

[Tutorial] Porting and Compiling ASM files

[Tutorial] Porting and Compiling ASM files

by [miguel8e](#) on 08 Feb 2009 06:04

Porting and Compiling ASM Files

This Tutorial is a continuation of [\[Tutorial\] Making ASM File](#)

Code: [Select all](#)

```
include "x.inc"

branch      equ      0x452ADDE8
hook        equ      0x45C00940+1
address1    equ      0x452ADF86+1
address2    equ      0x45719CFC
address3    equ      0x45004834+1
address4    equ      0x44FD5504+1
address5    equ      0x44F34E55
address6    equ      0x450FAD09
address7    equ      0x452ADC98+1

org 0x452ADD9C
    BEQ      branch

org 0x452ADDE8
    LDR      R3, off_452ADDEC
    BX      R3

off_452ADDEC    DCD hook

org 0x45C00940
loc_45C00940:
    PUSH     {R4}
    LDR      R3, off_45C00988
    BLX      R3
    CMP      R0, 0
    NOP
    LDR      R0, off_45C0098C
    LDR      R3, off_45C00994
    BLX      R3
    CMP      R0, 0
    BNE      loc_45C0096E
    LDR      R0, off_45C00990
    LDR      R3, off_45C00994
    BLX      R3
    CMP      R0, 0
    BNE      loc_45C0096E
    ADR      R1, aSlideropen_mp3
    CMP      R4, 0x3F
    BEQ      loc_45C00966
    ADR      R1, aSliderclose_mp
```

```

loc_45C00966:
    LDR    R0, off_45C00980
    MOVS   R2, 0x32
    LDR    R3, off_45C00984
    BLX    R3

loc_45C0096E:
    POP     {R4}
    MOVS    R0, 0x27
    CMP     R4, 0x40
    BNE     loc_45C00978
    MOVS    R0, 0x28

loc_45C00978:
    LDR     R3, off_45C0097C
    BX      R3

align 4

off_45C0097C    DCD address1
off_45C00980    DCD address2
off_45C00984    DCD address3
off_45C00988    DCD address4
off_45C0098C    DCD address5
off_45C00990    DCD address6
off_45C00994    DCD address7

aSlideropen_mp3    du "slideropen.mp3",0

align 4

aSliderclose_mp    du "sliderclose.mp3",0

```

-with UndoPatch.idc you will remove the patch applied before.

To port asm files to others models phones, is necessary to find the addresses at header:

```

branch equ 0x452ADDE8
hook equ 0x45C00940+1
address1 equ 0x452ADF86+1
address2 equ 0x45719CFC
address3 equ 0x45004834+1
address4 equ 0x44FD5504+1
address5 equ 0x44F34E55
address6 equ 0x450FAD09
address7 equ 0x452ADC98+1

```

This port will be for W850

1-Searching addresses

in IDA, press G key to jump to the addresses, analyze the code with C key, and the analyzed code is

this:

452ADDE8:

Code: [Select all](#)

```
ROM:452ADDE8          ;
-----
ROM:452ADDE8 27 20          MOV    R0, #0x27
ROM:452ADDEA CC E0          B      loc_452ADF86
ROM:452ADDEA          ;
-----
```

as the code is too short, is necessary to analyze more code to find quickly the address in the new model, like this:

branch 452ADDE8:

Code: [Select all](#)

```
ROM:452ADDE8          ;
-----
ROM:452ADDE8 27 20          MOV    R0, #0x27
ROM:452ADDEA CC E0          B      loc_452ADF86
ROM:452ADDEC          ;
-----
ROM:452ADDEC 28 20          MOV    R0, #0x28
ROM:452ADDEE CA E0          B      loc_452ADF86
ROM:452ADDF0          ;
-----
ROM:452ADDF0 68 46          MOV    R0, SP
ROM:452ADDF2 00 78          LDRB   R0, [R0]
ROM:452ADDF4 00 28          CMP    R0, #0
ROM:452ADDF6 03 D1          BNE    loc_452ADE00
ROM:452ADDF8 68 46          MOV    R0, SP
ROM:452ADDFA 40 78          LDRB   R0, [R0,#1]
ROM:452ADDFC 00 28          CMP    R0, #0
ROM:452ADDFE 01 D0          BEQ    loc_452ADE04
ROM:452ADE00
ROM:452ADE00          loc_452ADE00          ; CODE XREF: ROM:452ADDF6j
ROM:452ADE00 22 20          MOV    R0, #0x22
ROM:452ADE02 C0 E0          B      loc_452ADF86
ROM:452ADE04          ;
-----
ROM:452ADE04
ROM:452ADE04          loc_452ADE04          ; CODE XREF: ROM:452ADDFEj
ROM:452ADE04 21 20          MOV    R0, #0x21
ROM:452ADE06 BE E0          B      loc_452ADF86
ROM:452ADE06          ;
-----
```

address1 452ADF86:

