# Compression / Archive

## ZIP

```
$ unzip file.zip
```

50 B4 … | PK …

## GZIP

```
$ gunzip file.gz
$ gzip -d file.gz
```

1F 8B 08 … | .<. …

## RAR

```
$ unrar e file.rar
```

52 61 72 21 … | RAR! …

## 7z

```
$ 7z e file.7z
```

37 7A BC AF 27 … | 7z¼¯ …

## tar

```
$ tar -xvf file.tar
```

75 73 74 61 72 … | ustar …

## tar.z (compressed)

```
$ tar -zxvf file.tar.z
```

1F 9D … LZW

1F A0 … LZH

## CPIO

```
$ cpio -idv < file.cpio
```

C7 71 … → *oct* 070707

30 37 30 37 30 31 32 37 … | 07070 1 2 7 …

## zlib

```
$ zlib-flate -uncompress < in.z > out.bin
```

| *No preset dict.* | | *With preset dict.* |
|---|---|---|
| 78 01 5E 9C DA … | No compr.<br>Best speed<br>Default<br>Best compr. | 78 20 7D BB F9 … |

## LZMA

```
$ lzma -d file.lzma
```

5D 00 00 … | ]. …

## LZFSE

```
$ lzfse -decode -i file.z -o file
```

62 76 78 32 … | bvx2 …

# PE (.exe)

4D 5A … | MZ …

# ELF

7F 45 4C 46 … | .ELF …

# MachO

Universal: CA FE BA BE …

32/64-bit: CE CF FA ED FE …

*May be vice versa*

# Dalvik Executable

64 65 78 0A … | dex. …

*LIEF library to parse executable formats*

```
01  import lief
02
03  pe = lief.parse("explorer.exe")
04  elf = lief.parse("libc.so")
```

# Python bytecode (.pyc)

xx xx 0D 0A … | xx .. …

Depends on the Python's version

# WebAssembly

6D 73 61 00 … | msa. …

# PDF

25 50 44 46 … | %PDF …

# DjVu

41 54 26 54 … | AT&T …

# ARM-code

Repeating Ex-byte every 4 bytes

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 24 | C0 | 9F | **E5** | 00 | B0 | A0 | **E3** | 04 | 10 | 9D | **E4** | 0D | 20 | A0 | **E1** |
| 04 | 20 | 2D | **E5** | 04 | 00 | 2D | **E5** | 10 | 00 | 9F | **E5** | 10 | 30 | 9F | **E5** |
| 04 | C0 | 2D | **E5** | A5 | 26 | 0B | **EB** | 7C | 42 | 0B | **EB** | 30 | 1E | 2D | 00 |
| B4 | EC | 02 | 00 | 98 | 1D | 2D | 00 | 04 | A0 | 2D | **E5** | 20 | A0 | 9F | **E5** |
| 20 | 30 | 9F | **E5** | 0A | A0 | 8F | **E0** | 03 | 20 | 9A | **E7** | 00 | 00 | 52 | **E3** |

NOP instruction: `00 00 A0 E1` ARM-mode; `C0 46` THUMB-mode

# U-Boot / uImage

27 05 19 56 … | '..V …

# S7-PLC block

70 70 … | pp …

# Flash-memory

Flash

0×555
0×AAA
0×2AA

# DER encoded

(X.509 cert)

30 82 … | 0, …

# Random

0×343FD
0×269EC3

# Hash functions

MD4 / MD5 / SHA1

0×67452301
0×EFCDAB89
0×98BADCFE
0×10325476

# Cryptography

Rijndael (AES) S-box

63 7C 77 7B
F2 6B 6F C5
30 01 67 2B
FE D7 AB 76
...

# MS Office Document

Old 97-2003 format (.doc)

D0 CF 11 E0 … | ÐÏ.à …

Reverse Engineering Magics Cheatsheet

Pavel Rusanov