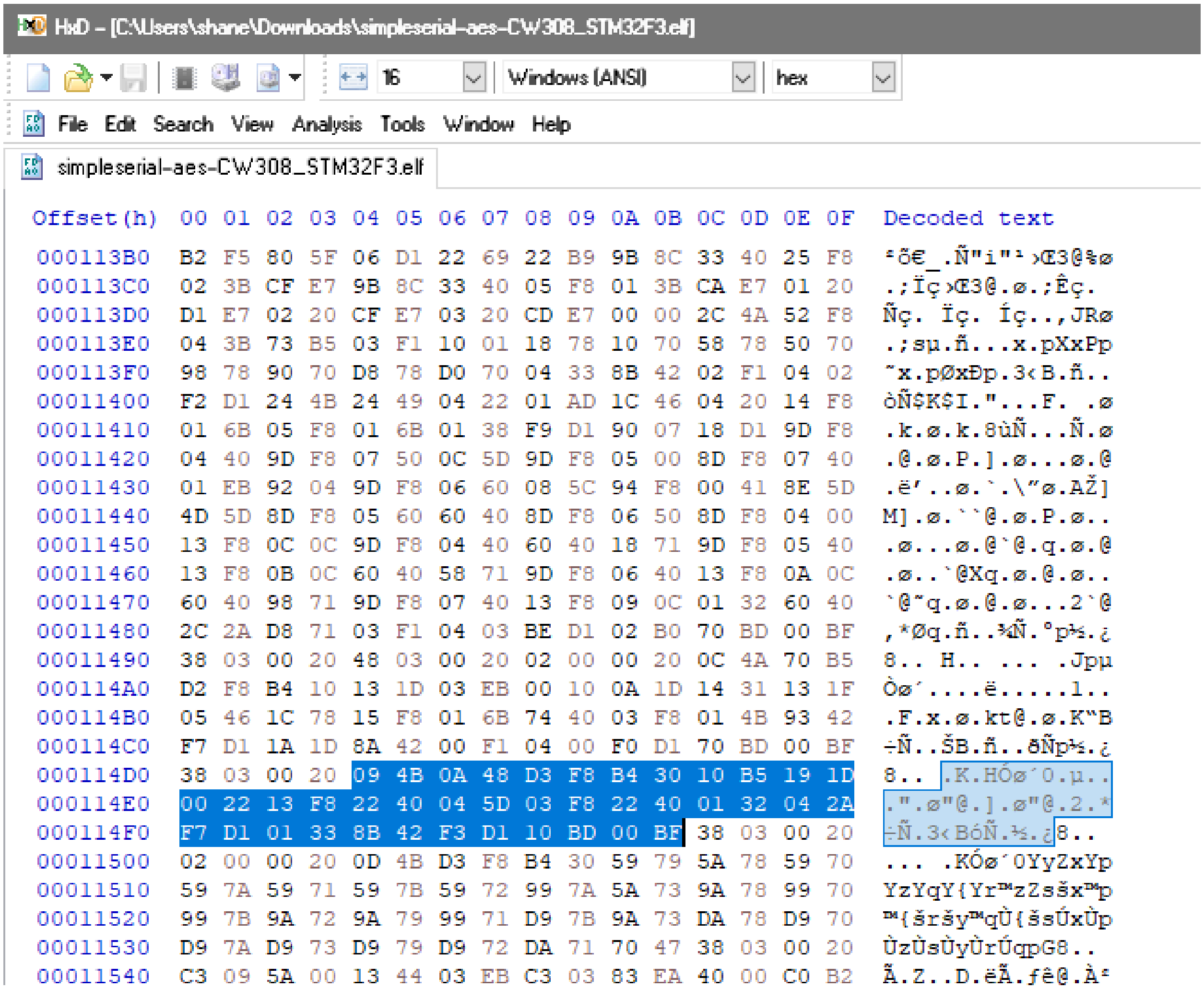


```
                     ***************************************************************
                     *                          FUNCTION                           *
                     ***************************************************************
                     void __stdcall SubBytes(void)
                       assume LRset = 0x0
                       assume TMode = 0x1
     void              <VOID>         <RETURN>
                     SubBytes                                   XREF[3]:     Cipher:08001560(c),
                                                                             Cipher:080015d4(c),
                                                                             .debug_frame::000004f4(*)
080014d4 09 4b          ldr        r3,[->Key]                                   = 20000338
080014d6 0a 48          ldr        r0,[->sbox]                                  = 20000002
080014d8 d3 f8 b4 30    ldr.w      r3,[r3,#0xb4]=>state                         = NaP
080014dc 10 b5          push       {r4,lr}
080014de 19 1d          adds       r1,r3,#0x4

                     LAB_080014e0                               XREF[1]:     080014f6(j)
080014e0 00 22          movs       r2,#0x0

                     LAB_080014e2                               XREF[1]:     080014f0(j)
080014e2 13 f8 22 40    ldrb.w     r4,[r3,r2,lsl #0x2]
080014e6 04 5d          ldrb       r4,[r0,r4]=>sbox                             = "c|w{",F2h,"ko",C5h,"0",01h,"g...
