DALVIK EXECUTABLE

```
>adb shell dalvikvm -cp /data/hw.zip hw
Hello World!
```

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
000:  .d .e .x 0A .0 .3 .5 00 6F 53 89 BC 1E 79 B2 4F
010:  1F 9C 09 66 15 23 2D 3B 56 65 32 C3 B5 81 B4 5A
020:  70 02 00 00 70 00 00 00 78 56 34 12 00 00 00 00
030:  00 00 00 00 DC 01 00 00 0C 00 00 00 70 00 00 00
040:  07 00 00 00 A0 00 00 00 02 00 00 00 BC 00 00 00
050:  01 00 00 00 D4 00 00 00 02 00 00 00 DC 00 00 00
060:  01 00 00 00 EC 00 00 00 64 01 00 00 0C 01 00 00
070:  A6 01 00 00 3A 01 00 00 8A 01 00 00 40 01 00 00
080:  B4 01 00 00 76 01 00 00 54 01 00 00 6C 01 00 00
090:  57 01 00 00 70 01 00 00 A1 01 00 00 C8 01 00 00
0A0:  01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00
0B0:  05 00 00 00 06 00 00 00 08 00 00 00 07 00 00 00
0C0:  05 00 00 00 34 01 00 00 07 00 00 00 05 00 00 00
0D0:  2C 01 00 00 04 00 01 00 0A 00 00 00 00 00 01 00
0E0:  09 00 00 00 01 00 00 00 0B 00 00 00 00 00 00 00
0F0:  01 00 00 00 02 00 00 00 00 00 00 00 FF FF FF FF
100:  00 00 00 00 D1 01 00 00 00 00 00 00 02 00 01 00
110:  02 00 00 00 00 00 00 00 08 00 00 00 62 00 00 00
120:  1A 01 00 00 6E 20 01 00 10 00 0E 00 01 00 00 00
130:  06 00 00 00 01 00 00 00 03 00 04 .L .h .w .; 00
140:  12 .L .j .a .v .a ./ .l .a .n .g ./ .O .b .j .e
150:  .c .t .; 00 01 .V 00 13 .[ .L .j .a .v .a ./ .l
160:  .a .n .g ./ .S .t .r .i .n .g .; 00 02 .V .L 00
170:  04 .m .a .i .n 00 12 .L .j .a .v .a ./ .l .a .n
180:  .g ./ .S .y .s .t .e .m .; 00 15 .L .j .a .v .a
190:  ./ .i .o ./ .P .r .i .n .t .S .t .r .e .a .m .;
1A0:  00 03 .o .u .t 00 0C .H .e .l .l .o 20 .W .o .r
1B0:  .l .d .! 00 12 .L .j .a .v .a ./ .l .a .n .g ./
1C0:  .S .t .r .i .n .g .; 00 07 .p .r .i .n .t .l .n
1D0:  00 00 00 01 00 00 09 8C 02 00 00 00 0C 00 00 00
1E0:  00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00
1F0:  0C 00 00 00 70 00 00 00 02 00 00 00 07 00 00 00
200:  A0 00 00 00 03 00 00 00 02 00 00 00 BC 00 00 00
210:  04 00 00 00 01 00 00 00 D4 00 00 00 05 00 00 00
220:  02 00 00 00 DC 00 00 00 06 00 00 00 01 00 00 00
230:  EC 00 00 00 01 20 00 00 01 00 00 00 0C 01 00 00
240:  01 10 00 00 02 00 00 00 2C 01 00 00 02 20 00 00
250:  0C 00 00 00 3A 01 00 00 00 20 00 00 01 00 00 00
260:  D1 01 00 00 00 10 00 00 01 00 00 00 DC 01 00 00
```

HEADER

magic	"dex\n035\0"
adler32	0xBC89536F
sha1	1e79b24f1f9c09661523 2d3b566532c3b581b45a
file_size	0x270
header_size	0x70
endian_tag	0x12345678 (little endian)
map offset	0x1DC
size /offsets	
strings ids	0x00C/0x070
type ids	0x007/0x0A0
proto ids	0x002/0x0BC
field ids	0x001/0x0D4
method ids	0x002/0x0DC
class defs	0x001/0x0EC
data	0x164/0x10C

STRING IDS
(A-Z ORDER)

offset (to string)	
0x1A6	("Hello World!")
0x13A	("Lhw;")
0x18A	("Ljava/io/PrintStream;")
0x140	("Ljava/lang/Object;")
0x1B4	("Ljava/lang/String;")
0x176	("Ljava/lang/System;")
0x154	("V")
0x16C	("VL")
0x157	("[Ljava/lang/String;")
0x170	("main")
0x1A1	("out")
0x1C8	("println")

TYPE IDS
(STRING LIST INDEXES)

1 2 3 4 5 6 8

PROTO IDS

string id descriptor	type id return type	offset parameters
7	5	0x134
7	5	0x12C

FIELD IDS

```
class 0x4 (Ljava/lang/System;)
type  0x1 ('Ljava/io/PrintStream;')
name  0xA ('out')
```

METHOD IDS

```
class      0x0 ("Lhw;")
prototype  0x1 ("[Ljava/lang/String;")
name       0x9 ("main")
class      0x1 ("Ljava/io/PrintStream;")
prototype  0x0 ("Ljava/lang/String;")
name       0xB ("println")
```

CLASS DEFS

```
class       0x0 ("hw")
access flag 0x1 (PUBLIC)
superclass  0x2 ("Ljava/lang/Object;")
source      0xFFFFFFFF (none)
data offset 0x1D1
```

CODE

```
registers     2
in args       1 (words)
out args      2 (words)
instructions  8 (words)
 sget-object    v0, Ljava/lang/System;
                ->out:Ljava/io/PrintStream;
 const-string   v1, "Hello World!"
 invoke-virtual {v0, v1}, Ljava/io/PrintStream;
                ->println(Ljava/lang/String;)V
 return-void
```

TYPE LIST

```
size  1
 type  6 ("[Ljava/lang/String;")
size  1
 type  3 ("Ljava/lang/String;")
```

STRING DATA
(MUTF-8)

len	string
04	"Lhw;"
18	"Ljava/lang/Object;"
1	"V"
19	"[Ljava/lang/String;"
2	"VL"
4	"main"
18	"Ljava/lang/System;"
21	"Ljava/io/PrintStream;"
3	"out"
12	"Hello World!"
18	"Ljava/lang/String;"
7	"println"

CLASS DATA

```
direct methods 1
 index diff    0x0
 flags         0x9 (PUBLIC STATIC)
 code offset   0x0208  (0x10C, encoded in uleb128)
```

MAP

```
count 12
          type  /  size / offset
0x0000 (HEADER)        1    0x000
0x0001 (STRING)       12    0x070
0x0002 (TYPE)          7    0x0A0
0x0003 (PROTO)         2    0x0BC
0x0004 (FIELD)         1    0x0D4
0x0005 (METHOD)        2    0x0DC
0x0006 (CLASS)         1    0x0EC
0x2001 (CODE)          1    0x10C
0x1001 (TYPE LIST)     2    0x12C
0x2002 (STRING DATA)  12    0x13A
0x2000 (CLASS DATA)    1    0x1D1
0x1000 (MAP LIST)      1    0x1DC
```


ANGE ALBERTINI
http://pics.corkami.com