

BACK OF THE NAPKIN HACKING

Modified Nonce

01920304050607080000000000000000 - SP dd7ea2fd Reset 362cf679

Break Payload

cli_programmer.exe COM6 write_qspi_bytes 0x2cf679 0xbe 0xff

Reset/Halt

J-Link>r
Reset delay: 0 ms
Reset type NORMAL: Resets core & peripherals via SYSRESETREQ & VECTRESET bit.
Reset: Halt core after reset via DEMCR.VC_COREREST.
Reset: Reset device via AIRCR.SYSRESETREQ.

Read @ 0x0

J-Link>mem32 0,2
00000000 = DD7EA2FD 362CF679 <----- our reset value

Break

J-Link>s
362CF678: FF BE BKPT #255



T-bit of XPSR is 0 but should be 1. Changed to 1

STILL NOT CONVINCED

We are here

