Basic - 3

2019/10/22

Bamboofox

To Do List

0x01 Basis of Forensics

0x02 Recall C, assembly, gdb

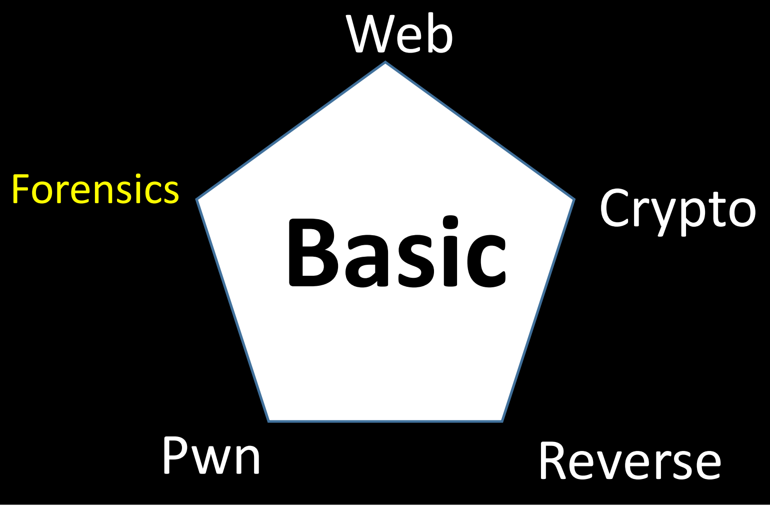
0x03 Basis of Pwn

Bamboofox

0x01 Basis of Forensics

Bamboofox

0x02. Talking About CTF



Web

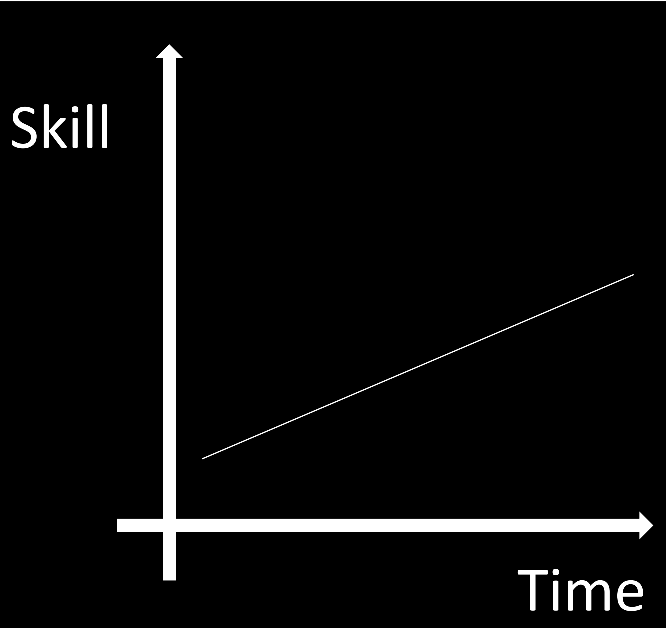
Forensics

Basic

Crypto

Pwn

Reverse



Forensics:

1. Usually given a picture, sound file, or others, you have to find the flag hidden.

2. The basic knowledge are various type of picture(PNG, JPG……), sound file(MP3, WAV……), analyzing Packet ……

Bamboofox

0x01 Basis of Forensics

What is Steganography (圖片隱碼術) ?

Every method that can hide messages or script is called steganography.

In cyber security, steganography is a way for hacker to do something bad.

ex. https://blog.trendmicro.com/trendlabs-security-intelligence/sunsets-and-cats-can-be-hazardous-to-your-online-bank-account/

Do It Yourself !!

