Don't fear the Hexdumps

Reverse engineering for the masses

Why poke around?

- For the same reasons as Open Source:
  - Port to other platforms
  - Modify for your own requirements
  - It's your own hardware, dammit
- ...it's satisfying

Example: SWF animation

- Some content providers don't like you downloading and playing offline
- They still make it available for download
- Disable the disabler – you will need:
  - Text editor
  - SWF dumper
  - Hex editor

SWFdump: before

```
[HEADER]        File version: 4
[HEADER]        File size: 2275359
[HEADER]        Frame rate: 12.000000
[HEADER]        Frame count: 3043
[HEADER]        Movie width: 640.00
[HEADER]        Movie height: 360.00
[009]         3 SETBACKGROUNDCOLOR (00/00/00)
                -=> 00 00 00                                            ...
[018]         0 PROTECT
[012]         6 SOUNDSTREAMHEAD
                -=> 0b 2b 2c 07 86 06                                   .+,.<86>.
[02b]         9 FRAMELABEL "loadData"
                -=> 6c 6f 61 64 44 61 74 61 00                          loadData.
[00c]       410 DOACTION
                 (    9 bytes) action: Push String:"key.txt"
                 (    5 bytes) action: Push String:"key"
                 (    0 bytes) action: GetVariable
                 (    1 bytes) action: GetUrl2 192
                 (    5 bytes) action: Push String:"EOF"
                 (    7 bytes) action: Push String:"false"

                                  [ some time later ]

                 (    4 bytes) action: Push String:"40"
                 (    2 bytes) action: Push String:""
                 (    4 bytes) action: Push String:"12"
                 (    0 bytes) action: GetProperty
                 (    0 bytes) action: Less
                 (    0 bytes) action: Not
                 (    2 bytes) action: If 10
                 (    2 bytes) action: GotoFrame 40
                 (    2 bytes) action: Jump 6
                 (    2 bytes) action: GotoFrame 7
                 (    0 bytes) action: Play
                 (    2 bytes) action: Jump 6
```

SWF: what to change

- Find instructions that start the movie

  ```
  81 02 00 28 00
  GotoFrame 40
  ```

- ...paste them in at the beginning

```
000000 46 57 53 04 1f b8 22 00  >FWS...".<
000008 78 00 06 40 00 00 0e 10  >x..@....<
000010 00 00 0c e3 0b 43 02 00  >.....C..<
000018 00 00 00 06 86 04 0b 2b  >.......+<
000020 2c 07 86 06 ff 0a 09 00  >,.......<
000028 00 00 6c 6f 61 64 44 61  >..loadDa<
000030 74 61 00 3f 03 9a 01 00  >ta.?....<
000038 00 96 09 00 00 6b 65 79  >.....key<
000040 2e 74 78 74 00 96 05 00  >.txt....<
000048 00 6b 65 79 00 1c 9a 01  >.key....<
000050 00 c0 96 05 00 00 45 4f  >......EO<
000058 46 00 96 07 00 00 66 61  >F.....fa<
000060 6c 73 65 00 1d 96 10 00  >lse.....<
000068 00 61 6d 49 6f 6e 42 42  >.amIonBB<
000070 43 73 65 72 76 65 72 00  >Cserver.<
```

```
000000 46 57 53 04 1f b8 22 00  >FWS...".<
000008 78 00 06 40 00 00 0e 10  >x..@....<
000010 00 00 0c e3 0b 43 02 00  >.....C..<
000018 00 00 00 06 86 04 0b 2b  >.......+<
000020 2c 07 86 06 ff 0a 09 00  >,.......<
000028 00 00 6c 6f 61 64 44 61  >..loadDa<
000030 74 61 00 3f 03 9a 01 00  >ta.?....<
000038 00 81 02 00 28 00 65 79  >....(.ey<
000040 2e 74 78 74 00 96 05 00  >.txt....<
000048 00 6b 65 79 00 1c 9a 01  >.key....<
000050 00 c0 96 05 00 00 45 4f  >......EO<
000058 46 00 96 07 00 00 66 61  >F.....fa<
000060 6c 73 65 00 1d 96 10 00  >lse.....<
000068 00 61 6d 49 6f 6e 42 42  >.amIonBB<
000070 43 73 65 72 76 65 72 00  >Cserver.<
```

SWFdump: after

```
[HEADER]        File version: 4
[HEADER]        File size: 2275359
[HEADER]        Frame rate: 12.000000
[HEADER]        Frame count: 3043
[HEADER]        Movie width: 640.00
[HEADER]        Movie height: 360.00
[009]         3 SETBACKGROUNDCOLOR (00/00/00)
                -=> 00 00 00                                                ...
[018]         0 PROTECT
[012]         6 SOUNDSTREAMHEAD
                -=> 0b 2b 2c 07 86 06                                       .+,.<86>.
[02b]         9 FRAMELABEL "loadData"
                -=> 6c 6f 61 64 44 61 74 61 00                              loadData.
[00c]       410 DOACTION
                 (    2 bytes) action: GotoFrame 40
                 (    0 bytes) action: BitURShift
                 (    0 bytes) action: unknown[79]
                 (    0 bytes) action: unknown[2e]
                 (    0 bytes) action: unknown[74]
                 (    0 bytes) action: unknown[78]
                 (    0 bytes) action: unknown[74]
                 (    0 bytes) action: End
                -=> 81 02 00 28 00 65 79 2e 74 78 74 00 96 05 00 00         <81>..(.ey.txt.<96>...
                -=> 6b 65 79 00 1c 9a 01 00 c0 96 05 00 00 45 4f 46         key..<9a>..À<96>...EOF
                -=> 00 96 07 00 00 66 61 6c 73 65 00 1d 96 10 00 00         .<96>...false..<96>...
                -=> 61 6d 49 6f 6e 42 42 43 73 65 72 76 65 72 00 96         amIonBBCserver.<96>
                -=> 03 00 00 30 00 1d 96 07 00 00 6d 79 55 72 6c 00         ...0..<96>...myUrl.
                -=> 96 02 00 00 00 96 04 00 00 31 35 00 22 1d 96 0a         <96>....<96>...15.".<96>.
                -=> 00 00 6d 79 4c 65 6e 67 74 68 00 96 07 00 00 6d         ..myLength.<96>...m
                -=> 79 55 72 6c 00 1c 14 1d 96 08 00 00 62 62 63 53         yUrl....<96>...bbcS
                -=> 74 72 00 96 0b 00 00 62 62 63 2e 63 6f 2e 75 6b         tr.<96>...bbc.co.uk
```

```
<html> <body>
    <object>
      <embed src="after.swf" width="640" height="360" type="application/x-shockwave-flash" />
    </object>
</body> </html>
```

Drawbacks

- Some documentation not entirely open
- Many apps under EULA
- Can be seen as aiding copyright violation
  - Advanced eBook Processor
  - rtmpdump
- Complicated – obfuscation arms race