# Binwalk

Presented by
1805091 Ruhul Azgor
1805093 Md. Nazmul Islam Ananto

93 Presenting

# Usage

- Signature Finding
- Entropy Analysis
- Forensic Analysis
- Reverse Engineering
  - Developing Compatible Software for Closed-Source Systems
  - Discovering Hidden Vulnerabilities

# Signature Finding

*binwalk -B <file>*

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -B Firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             BIN-Header, board ID: W54G, hardware version: 4702, firmware version: 4.30.30, build dat
e: 2016-01-08
32            0x20            TRX firmware header, little endian, image size: 3534848 bytes, CRC32: 0xB14A8109, flags:
 0x0, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0xB9A70, rootfs offset: 0x0
60            0x3C            gzip compressed data, maximum compression, has original file name: "piggy", from Unix, l
ast modified: 2016-01-08 05:56:58
760464        0xB9A90         Squashfs filesystem, little endian, non-standard signature, version 3.0, size: 2769153 b
ytes, 539 inodes, blocksize: 65536 bytes, created: 2016-01-08 05:58:38

ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -B cool_cat.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1280 x 851, 8-bit/color RGBA, non-interlaced
54            0x36            Zlib compressed data, best compression
442148        0x6BF24         ELF, 32-bit LSB shared object, Intel 80386, version 1 (SYSV)
```

# All signatures [ inc. invalid ones]

*binwalk -I firmware.bin*

Useful when binwalk is treating a valid file as invalid, may mislead with garbages

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -I -B cool_cat.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1280 x 851, 8-bit/color RGBA, non-inter
laced
8             0x8             VxWorks symbol table, big endian, first entry: [ty
pe: function, code address: 0x49484452, symbol address: 0xD],,,,,,,,,
19969         0x4E01          PC bitmap,
26030         0x65AE          ARJ archive data, header size: -25600, version¾½Üv
ÛmjÜòÕöÏ", original file date: 2059-12-15 23:39:18, compressed file size: 140489
0939, uncompressed file size: -1048835,
41213         0xA0FD          Linux EXT filesystem, blocks count: 2137105166, im
age size: 2188395689984, invalid state invalid error behavior invalid major revi
sion rev 761771608.11623, ext4 fiçÚkNó³¿öøã¹Ï}2R<%+°x8b6ddcde-5972-58d1-18cb-b05
9e16ae16a, volume name "*Ü¢A!ÅDYí                    Ã³\Ñ.¶»ãU&$S(ùQ7#ÀÉd2"
```

# Raw String Finding

*binwalk -R ‘<string or escaped in octal>’ <filename>*

This allows to search the specified file(s) for a custom string.

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -R 'hello' cool_cat.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
450348        0x6DF2C         Raw signature (hello)
```

# Opcode Analysis

*binwalk -A <file_name>* or *binwalk -- opcode <file_name>*

Searches for opcode to determine the architecture of the file. Can be misleading.

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -A cool_cat.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
446505        0x6D029         Intel x86 instructions, function prologue
```

# Extraction

*binwalk -e firmware.bin*

Loads common *--dd* extraction rules from a predefined file

```
(base) azgor@azgor-MS-7B98:~/BinwalkPresentation$ binwalk -e hello.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, uncompressed size:
 15588, name: hello
2903          0xB57           End of Zip archive, footer length: 22
```

```
(base) azgor@azgor-MS-7B98:~/BinwalkPresentation$ cd _hello.zip.extracted/
(base) azgor@azgor-MS-7B98:~/BinwalkPresentation/_hello.zip.extracted$ ls
0.zip  hello
```

