BOOTROM

Small code block executed first

- Initializes the system
- Handles transition to application/customer code
- Immutable (some exceptions)
  - Manufacturer only “patch” section
  - Focused-ion-beam (FIB)

Security Implemented Here

- Secureboot
- OTP
- Debug/Readback protections

Notable bug examples

- iPhone bugs (limera1n/checkm8)

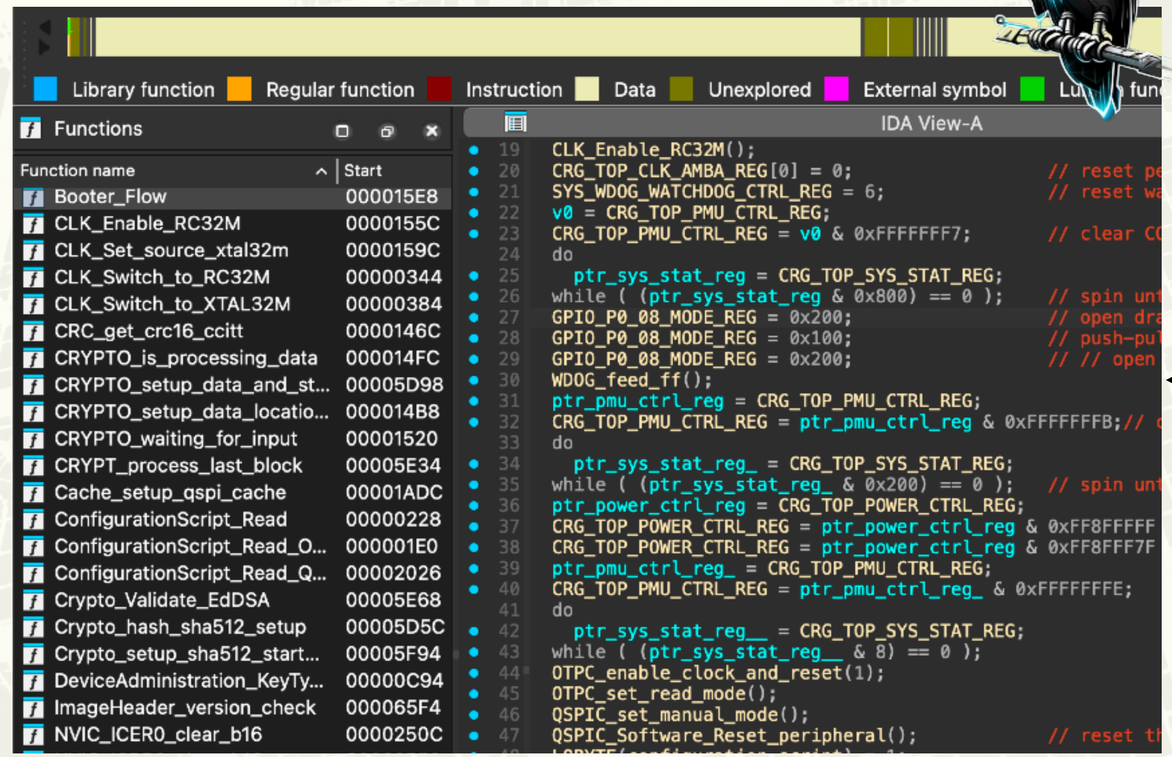
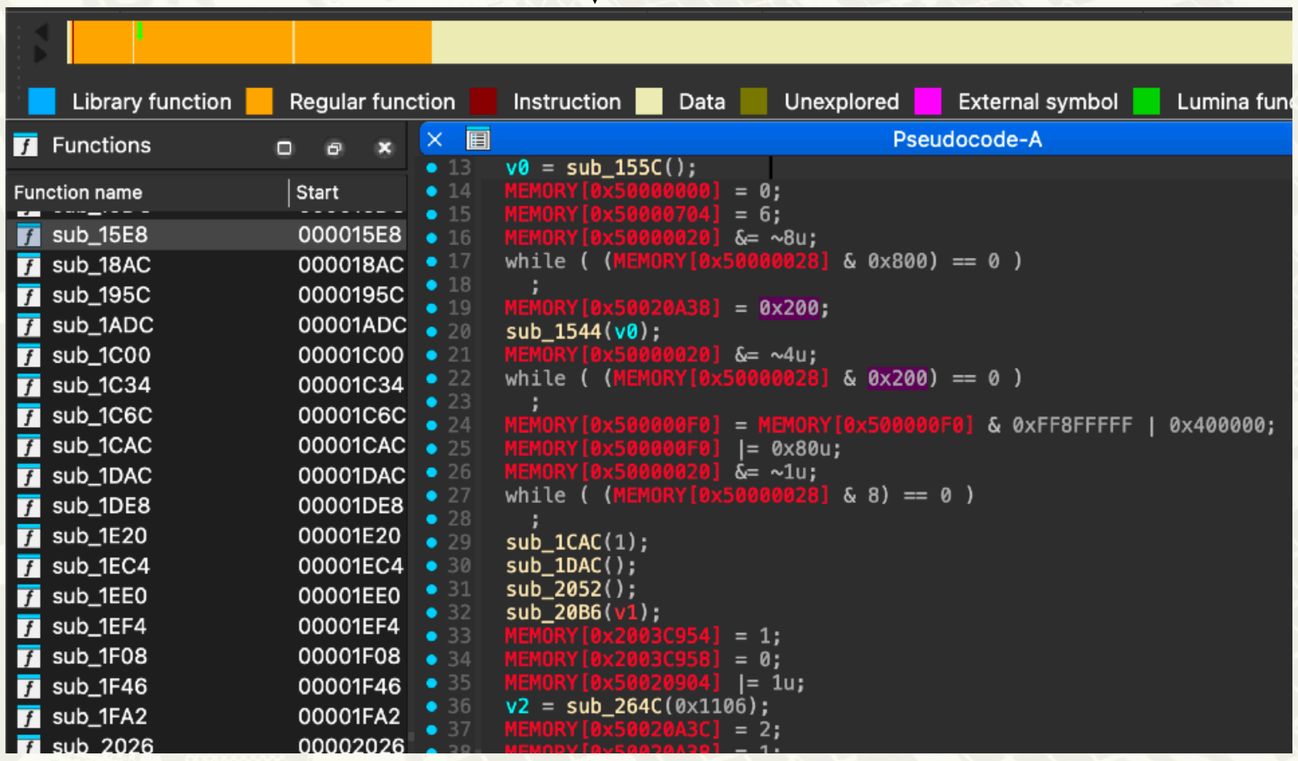
EXTRACTION

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.
```