080014e8 03 f8 22 40    strb.w     r4,[r3,r2,lsl #0x2]
080014ec 01 32          adds       r2,#0x1
080014ee 04 2a          cmp        r2,#0x4
080014f0 f7 d1          bne        LAB_080014e2
080014f2 01 33          adds       r3,#0x1
080014f4 8b 42          cmp        r3,r1
080014f6 f3 d1          bne        LAB_080014e0
080014f8 10 bd          pop        {r4,pc}
080014fa 00             ??         00h
080014fb bf             ??         BFh
```

3. Open simpleserial-aes-CW308_STM32F3 inside of HxD32 (https://mh-nexus.de/en/hxd/). Use the search function to search for the byte pattern of the **`SubBytes`** function (**`09 4b 0a 48 d2 f8`**…)

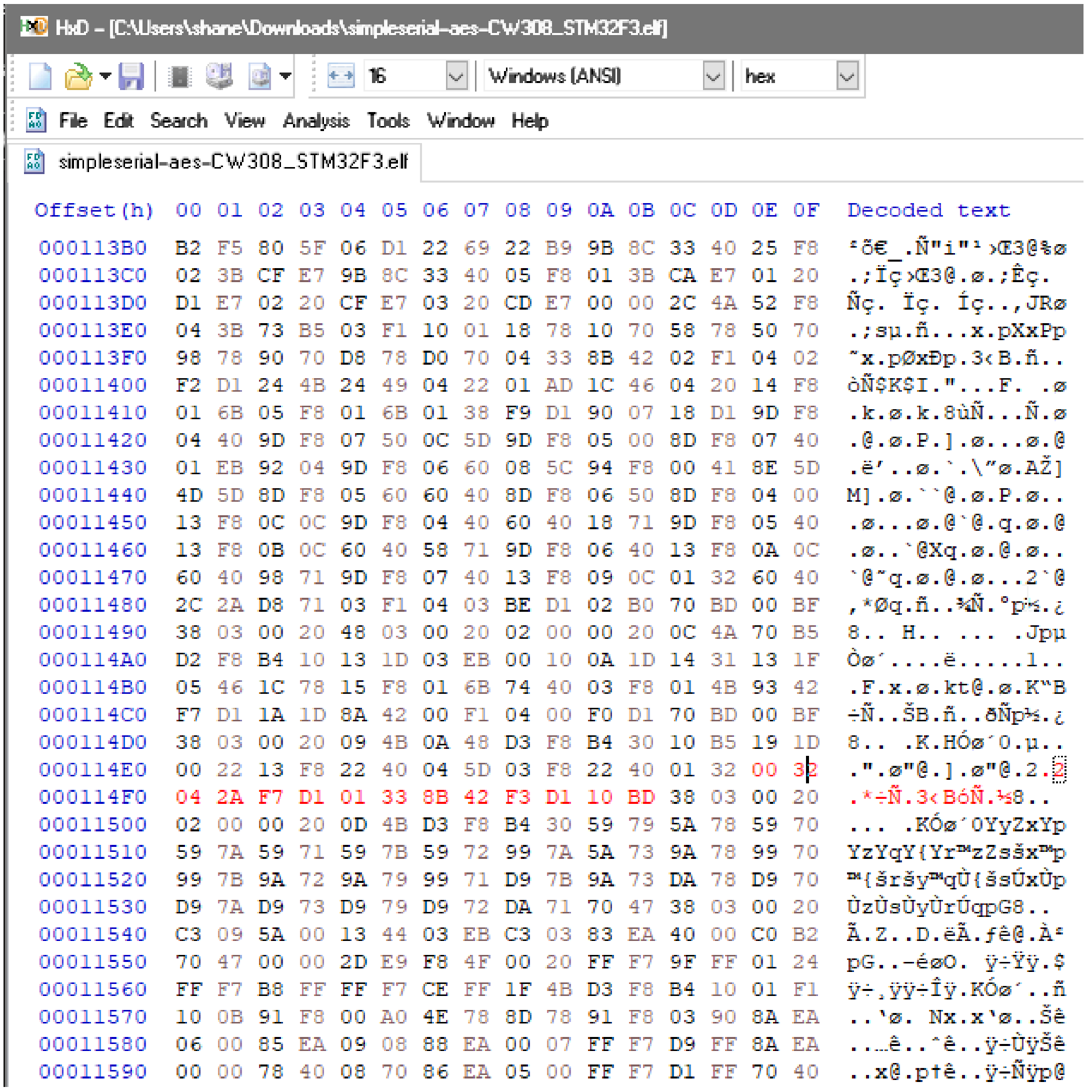

HxD - [C:\Users\shane\Downloads\simpleserial-aes-CW308_STM32F3.elf]
File
Edit
Search
View
Analysis
Tools
Window
Help
simpleserial-aes-CW308_STM32F3.elf

16 | Windows (ANSI) | hex

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

000113B0  B2 F5 80 5F 06 D1 22 69 22 B9 9B 8C 33 40 25 F8  ²õ€_.Ñ"i"¹›Œ3@%ø
000113C0  02 3B CF E7 9B 8C 33 40 05 F8 01 3B CA E7 01 20  .;Ïç›Œ3@.ø.;Êç. 