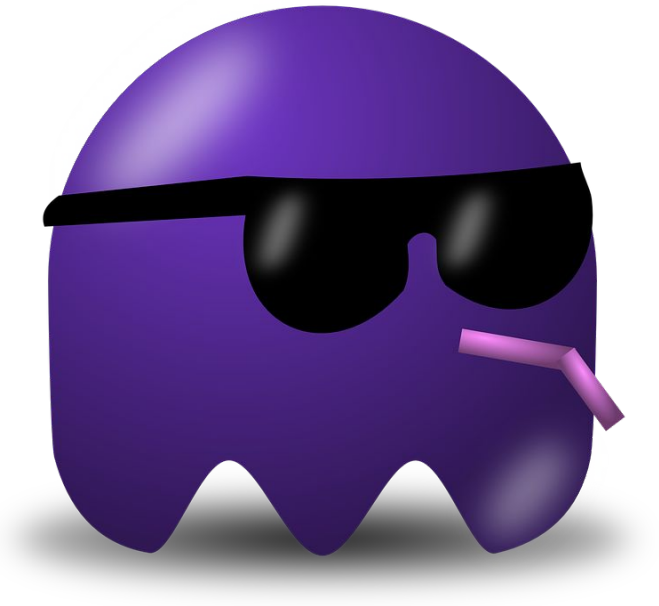
# Extraction

*binwalk -e --dd=".*" firmware.bin*

*--dd =<type[:ext[:cmd]]>* extracts files identified during a *--signature* scan

# Example

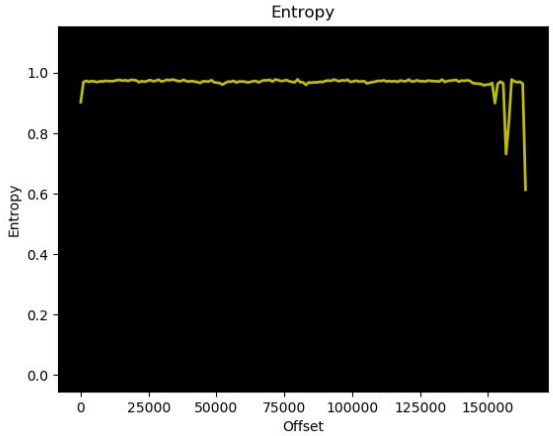
What could be under this seemingly Innocent picture?



# Example

```
ni@nanto:~/4-1/Project/glasses$ binwalk PurpleThing.jpeg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 780 x 720, 8-bit/color RGBA, non-interl
aced
41            0x29            Zlib compressed data, best compression
153493        0x25795         PNG image, 802 x 118, 8-bit/color RGBA, non-interl
aced
ni@nanto:~/4-1/Project/glasses$ binwalk -E PurpleThing.jpeg

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
1024          0x400           Rising entropy edge (0.969866)
153600        0x25800         Rising entropy edge (0.963949)
156672        0x26400         Falling entropy edge (0.731285)
158720        0x26C00         Rising entropy edge (0.977674)
163840        0x28000         Falling entropy edge (0.613432)
```

# Example




```
ni@nanto:~/4-1/Project/doll$ strings dolls.jpg | tail -n10
6~vz
\3 @
q.*     f%
Og\*8
?41v57
4wed34e
` 'h
pR}tt
base_images/2_c.jpgUT
O`ux
```

# Example

```
ni@nanto:~/4-1/Project/glasses$ binwalk -e PurpleThing.jpeg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 780 x 720, 8-bit/color RGBA, non-interl
aced
41            0x29            Zlib compressed data, best compression
153493        0x25795         PNG image, 802 x 118, 8-bit/color RGBA, non-interl
aced

ni@nanto:~/4-1/Project/glasses$ cd _PurpleThing.jpeg.extracted/
ni@nanto:~/4-1/Project/glasses/_PurpleThing.jpeg.extracted$ ll
total 172
drwxrwxr-x 2 ni ni   4096 সেপ্টে ম্বর  7 01:13 ./
drwxrwxr-x 4 ni ni   4096 সেপ্টে ম্বর  7 01:13 ../
-rw-rw-r-- 1 ni ni      0 সেপ্টে ম্বর  7 01:13 29
-rw-rw-r-- 1 ni ni 164761 সেপ্টে ম্বর  7 01:13 29.zlib
```

# Example

```
ni@nanto:~/4-1/Project/glasses$ binwalk -e --dd=".*" PurpleThing.jpeg
ni@nanto:~/4-1/Project/glasses$ cd _PurpleThing.jpeg.extracted/
ni@nanto:~
total 348
drwxrwxr-x
drwxrwxr-x
-rw-rw-r--
-rw-rw-r--
-rw-rw-r--
-rw-rw-r--
```

100% 25795

# Demo

Now what about this doll?
Does this shape look familiar?