Code: [Select all](#)

```
ROM:452ADF86          ;
-----
```

```

ROM:452ADF86
ROM:452ADF86          loc_452ADF86                      ; CODE XREF: ROM:452ADDEAj
ROM:452ADF86                      ; ROM:452ADDEEj ...
ROM:452ADF86 FE F7 A3 FF          BL      sub_452ACED0
ROM:452ADF8A 38 BD                POP     {R3-R5,PC}
ROM:452ADF8C          ;
-----
ROM:452ADF8C F0 B5                PUSH    {R4-R7,LR}
ROM:452ADF8E 12 06                LSL     R2, R2, #0x18
ROM:452ADF90 58 D1                BNE     loc_452AE044
ROM:452ADF92 2D 4C                LDR     R4, dword_452AE048
ROM:452ADF94 A8 F0 A6 F9          BL      sub_453562E4
ROM:452ADF98 00 28                CMP     R0, #0
ROM:452ADF9A 51 D0                BEQ     loc_452AE040
ROM:452ADF9C 2B 4E                LDR     R6, off_452AE04C
ROM:452ADF9E 00 20                MOV     R0, #0
ROM:452ADFA0 01 F0 A8 FF          BL      sub_452AFEF4
ROM:452ADFA4 05 1C                ADD     R5, R0, #0
ROM:452ADFA6 30 1C                ADD     R0, R6, #0
ROM:452ADFA8 7B F5 80 FC          BL      sub_450298AC
ROM:452ADFAC 00 2D                CMP     R5, #0
ROM:452ADFAE 49 D0                BEQ     loc_452AE044
ROM:452ADFB0 28 1C                ADD     R0, R5, #0
ROM:452ADFB2 01 F0 B5 FB          BL      sub_452AF720
ROM:452ADFB6 FE F7 CB FA          BL      sub_452AC550
ROM:452ADFB8 07 1C                ADD     R7, R0, #0
ROM:452ADFB0 60 68                LDR     R0, [R4,#4]
ROM:452ADFB2 87 42                CMP     R7, R0
ROM:452ADFC0 03 D0                BEQ     loc_452ADFCA
ROM:452ADFC2 01 20                MOV     R0, #1
ROM:452ADFC4 20 60                STR     R0, [R4]
ROM:452ADFC6 67 60                STR     R7, [R4,#4]
ROM:452ADFC8 F0 BD                POP     {R4-R7,PC}
ROM:452ADFCA          ;
-----

```

address2 45719CFC:

This address goes to a path (unicode), to analyze this, we'll press A instead C, first, select the whole pat, in this case since 45719CFC until 45719D2A, then press A key, and the new code is:

Code: [Select all](#)

```

ROM:45719CFC 2F 00 74 00+aTpaPresetSyste DCB
"/",0,"t",0,"p",0,"a",0,"/",0,"p",0,"r",0,"e",0,"s",0,"e",0,"t"
ROM:45719CFC 70 00 61 00+          DCB
0,"/",0,"s",0,"y",0,"s",0,"t",0,"e",0,"m",0,"/",0,"s",0,"o",0
ROM:45719CFC 2F 00 70 00+          DCB "u",0,"n",0,"d"

```

address3 45004834:

Code: [Select all](#)

```

ROM:45004834          ;
-----
ROM:45004834 F7 B5                PUSH    {R0-R2,R4-R7,LR}
ROM:45004836 05 1C                ADD     R5, R0, #0
ROM:45004838 0E 1C                ADD     R6, R1, #0
ROM:4500483A 00 F0 A1 F8          BL      sub_45004980