000113D0  D1 E7 02 20 CF E7 03 20 CD E7 00 00 2C 4A 52 F8  Ñç. Ïç. Íç..,JRø
000113E0  04 3B 73 B5 03 F1 10 01 18 78 10 70 58 78 50 70  .;sµ.ñ...x.pXxPp
000113F0  98 78 90 70 D8 78 D0 70 04 33 8B 42 02 F1 04 02  ˜x.pØxÐp.3‹B.ñ..
00011400  F2 D1 24 4B 24 49 04 22 01 AD 1C 46 04 20 14 F8  òÑ$K$I."..F. .ø
00011410  01 6B 05 F8 01 6B 01 38 F9 D1 90 07 18 D1 9D F8  .k.ø.k.8ùÑ...Ñ.ø
00011420  04 40 9D F8 07 50 0C 5D 9D F8 05 00 8D F8 07 40  .@.ø.P.].ø...ø.@
00011430  01 EB 92 04 9D F8 06 60 08 5C 94 F8 00 41 8E 5D  .ë’..ø.`.\”ø.AŽ]
00011440  4D 5D 8D F8 05 60 60 40 8D F8 06 50 8D F8 04 00  M].ø.``@.ø.P.ø..
00011450  13 F8 0C 0C 9D F8 04 40 60 40 18 71 9D F8 05 40  .ø...ø.@`@.q.ø.@
00011460  13 F8 0B 0C 60 40 58 71 9D F8 06 40 13 F8 0A 0C  .ø..`@Xq.ø.@.ø..
00011470  60 40 98 71 9D F8 07 40 13 F8 09 0C 01 32 60 40  `@˜q.ø.@.ø...2`@
00011480  2C 2A D8 71 03 F1 04 03 BE D1 02 B0 70 BD 00 BF  ,*Øq.ñ..¾Ñ.°p½.¿
00011490  38 03 00 20 48 03 00 20 02 00 00 20 0C 4A 70 B5  8.. H.. ... .Jpµ
000114A0  D2 F8 B4 10 13 1D 03 EB 00 10 0A 1D 14 31 13 1F  Òø´....ë.....1..