# Demo

```
ni@nanto:~/4-1/Project/doll$ binwalk dolls.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 594 x 1104, 8-bit/color RGBA, non-inter
laced
3226          0xC9A           TIFF image data, big-endian, offset of first image
 directory: 8
272492        0x4286C         Zip archive data, at least v2.0 to extract, compre
ssed size: 378956, uncompressed size: 383938, name: base_images/2_c.jpg
651614        0x9F15E         End of Zip archive, footer length: 22
ni@nanto:~/4-1/Project/doll$ binwalk -e dolls.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 594 x 1104, 8-bit/color RGBA, non-inter
laced
3226          0xC9A           TIFF image data, big-endian, offset of first image
 directory: 8
272492        0x4286C         Zip archive data, at least v2.0 to extract, compre
ssed size: 378956, uncompressed size: 383938, name: base_images/2_c.jpg
651614        0x9F15E         End of Zip archive, footer length: 22
```

# Demo

```
ni@nanto:~/4-1/Project/doll$ cd _dolls.jpg.extracted/
ni@nanto:~/4-1/Project/doll/_dolls.jpg.extracted$ ll
total 384
drwxrwxr-x 3 ni ni   4096 সেপ্টে ম্বর  7 01:33 ./
drwxrwxr-x 3 ni ni   4096 সেপ্টে ম্বর  7 01:33 ../
-rw-rw-r-- 1 ni ni 379144 সেপ্টে ম্বর  7 01:33 4286C.zip
drwxrwxr-x 2 ni ni   4096 সেপ্টে ম্বর  7 01:33 base_images/
ni@nanto:~/4-1/Project/doll/_dolls.jpg.extracted$ cd base_images/
ni@nanto:~/4-1/Project/doll/_dolls.jpg.extracted/base_images$ ll
total 384
drwxrwxr-x 2 ni ni   4096 সেপ্টে ম্বর  7 01:33 ./
drwxrwxr-x 3 ni ni   4096 সেপ্টে ম্বর  7 01:33 ../
-rw-r--r-- 1 ni ni 383938 মা র্চ     16  2021 2_c.jpg
ni@nanto:~/4-1/Project/doll$ binwalk -Me dolls.jpg

Scan Time:     2023-09-07 01:37:51
Target File:   /home/ni/4-1/Project/doll/dolls.jpg
MD5 Checksum:  a014c36d8af2652b08c009fc00bb1597
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 594 x 1104, 8-bit/color RGBA, non-inter
```

# Demo

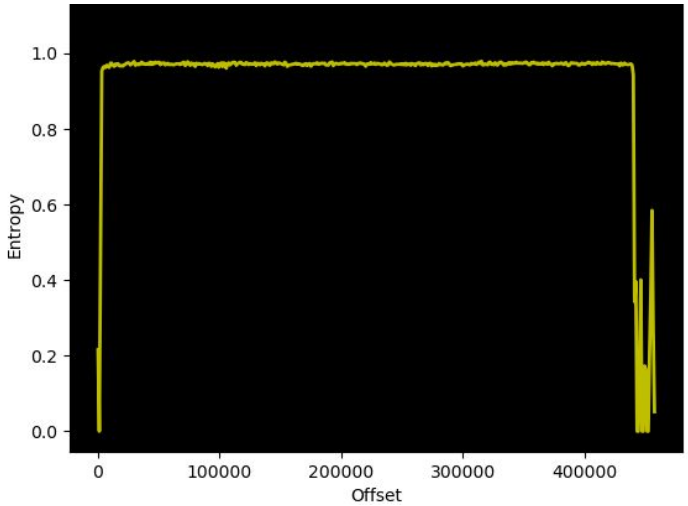
```
ni@nanto:~/4-1/Project/doll$ cd _dolls.jpg-0.extracted/base_images/_2_c.jpg.extr
acted/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted/
ni@nanto:~/4-1/Project/doll/_dolls.jpg-0.extracted/base_images/_2_c.jpg.extracte
d/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted$ ll
total 16
drwxrwxr-x 2 ni ni 4096 সেপ্টে ম্বর  7 01:37 ./
drwxrwxr-x 3 ni ni 4096 সেপ্টে ম্বর  7 01:37 ../
-rw-rw-r-- 1 ni ni  230 সেপ্টে ম্বর  7 01:37 136DA.zip
-rw-r--r-- 1 ni ni   81 মা র্চ     16  2021 flag.txt
ni@nanto:~/4-1/Project/doll/_dolls.jpg-0.extracted/base_images/_2_c.jpg.extracte
d/base_images/_3_c.jpg.extracted/base_images/_4_c.jpg.extracted$ cat flag.txt
picoCTF{336cf6d51c9d9774fd37196c1d7320ff}ni@nanto:~/4-1/Project/doll/_dolls.jpg-
```

