THIS WILL NEVER WORK

QSPI Flash mappings are quite large...

```
QSPI FLASH (Code)   0x16000000 0x16800000
QSPI FLASH (System) 0x36000000 0x36800000
```

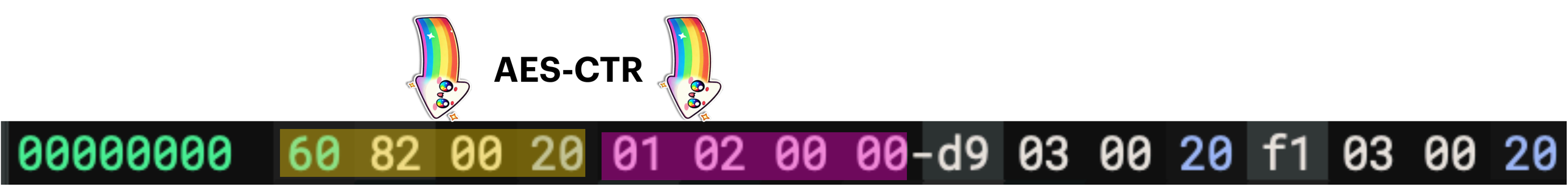
Where could the Reset Vector point to?

First blocks of the encrypted image:

Key: FAA30A7DCC58C862576C486BC858DBDCDE88B6DDE0612E8C3D292A30D6447B02

IV: 59CD394A2E99EE4B0000000000000000


[Stack Pointer]
[Reset Vector]
00000000
a4 69 b0 85
8e ba 5b b1
-fb d1 03 c1 d7 c9 0f 67


AES-CTR
00000000 60 82 00 20 01 02 00 00-d9 03 00 20 f1 03 00 20

THIS WILL NEVER WORK

First blocks of the encrypted image:

```
                [   Stack Pointer    ] [   Reset Vector   ]
00000000  a4 69 b0 85 8e ba 5b b1-fb d1 03 c1 d7 c9 0f 67
```

Key: FAA30A7DCC58C862576C486BC858DBDCDE88B6DDE0612E8C3D292A30D6447B02

IV: 59CD394A2E99EE4B0000000000000000

AES-CTR

```
00000000  60 82 00 20 01 02 00 00-d9 03 00 20 f1 03 00 20
```

Where could the Reset Vector point to?

QSPI Flash mappings are quite large...

```
QSPI FLASH (Code)   0x16000000 0x16800000
QSPI FLASH (System) 0x36000000 0x36800000
```

BACK OF THE NAPKIN HACKING

Quick test script

- **Decrypt a known initial block using a known Nonce/Key**
- **Iterate over Nonce changes**

```
Key                 - FAA30A7DCC58C862576C486BC858DBDCDE88B6DDE0612E8C3D292A30D6447B02
IV(Nonce+Counter)   - 01020304050607080000000000000000
Encrypted Value     - 5D10BBDA05498A9200878AE0A92E56DF
```