```

ROM:4500483E	04	1C	ADD	R4, R0, #0
ROM:45004840	68	46	MOV	R0, SP
ROM:45004842	00	21	MOV	R1, #0
ROM:45004844	01	71	STRB	R1, [R0,#4]
ROM:45004846	00	2C	CMP	R4, #0
ROM:45004848	34	D0	BEQ	loc_450048B4
ROM:4500484A	31	1C	ADD	R1, R6, #0
ROM:4500484C	28	1C	ADD	R0, R5, #0
ROM:4500484E	00	F0 F9 F8	BL	sub_45004A44
ROM:45004852	05	1C	ADD	R5, R0, #0
ROM:45004854	2E	D0	BEQ	loc_450048B4
ROM:45004856	37	4E	LDR	R6, dword_45004934
ROM:45004858	6B	46	MOV	R3, SP
ROM:4500485A	37	6A	LDR	R7, [R6,#0x20]
ROM:4500485C	00	22	MOV	R2, #0
ROM:4500485E	7F	1C	ADD	R7, R7, #1
ROM:45004860	37	62	STR	R7, [R6,#0x20]
ROM:45004862	11	1C	ADD	R1, R2, #0
ROM:45004864	0F	B4	PUSH	{R0-R3}
ROM:45004866	69	4A	LDR	R2, dword_45004A0C
ROM:45004868	3B	1C	ADD	R3, R7, #0
ROM:4500486A	27	68	LDR	R7, [R4]
ROM:4500486C	20	1C	ADD	R0, R4, #0
ROM:4500486E	BF	6F	LDR	R7, [R7,#0x78]
ROM:45004870	B8	47	BLX	R7
ROM:45004872	91	4A	LDR	R2, off_45004AB8
ROM:45004874	07	1C	ADD	R7, R0, #0
ROM:45004876	FF	23	MOV	R3, #0xFF
ROM:45004878	42	33	ADD	R3, #0x42
ROM:4500487A	29	1C	ADD	R1, R5, #0
ROM:4500487C	00	20	MOV	R0, #0
ROM:4500487E	FF	F7 91 FF	BL	sub_450047A4
ROM:45004882	04	B0	ADD	SP, SP, #0x10
ROM:45004884	00	2F	CMP	R7, #0
ROM:45004886	15	D4	BMI	loc_450048B4
ROM:45004888	23	68	LDR	R3, [R4]
ROM:4500488A	00	99	LDR	R1, [SP]
ROM:4500488C	68	46	MOV	R0, SP
ROM:4500488E	02	7A	LDRB	R2, [R0,#8]
ROM:45004890	20	1C	ADD	R0, R4, #0
ROM:45004892	F0	33	ADD	R3, #0xF0
ROM:45004894	1B	68	LDR	R3, [R3]
ROM:45004896	98	47	BLX	R3
ROM:45004898	30	1C	ADD	R0, R6, #0
ROM:4500489A	10	30	ADD	R0, #0x10
ROM:4500489C	00	F0 C2 F8	BL	sub_45004A24
ROM:450048A0	00	99	LDR	R1, [SP]
ROM:450048A2	32	6A	LDR	R2, [R6,#0x20]
ROM:450048A4	00	23	MOV	R3, #0
ROM:450048A6	10	36	ADD	R6, #0x10
ROM:450048A8	30	1C	ADD	R0, R6, #0
ROM:450048AA	00	F0 B3 F8	BL	sub_45004A14
ROM:450048AE	68	46	MOV	R0, SP
ROM:450048B0	01	21	MOV	R1, #1
ROM:450048B2	01	71	STRB	R1, [R0,#4]
ROM:450048B4				
ROM:450048B4		loc_450048B4		; CODE XREF:
ROM:45004848j				
ROM:450048B4				;

```

ROM:45004854j ...
ROM:450048B4 68 46          MOV      R0, SP
ROM:450048B6 00 79          LDRB     R0, [R0,#4]
ROM:450048B8 FE BD          POP      {R1-R7,PC}
ROM:450048B8                ;
-----

```

address4 44FD5504:

Code: [Select all](#)

```

ROM:44FD5504                ;
-----
ROM:44FD5504 4F 48          LDR      R0, dword_44FD5644
ROM:44FD5506 00 7F          LDRB     R0, [R0,#0x1C]
ROM:44FD5508 70 47          BX       LR
ROM:44FD550A                ;
-----
ROM:44FD550A 00 00          LSL      R0, R0, #0
ROM:44FD550C 4D 48          LDR      R0, dword_44FD5644
ROM:44FD550E 20 30          ADD      R0, #0x20
ROM:44FD5510 00 78          LDRB     R0, [R0]
ROM:44FD5512 70 47          BX       LR
ROM:44FD5514                ;
-----
ROM:44FD5514 73 B5          PUSH     {R0,R1,R4-R6,LR}
ROM:44FD5516 04 1C          ADD      R4, R0, #0
ROM:44FD5518 00 20          MOV      R0, #0
ROM:44FD551A 00 90          STR      R0, [SP]
ROM:44FD551C 68 46          MOV      R0, SP
ROM:44FD551E 00 21          MOV      R1, #0
ROM:44FD5520 01 71          STRB     R1, [R0,#4]
ROM:44FD5522 00 F0 29 FD    BL       sub_44FD5F78
ROM:44FD5526 05 1C          ADD      R5, R0, #0
ROM:44FD5528 00 F0 26 FD    BL       sub_44FD5F78
ROM:44FD552C 19 4A          LDR      R2, off_44FD5594
ROM:44FD552E 1A 49          LDR      R1, off_44FD5598
ROM:44FD5530 06 1C          ADD      R6, R0, #0
ROM:44FD5532 28 1C          ADD      R0, R5, #0
ROM:44FD5534 35 68          LDR      R5, [R6]
ROM:44FD5536 6B 46          MOV      R3, SP
ROM:44FD5538 2D 6A          LDR      R5, [R5,#0x20]
ROM:44FD553A A8 47          BLX     R5
ROM:44FD553C 00 2C          CMP      R4, #0
ROM:44FD553E 02 D0          BEQ      loc_44FD5546
ROM:44FD5540 01 2C          CMP      R4, #1
ROM:44FD5542 02 D0          BEQ      loc_44FD554A
ROM:44FD5544 03 E0          B       loc_44FD554E
ROM:44FD5546                ;
-----

```

address5 44F34E55:

Sometimes it is necessary to subtract 1 to the addresses to be analyzed, otherwise, the IDA will say "Command MakeCode failed"

in this case 44F34E55-1 = **44F34E54**

Code: [Select all](#)

```
ROM:44F34E54          ;
-----
ROM:44F34E54 09 49          LDR    R1, off_44F34E7C
ROM:44F34E56 40 68          LDR    R0, [R0,#4]
ROM:44F34E58 88 42          CMP     R0, R1
ROM:44F34E5A 01 D1          BNE     loc_44F34E60
ROM:44F34E5C 01 20          MOV     R0, #1
ROM:44F34E5E 70 47          BX      LR
ROM:44F34E60          ;
-----
ROM:44F34E60
ROM:44F34E60          loc_44F34E60          ; CODE XREF: ROM:44F34E5Aj
ROM:44F34E60 00 20          MOV     R0, #0
ROM:44F34E62 70 47          BX      LR
ROM:44F34E64          ;
-----
ROM:44F34E64 05 4B          LDR    R3, off_44F34E7C
ROM:44F34E66 01 1C          ADD     R1, R0, #0
ROM:44F34E68 4A 68          LDR    R2, [R1,#4]
ROM:44F34E6A 00 20          MOV     R0, #0
ROM:44F34E6C 9A 42          CMP     R2, R3
ROM:44F34E6E 04 D1          BNE     loc_44F34E7A
ROM:44F34E70 4C 31          ADD     R1, #0x4C
ROM:44F34E72 09 78          LDRB   R1, [R1]
ROM:44F34E74 03 29          CMP     R1, #3
ROM:44F34E76 00 D1          BNE     loc_44F34E7A
ROM:44F34E78 01 20          MOV     R0, #1
ROM:44F34E7A
ROM:44F34E7A          loc_44F34E7A          ; CODE XREF: ROM:44F34E6Ej
ROM:44F34E7A          ; ROM:44F34E76j
ROM:44F34E7A 70 47          BX      LR
ROM:44F34E7A          ;
-----
ROM:44F34E7C 0D 60 F3 44 off_44F34E7C  DCD  unk_44F3600D          ; DATA XREF: ROM:44F34E54r
ROM:44F34E7C          ; ROM:44F34E64r
ROM:44F34E80          ;
-----
ROM:44F34E80 00 B5          PUSH   {LR}
ROM:44F34E82 00 23          MOV     R3, #0
ROM:44F34E84 1A 1C          ADD     R2, R3, #0
ROM:44F34E86 00 F0 E3 FB          BL      sub_44F35650
ROM:44F34E8A 00 BD          POP     {PC}
```

address6 450FAD09:

Code: [Select all](#)

```
ROM:450FAD08          loc_450FAD08          ; DATA XREF:
ROM:off_450FAD04o
ROM:450FAD08 03 49          LDR     R1, loc_450FAD18
ROM:450FAD0A 40 68          LDR     R0, [R0,#4]
ROM:450FAD0C 88 42          CMP     R0, R1
ROM:450FAD0E 01 D1          BNE     loc_450FAD14
ROM:450FAD10 01 20          MOV     R0, #1
ROM:450FAD12 70 47          BX      LR
ROM:450FAD14          ;
-----
ROM:450FAD14
```


-The hook 45C00940, won't be analyzed, because 45C00940 is a blank zone in the main.