91 Presenting

# Entropy

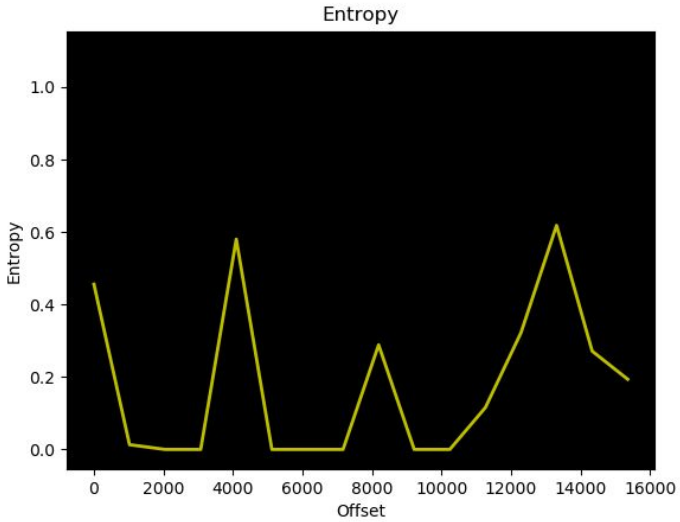
*binwalk -E firmware.bin*

Performs an entropy analysis on the input file(s), prints raw entropy data and generates entropy graphs



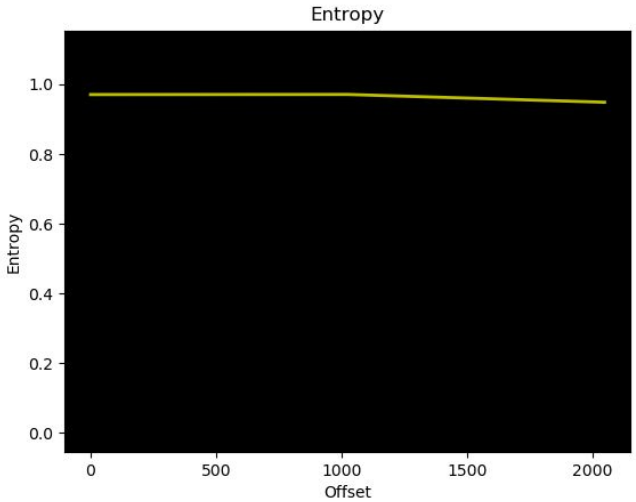
# Entropy

Entropy of a regular file:



# Entropy

Entropy of a zipped file:



# Finding Custom magic signature

*binwalk -m <file.mgc> <firmware.bin*

Search for customize file signature. File signature may look like this:

foobar.mgc

```
0    string    SIG0      SIG0 firmware header,
>4   string    x         description: "%s",
>16  lelong    x         header size: %d,
>20  lelong    x         size: %d,
>24  ledate    x         date: %s
```

More info about Magic Signature

# Finding Custom magic signature Continue…

*binwalk -m <file.mgc> <firmware.bin*

Search for customize file signature. Example:

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -m foobar.mgc magicFile
.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             SIG0 firmware header, description: "This is a samp
le firmware header", header size: 1701605485, size: 1919510048, date: 2030-10-23
 12:49:49
```

More info about [Magic Signature]

# Signatures that match the specified include filter

*binwalk -y 'filesystem' firmware.bin #* only search for filesystem signatures

Useful when searching only for specific signatures or types of signature

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -y 'filesystem' Firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
760464        0xB9A90         Squashfs filesystem, little endian, non-standard signature,
 version 3.0, size: 2769153 bytes, 539 inodes, blocksize: 65536 bytes, created: 2016-01-0
8 05:58:38

ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$
```

