

EXTRACTION

Datasheet provides the memory map

Debugger/JLink to read to a file

Load into IDA

Draw the rest of the owl

Resource	Start Address	End Address	Size (kB)	PD	AMBA	Comments
Remapped Devices	0	800000	8192	PD_SYS	AHB	Remap IVT into SYSRAM
SYSRAM (code)	800000	880000	512	PD_MEM	AHB	Remapped at 0x0. DA14691 end address: 0x860000
Reserved						
ROM	900000	920000	128	PD_SYS	AHB	Remapped at 0x0

```
→ J-Link>savebin c:\users\chris\bootrom.bin, 0x900000, 0x20000  
Opening binary file for writing... [c:\users\chris\bootrom.bin]  
Reading 131072 bytes from addr 0x00900000 into file...O.K.
```

The figure shows the IDA View-A window with the following details:

- Functions** tab is selected.
- Library function**, **Regular function**, **Instruction**, **Data**, **Unexplored**, **External symbol**, and **Lu** buttons are present at the top.
- IDA View-A** title is displayed.
- Function name** column lists various functions, with **Booter_Flow** currently selected.
- Address** column lists the memory addresses for each function.
- Assembly Code**: The assembly code for the **Booter_Flow** function is shown, starting with:

```
19 CLK_Enable_RC32M();  
20 CRG_TOP_CLK_AMBA_REG[0] = 0;  
21 SYS_WDOG_WATCHDOG_CTRL_REG = 6;  
22 v0 = CRG_TOP_PMU_CTRL_REG;  
23 CRG_TOP_PMU_CTRL_REG = v0 & 0xFFFFFFFF7;  
24 do  
25     ptr_sys_stat_reg = CRG_TOP_SYS_STAT_REG;  
26     while ( (ptr_sys_stat_reg & 0x800) == 0 );  
27     GPIO_P0_08_MODE_REG = 0x200;  
28     GPIO_P0_08_MODE_REG = 0x100;  
29     GPIO_P0_08_MODE_REG = 0x200;  
30     WDOG_feed_ff();  
31     ptr_pmu_ctrl_reg = CRG_TOP_PMU_CTRL_REG;  
32     CRG_TOP_PMU_CTRL_REG = ptr_pmu_ctrl_reg & 0xFFFFFFFFF;  
33 do  
34     ptr_sys_stat_reg_ = CRG_TOP_SYS_STAT_REG;  
35     while ( (ptr_sys_stat_reg_ & 0x200) == 0 );  
36     ptr_power_ctrl_reg = CRG_TOP_POWER_CTRL_REG;  
37     CRG_TOP_POWER_CTRL_REG = ptr_power_ctrl_reg & 0xFF8F;  
38     CRG_TOP_POWER_CTRL_REG = ptr_power_ctrl_reg & 0xFF8F;  
39     ptr_pmu_ctrl_reg_ = CRG_TOP_PMU_CTRL_REG;  
40     CRG_TOP_PMU_CTRL_REG = ptr_pmu_ctrl_reg_ & 0xFFFFFFFF;  
41 do  
42     ptr_sys_stat_reg_ = CRG_TOP_SYS_STAT_REG;  
43     while ( (ptr_sys_stat_reg_ & 8) == 0 );  
44     OTPC_enable_clock_and_reset(1);  
45     OTPC_set_read_mode();  
46     QSPIC_set_manual_mode();  
47     QSPIC_Software_Reset_peripheral();  
48 LSPBYTE(configuration_point) - 1;
```

The screenshot shows the Lumina debugger interface. The top navigation bar includes icons for back, forward, search, and zoom, followed by color-coded category indicators: Library function (blue), Regular function (orange), Instruction (red), Data (yellow), Unexplored (green), External symbol (magenta), and Lumina function (dark green). Below the bar is a legend with the same color-coding.

The main window has two panes. The left pane, titled "Functions", lists 20 functions with their addresses:

Function name	Start
sub_15E8	000015E8
sub_18AC	000018AC
sub_195C	0000195C
sub_1ADC	00001ADC
sub_1C00	00001C00
sub_1C34	00001C34
sub_1C6C	00001C6C
sub_1CAC	00001CAC
sub_1DAC	00001DAC
sub_1DE8	00001DE8
sub_1E20	00001E20
sub_1EC4	00001EC4
sub_1EE0	00001EE0
sub_1EF4	00001EF4
sub_1F08	00001F08
sub_1F46	00001F46
sub_1FA2	00001FA2
sub_2026	00002026

The right pane, titled "Pseudocode-A", displays assembly-like pseudocode:

```
v0 = sub_155C();
MEMORY[0x50000000] = 0;
MEMORY[0x50000704] = 6;
MEMORY[0x50000020] &= ~8u;
while ( (MEMORY[0x50000028] & 0x800) == 0 )
;
MEMORY[0x50020A38] = 0x200;
sub_1544(v0);
MEMORY[0x50000020] &= ~4u;
while ( (MEMORY[0x50000028] & 0x200) == 0 )
;
MEMORY[0x50000F0] = MEMORY[0x50000F0] & 0xFF8FFFFF | 0x400000;
MEMORY[0x50000F0] |= 0x80u;
MEMORY[0x50000020] &= ~1u;
while ( (MEMORY[0x50000028] & 8) == 0 )
;
sub_1CAC(1);
sub_1DAC();
sub_2052();
sub_20B6(v1);
MEMORY[0x2003C954] = 1;
MEMORY[0x2003C958] = 0;
MEMORY[0x50020904] |= 1u;
v2 = sub_264C(0x1106);
MEMORY[0x50020A3C] = 2;
MEMORY[0x50020A381] = 1;
```

ANALYSIS CHALLENGES

Dense code

- No strings
- No symbols
- No debug statements/printf-like functions
- No external libraries

Strings		Hex View-1	
Address	Length	Type	String
ROM:00002...	00000006	C	\n \vJ\vK
ROM:00007...	00000020	C	SigEd25519 no Ed25519 collisions

Line 1 of 2



SUBWAY

Function name	Start
f sub_100	00000100
f sub_1E0	000001E0
f sub_228	00000228
f sub_32C	0000032C
f sub_344	00000344
f sub_384	00000384
f sub_3C4	000003C4
f sub_3E0	000003E0
f sub_3F4	000003F4
f sub_418	00000418
f sub_4D0	000004D0