

# 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	.. <sup>a</sup> ..... yyyy
FF FF FF FF	yyyyyyyyyyyyyyyy			
FF FF FF FF	.....			

# PROGRESS

Slowing down the target to Single SPI allows capture, showing the SoC accessing the payload at **0x1d4744**

CMD	ADDRESS	DATA
NORMAL READ(0X03)	1D 47 44	00 BF 00 BF 00 BF 00 BF
NORMAL READ(0X03)	1D 47 60	00 BF 00 BF 00 BF 00 BF