2- Making patterns

The easy way for making patterns is putting "?" in the first bytes of an instruction, without change the other couple. For instructions like a BL, dwords and other 8 digit instructions, will be replaced for ????????

example:

[non-available imaged posted]

branch 452ADDE8:

Code: [Select all](#)

```
??20??E0??20??E0??46??78??28??D1??46??78??28??D0??20??E0
```

address1 452ADF86:

Code: [Select all](#)

```
??????????BD??B5??06??D1??4C??????????28??D0??4E??20??????????1C??1C??????????2D??  
D0??1C??????????????????1C??68??42??D0??20??60??60??BD
```

address2 45719CFC:

For this unicode, we only need the exact path:

/tpa/preset/system/sound

address3 45004834:

Code: [Select all](#)

```
??B5??1C??1C??????????1C??46??21??71??2C??D0??1C??1C??????????1C??D0??4E??46??6A??  
22??1C??62??1C??B4??4A??1C??68??1C??6F??47??4A??1C??23??33??1C??20??????????B0??  
2F??D4??68??99??46??7A??1C??33??68??47??1C??30??????????99??6A??23??36??  
1C??????????46??21??71??46??79??BD
```

address4 44FD5504:

Code: [Select all](#)

```
??48??7F??47??00??48??30??78??47??B5??1C??20??90??46??21??71??????????1C??????????  
4A??49??1C??1C??68??46??6A??47??2C??D0??2C??D0??E0
```

address5 44F34E55-1=44F34E54:

Code: [Select all](#)

```
??49??68??42??D1??20??47??20??47??4B??1C??68??20??42??D1??31??78??29??D1??20??  
47??????????B5??23??1C??????????BD
```

address6 450FAD09:

Code: [Select all](#)

```
??49??68??42??D1??20??47??20??47??84
```

address7 452ADC98:

Code: [Select all](#)

```
??B5??????????BD??B5??????????BD??B5??????????BD??20??E7??B5??24??????????28??  
D0??????????28??D0??????????1C??1C??BD
```

3- Using Smelter

To find all addresses, just copy the pattern and B button at Smelter, then paste the pattern. Press F3 to copy the full offset.

To find strings like in address2 (45719CFC), press T button, and put this:
@/tpa/preset/system/sound

then click in Ok, and Smelter will find all the strings, look for it and press F3 to copy the full offset.

The result of each addresses are:

```
branch: 453CEF64  
address1: 453CF0FA  
address2: 45878B64  
address3: 45135298  
address4: 450F6974  
address5: 4505AF58+1=4505AF59  
address6: 45328760  
address7: 453CEE1C
```

more about Smelter here -> [\[b\]Smelter using tutorial](#)

4- Replacing and Redirecting

Now we can replace in asm the addresses for the new ones.

```
branch equ 0x453CEF64
hook equ 0x45C00940+1
address1 equ 0x453CF0FA+1
address2 equ 0x45878B64
address3 equ 0x45135298+1
address4 equ 0x450F6974+1
address5 equ 0x4505AF58
address6 equ 0x45328760
address7 equ 0x453CEE1C+1
```

to changes the hook, we have to look the Patch Addresses of the model.

Patch Addresses is a kind of library with all the ranges of the patches that use the blank zone of the main.

To know how many space is used by this patch, we need to take the last offset and substract the first offset (offsets that use blank zone), in this case they are: 45c009d0-45c00940, the different is 90, which mean that we need to find a free space of 90 bytes in the Patch Addresses.

for w850, there is a free space of 3B1 bytes between 45CF772F-45CF7AE0, that's perfect.

the hook could be between 45CF7730 and 45CF77C0 (45CF7730+90)

Now the addresses are finally ready

```
branch equ 0x453CEF64
hook equ 0x45CF7730+1
address1 equ 0x453CF0FA+1
address2 equ 0x45878B64
address3 equ 0x45135298+1
address4 equ 0x450F6974+1
address5 equ 0x4505AF58
address6 equ 0x45328760
address7 equ 0x453CEE1C+1
```

5- Compiling

This last step is to generate the VKP file.

a quickly way to compile the asm file is with [ARM Patch Compiler GUI](#) is required the RAW file of the new model phone and of course, the asm file.

(c) miguel8e

<http://www.se-developers.net/>