Iterate over where its being stored in flash to determine where it actually is (0xa7f0-0x200000)

- Make window smaller and smaller until it stopped
- Backup until it works again

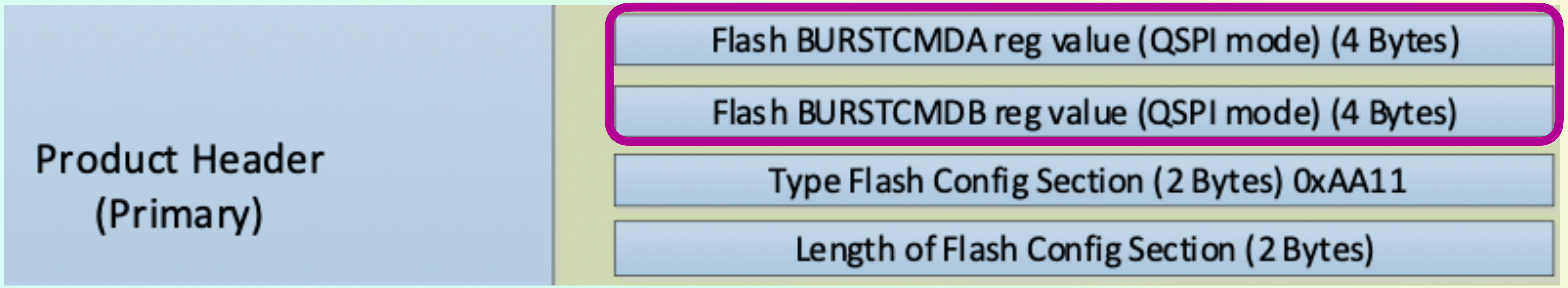
🎉 0x1d4744 - 0x1d4747

NOW WHAT

How to get the encrypted firmware?

Header Config specifies BURSTCMDA/B Registers

- **these control how the SoC talks to the SPI flash**
- **reconfigure to use single mode (0x03)**



Product Header (Primary)

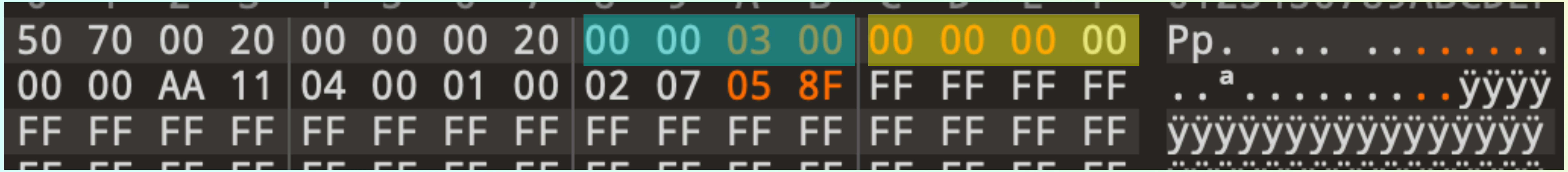
Flash BURSTCMDA reg value (QSPI mode) (4 Bytes)

Flash BURSTCMDB reg value (QSPI mode) (4 Bytes)

Type Flash Config Section (2 Bytes) 0xAA11

Length of Flash Config Section (2 Bytes)

Modified FW



```
50 70 00 20  00 00 00 20  00 00 03 00  00 00 00 00   Pp. ... ........
00 00 AA 11  04 00 01 00  02 07 05 8F  FF FF FF FF   ..ª.........ÿÿÿÿ
FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```