# Excludes signatures that match the specified exclude filter

*binwalk -x 'mach-o' -x '^hp' firmware.bin* # exclude HP calculator and OSX mach-o signatures

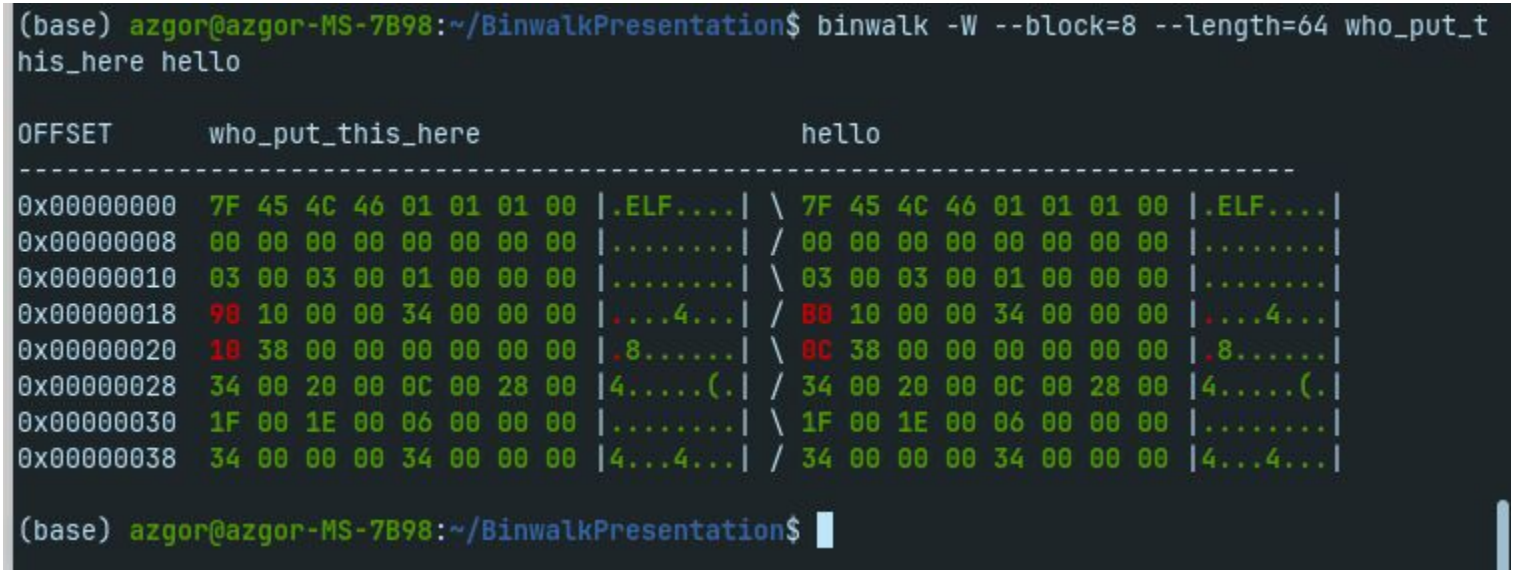
Useful for excluding unneeded or uninteresting results

```
ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -x foobar.mgc exclude.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1280 x 851, 8-bit/color RGBA, non-interlaced
54            0x36            Zlib compressed data, best compression
442148        0x6BF24         ELF, 32-bit LSB shared object, Intel 80386, version 1 (SYSV
)

ruhul@ruhul-Inspiron-3442:~/BinwalkPresentation$ binwalk -m foobar.mgc exclude.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
457740        0x6FC0C         SIG0 firmware header, description: "This is a sample firmwa
re header", header size: 1701605485, size: 1919510048, date: 2030-10-23 12:49:49
```

# Hexdump

Command:binwalk -W --block=8 --length=64 firmware1.bin firmware2.bin firmware3.bin

Performs a hex dump of the input file(s) and color-codes bytes



# Hexdump continue…

- -G =>Only display lines that contain green bytes
- -i  =>Only display lines that contain red bytes

# Demo 03

Cool Cat

# Demo 04

Firmware

# Disables "smart" signature matching.

Command: binwalk -b firmware.bin

Useful when smart signature keywords in false positive signatures cause other valid signatures to be missed