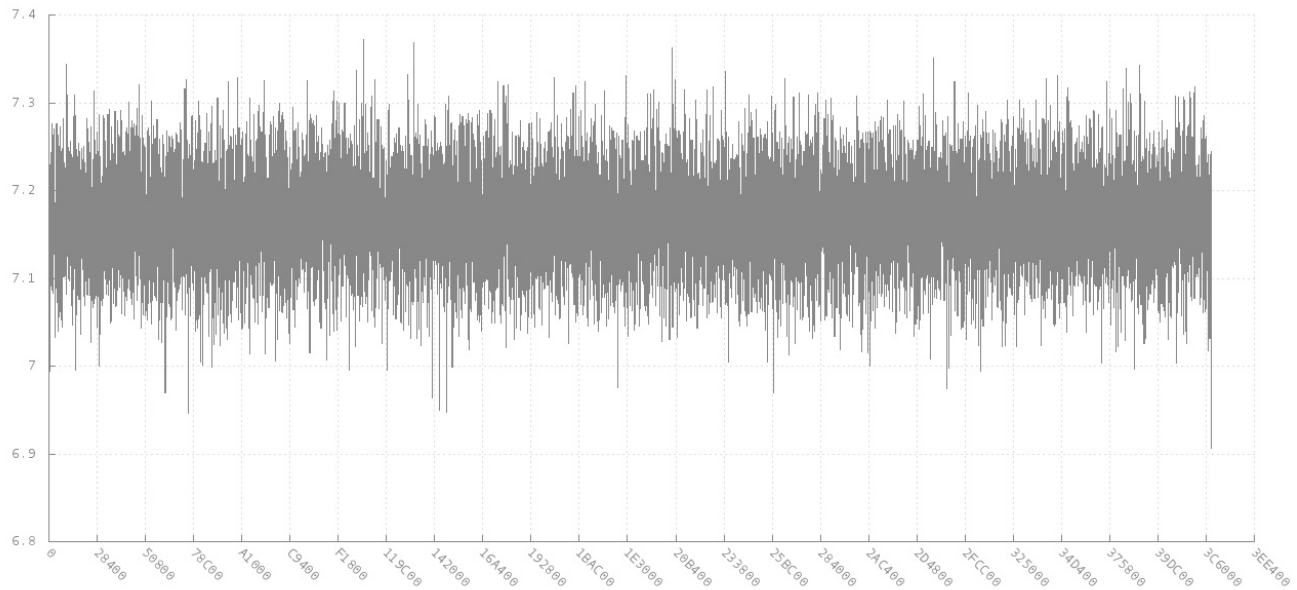


4mbjpg.zip

Analysis conducted on Tue 1 Oct 2013 19:13:55 CEST.
File size: 3975482 (0x3CA93A)

Entropy



Signatures

```
0x00000000: ZIP local file header {
  name:      "4mbjpg"
  crc:       0x127443d8
  compr. size: 0x003ca898
  uncompr. size: 0x003d619c
}
0x003ca8d8: ZIP central directory header {
  name:      "4mbjpg"
  crc:       0x127443d8
  compr. size: 0x003ca898
  uncompr. size: 0x003d619c
}
```

Command Line Reference

Entropy data:

```
BLOCKSIZE=256 /Users/user/git/libdisorder/code/tools/tropy 4mbjpg.zip > 4mbjpg.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 164864;
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/4mbjpg.zip.entropy.png";
plot "<awk '{x=$2*256; print x,$4}' 4mbjpg.zip.entropy.dat" with steps lc rgb "#888888";
DELIM
gnuplot -e 'load "tmp.dot"'
```

Signature scan - Sigscan

```
/Users/user/seck/often/Signaturesearch/sigscan/sigscan/trunk/bin/sigscan.osx10.7.4 4mbjpg.zip
```

Signature scan - Signsrch

```
wine /Users/user/seck/often/Signaturesearch/signsrch/signsrch.exe 4mbjpg.zip
```