000114B0  05 46 1C 78 15 F8 01 6B 74 40 03 F8 01 4B 93 42  .F.x.ø.kt@.ø.K“B
000114C0  F7 D1 1A 1D 8A 42 00 F1 04 00 F0 D1 70 BD 00 BF  ÷Ñ..ŠB.ñ..ðÑp½.¿
000114D0  38 03 00 20 09 4B 0A 48 D3 F8 B4 30 10 B5 19 1D  8.. .K.HÓø´0.µ..
000114E0  00 22 13 F8 22 40 04 5D 03 F8 22 40 01 32 04 2A  .".ø"@.].ø"@.2.*
000114F0  F7 D1 01 33 8B 42 F3 D1 10 BD 00 BF 38 03 00 20  ÷Ñ.3‹BóÑ.½.¿8.. 
00011500  02 00 00 20 0D 4B D3 F8 B4 30 59 79 5A 78 59 70  ... .KÓø´0YyZxYp
00011510  59 7A 59 71 59 7B 59 72 99 7A 5A 73 9A 78 99 70  YzYqY{Yr™zZsšx™p
00011520  99 7B 9A 72 9A 79 99 71 D9 7B 9A 73 DA 78 D9 70  ™{šršy™qÙ{šsÚxÙp
00011530  D9 7A D9 73 D9 79 D9 72 DA 71 70 47 38 03 00 20  ÙzÙsÙyÙrÚqpG8.. 
00011540  C3 09 5A 00 13 44 03 EB C3 03 83 EA 40 00 C0 B2  Ã.Z..D.ëÃ.ƒê@.À²
```

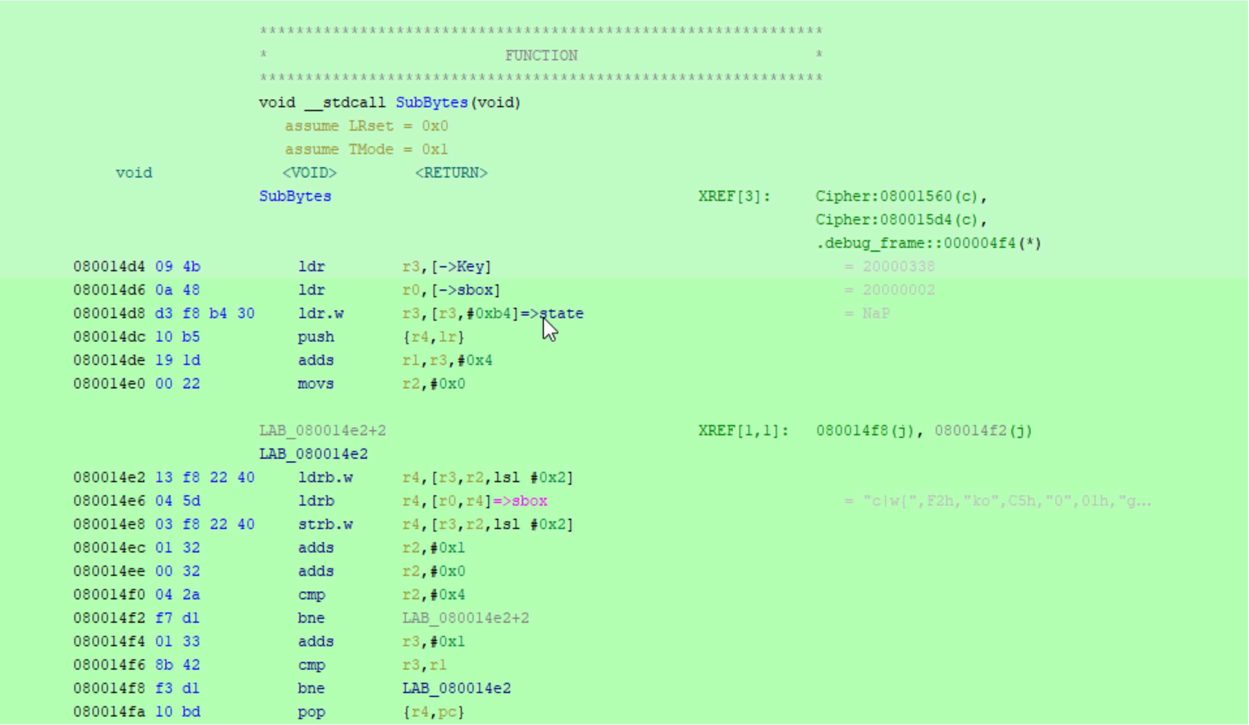
4. Erase the **`00 bf`** bytes, and shift the rest of the bytes forward starting from the location where the desired instruction will be inserted. This example is adding the bytes **`00 33`** (**`adds r2, #0`**). Save when finished.


