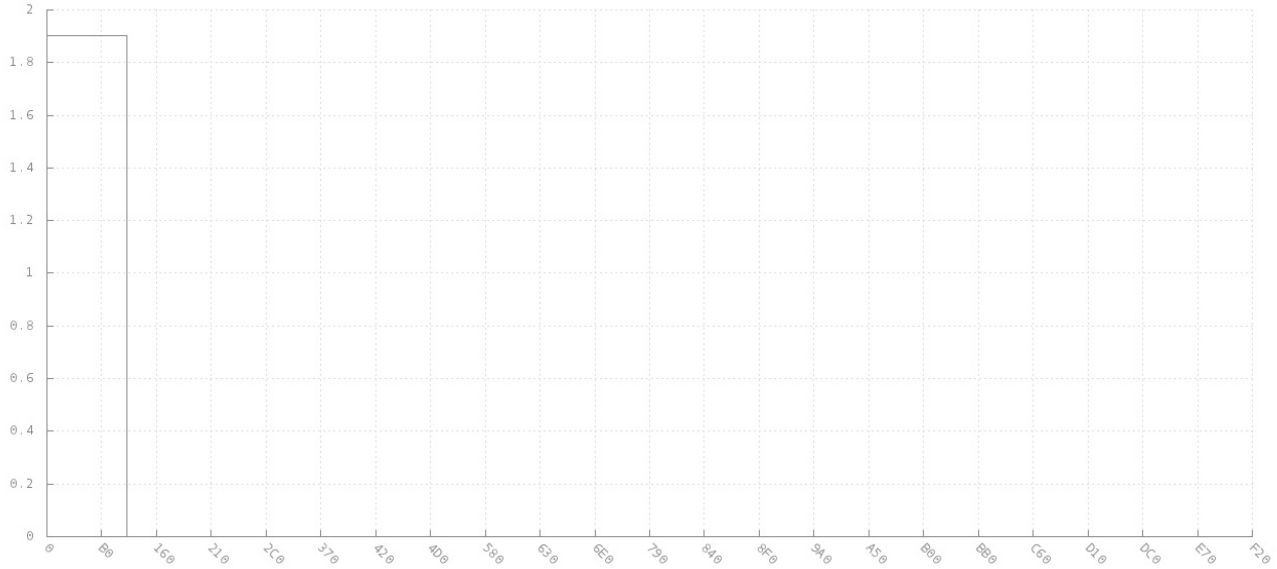
zero.zip

Analysis conducted on Tue 1 Oct 2013 19:22:58 CEST.
File size: 4238 (0x108E)

Entropy



Signatures

```
   0x00000000: ZIP local file header {
   name:          "zero"
   crc:           0x1147406a
   compr. size:   0x00000ff0
   uncompr. size: 0x00400000
}
0x0000102e: ZIP central directory header {
   name:         "zero"
   crc:           0x1147406a
   compr. size:   0x00000ff0
   uncompr. size: 0x00400000
}
```

Command Line Reference

Entropy data:

```
BLOCKSIZE=256 /Users/user/git/libdisorder/code/tools/tropy zero.zip > zero.zip.entropy.dat
```

Entropy graph:

```
   cat > tmp.dot <<"DELIM"

set border 3;
    set xtics nomirror rotate by -45;
    set format x "%X";
    set xtics autofreq 176;
    set border lc rgb "#888888";
    set grid xtics lt 0 lw 1 lc rgb "#e0e0e0";
    set grid ytics lt 0 lw 1 lc rgb "#e0e0e0";
    set ytics nomirror;
    set key inside right bottom enhanced autotitles;
    set nokey;
    set terminal png size 1280, 600 truecolor enhanced font "Andale Mono,10";
    set bmargin 4.5;
    set rmargin 5.0;
    set output "/Users/user/enc/work/samsung/firmware/examples/zero.zip.entropy.png";
    plot "<awk '{x=$2*256; print x,$4}' zero.zip.entropy.dat" with steps lc rgb "#888888";
DELIM
gnuplot -e 'load "tmp.dot"'
```

Signature scan - Sigscan

```
/Users/user/sectk/often/Signatureseach/sigscan/sigscan/trunk/bin/sigscan.osx10.7.4 zero.zip
```

Signature scan - Signsrch

```
wine /Users/user/sectk/often/Signatureseach/signsrch/signsrch.exe zero.zip
```