BACK OF THE NAPKIN HACKING

```
└─[$]> python nonce_hunt\ copy.py FAA30A7DCC58C862576C486BC858DBDCDE88B6DDE0
Searching by byte
potential iv 01920304050607080000000000000000 - SP dd7ea2fd Reset 362cf679
potential iv 01020304050c07080000000000000000 - SP dbdbbef4 Reset 36706836
searching by 4byte blocks
potential iv 01920304050607080000000000000000 - SP dd7ea2fd Reset 362cf679
potential iv 02820304050607080000000000000000 - SP 69b0b6c7 Reset 3634e178
potential iv 050a0304050607080000000000000000 - SP c20a37db Reset 161b2fee
potential iv 05720304050607080000000000000000 - SP fe4dc684 Reset 160d9b52
potential iv 06480304050607080000000000000000 - SP 01eb79c4 Reset 367e69ee
potential iv 06820304050607080000000000000000 - SP 8d43ae5b Reset 1602df1d
potential iv 06ea0304050607080000000000000000 - SP 3fdf567f Reset 164b236f
potential iv 08150304050607080000000000000000 - SP 9093b11d Reset 16545aaf
potential iv 08440304050607080000000000000000 - SP 1f25dbbf Reset 160aaea2
potential iv 098a030405060708000000000000000 - SP 8657becd Reset 3627840e
```

IV = Nonce + Block Counter

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_CORERESET.
Reset: Reset device via AIRCR.SYSRESETREQ.
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