HxD - [C:\Users\shane\Downloads\simpleserial-aes-CW308_STM32F3.elf]
16
Windows (ANSI)
hex
File Edit Search View Analysis Tools Window Help
simpleserial-aes-CW308_STM32F3.elf

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

000113B0  B2 F5 80 5F 06 D1 22 69 22 B9 9B 8C 33 40 25 F8  ²õ€_.Ñ"i"¹›Œ3@%ø
000113C0  02 3B CF E7 9B 8C 33 40 05 F8 01 3B CA E7 01 20  .;Ïç›Œ3@.ø.;Êç. 
000113D0  D1 E7 02 20 CF E7 03 20 CD E7 00 00 2C 4A 52 F8  Ñç. Ïç. Íç..,JRø
000113E0  04 3B 73 B5 03 F1 10 01 18 78 10 70 58 78 50 70  .;sµ.ñ...x.pXxPp
000113F0  98 78 90 70 D8 78 D0 70 04 33 8B 42 02 F1 04 02  ˜x.pØxÐp.3‹B.ñ..
00011400  F2 D1 24 4B 24 49 04 22 01 AD 1C 46 04 20 14 F8  òÑ$K$I."...F. .ø
00011410  01 6B 05 F8 01 6B 01 38 F9 D1 90 07 18 D1 9D F8  .k.ø.k.8ùÑ...Ñ.ø
00011420  04 40 9D F8 07 50 0C 5D 9D F8 05 00 8D F8 07 40  .@.ø.P.].ø...ø.@
00011430  01 EB 92 04 9D F8 06 60 08 5C 94 F8 00 41 8E 5D  .ë’..ø.`.\”ø.AŽ]
00011440  4D 5D 8D F8 05 60 60 40 8D F8 06 50 8D F8 04 00  M].ø.``@.ø.P.ø..
00011450  13 F8 0C 0C 9D F8 04 40 60 40 18 71 9D F8 05 40  .ø...ø.@`@.q.ø.@
00011460  13 F8 0B 0C 60 40 58 71 9D F8 06 40 13 F8 0A 0C  .ø..`@Xq.ø.@.ø..
00011470  60 40 98 71 9D F8 07 40 13 F8 09 0C 01 32 60 40  `@˜q.ø.@.ø...2`@
00011480  2C 2A D8 71 03 F1 04 03 BE D1 02 B0 70 BD 00 BF  ,*Øq.ñ..¾Ñ.°p½.¿
00011490  38 03 00 20 48 03 00 20 02 00 00 20 0C 4A 70 B5  8.. H.. ... .Jpµ
000114A0  D2 F8 B4 10 13 1D 03 EB 00 10 0A 1D 14 31 13 1F  Òø´....ë.....1..
000114B0  05 46 1C 78 15 F8 01 6B 74 40 03 F8 01 4B 93 42  .F.x.ø.kt@.ø.K“B
000114C0  F7 D1 1A 1D 8A 42 00 F1 04 00 F0 D1 70 BD 00 BF  ÷Ñ..ŠB.ñ..ðÑp½.¿
000114D0  38 03 00 20 09 4B 0A 48 D3 F8 B4 30 10 B5 19 1D  8.. .K.HÓø´0.µ..
000114E0  00 22 13 F8 22 40 04 5D 03 F8 22 40 01 32 00 32  .".ø"@.].ø"@.2.2
000114F0  04 2A F7 D1 01 33 8B 42 F3 D1 10 BD 38 03 00 20  .*÷Ñ.3‹BóÑ.½8.. 
00011500  02 00 00 20 0D 4B D3 F8 B4 30 59 79 5A 78 59 70  ... .KÓø´0YyZxYp
00011510  59 7A 59 71 59 7B 59 72 99 7A 5A 73 9A 78 99 70  YzYqY{Yr™zZsšx™p
00011520  99 7B 9A 72 9A 79 99 71 D9 7B 9A 73 DA 78 D9 70  ™{šršy™qÙ{šsÚxÙp
00011530  D9 7A D9 73 D9 79 D9 72 DA 71 70 47 38 03 00 20  ÙzÙsÙyÙrÚqpG8.. 
00011540  C3 09 5A 00 13 44 03 EB C3 03 83 EA 40 00 C0 B2  Ã.Z..D.ëÃ.ƒê@.À²
00011550  70 47 00 00 2D E9 F8 4F 00 20 FF F7 9F FF 01 24  pG..-éøO. ÿ÷Ÿÿ.$
00011560  FF F7 B8 FF FF F7 CE FF 1F 4B D3 F8 B4 10 01 F1  ÿ÷¸ÿÿ÷Îÿ.KÓø´..ñ
00011570  10 0B 91 F8 00 A0 4E 78 8D 78 91 F8 03 90 8A EA  ..‘ø. Nx.x‘ø..Šê
00011580  06 00 85 EA 09 08 88 EA 00 07 FF F7 D9 FF 8A EA  ..…ê..ˆê..ÿ÷ÙÿŠê
00011590  00 00 78 40 08 70 86 EA 05 00 FF F7 D1 FF 70 40  ..x@.p†ê..ÿ÷Ñÿp@
```

5. To view the changes, re-import the altered file into Ghidra. Observe that there is now a new instruction. The changed sample file is saved in the **`/samples`** folder of this repository with the name **`after_simpleserial-aes-CW308_STM32F3`**.



```
                        ****************************************************************
                        *                            FUNCTION                          *
                        ****************************************************************
                        void __stdcall SubBytes(void)
                          assume LRset = 0x0
                          assume TMode = 0x1
     void                 <VOID>          <RETURN>
                        SubBytes                                        XREF[3]:     Cipher:08001560(c),
                                                                                     Cipher:080015d4(c),
                                                                                     .debug_frame::000004f4(*)
080014d4 09 4b               ldr         r3,[->Key]                                     = 20000338
080014d6 0a 48               ldr         r0,[->sbox]                                    = 20000002
080014d8 d3 f8 b4 30         ldr.w       r3,[r3,#0xb4]=>state                           = NaP
080014dc 10 b5               push        {r4,lr}
080014de 19 1d               adds        r1,r3,#0x4
080014e0 00 22               movs        r2,#0x0

                        LAB_080014e2+2                                  XREF[1,1]:   080014f8(j), 080014f2(j)
                        LAB_080014e2
080014e2 13 f8 22 40         ldrb.w      r4,[r3,r2,lsl #0x2]
080014e6 04 5d               ldrb        r4,[r0,r4]=>sbox                               = "c|w{",F2h,"ko",C5h,"0",01h,"g...
080014e8 03 f8 22 40         strb.w      r4,[r3,r2,lsl #0x2]
080014ec 01 32               adds        r2,#0x1
080014ee 00 32               adds        r2,#0x0
080014f0 04 2a               cmp         r2,#0x4
080014f2 f7 d1               bne         LAB_080014e2+2
080014f4 01 33               adds        r3,#0x1
080014f6 8b 42               cmp         r3,r1
080014f8 f3 d1               bne         LAB_080014e2
080014fa 10 bd               pop         {r4,pc}
```

6. To create a hex file from the binary to flash on to the target board, run the following command (where **simpleserial-aes-CW308_STM32F3.elf** is the name of your altered ELF file):

   ```
   arm-none-eabi-objcopy -O ihex -R .eeprom -R .fuse -R .lock -R .signature
   simpleserial-aes-CW308_STM32F3.elf simpleserial-aes-CW308_STM32F3.hex
   ```