http

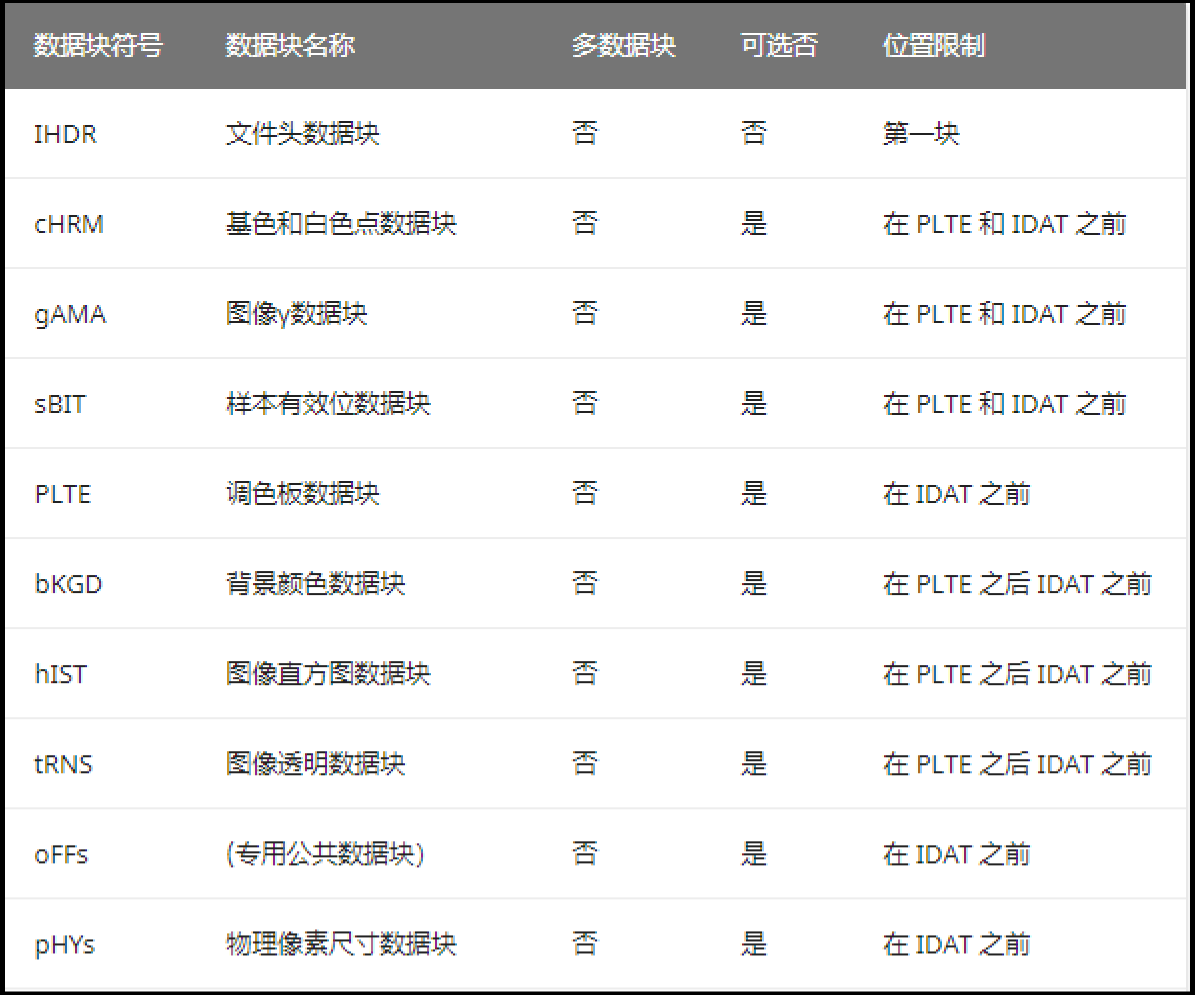
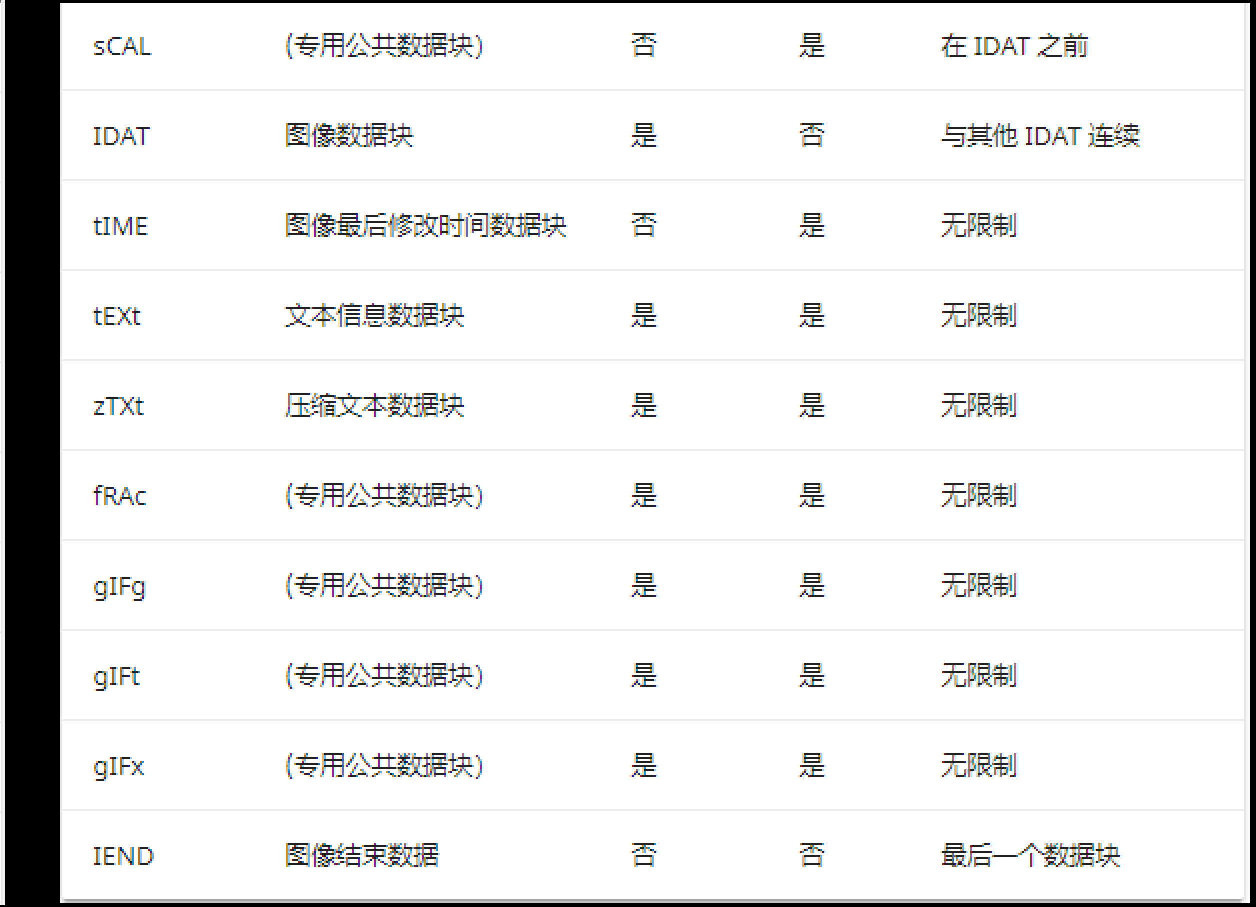
0x01 Basis of Forensics

Take png as example

png : a kind of image file

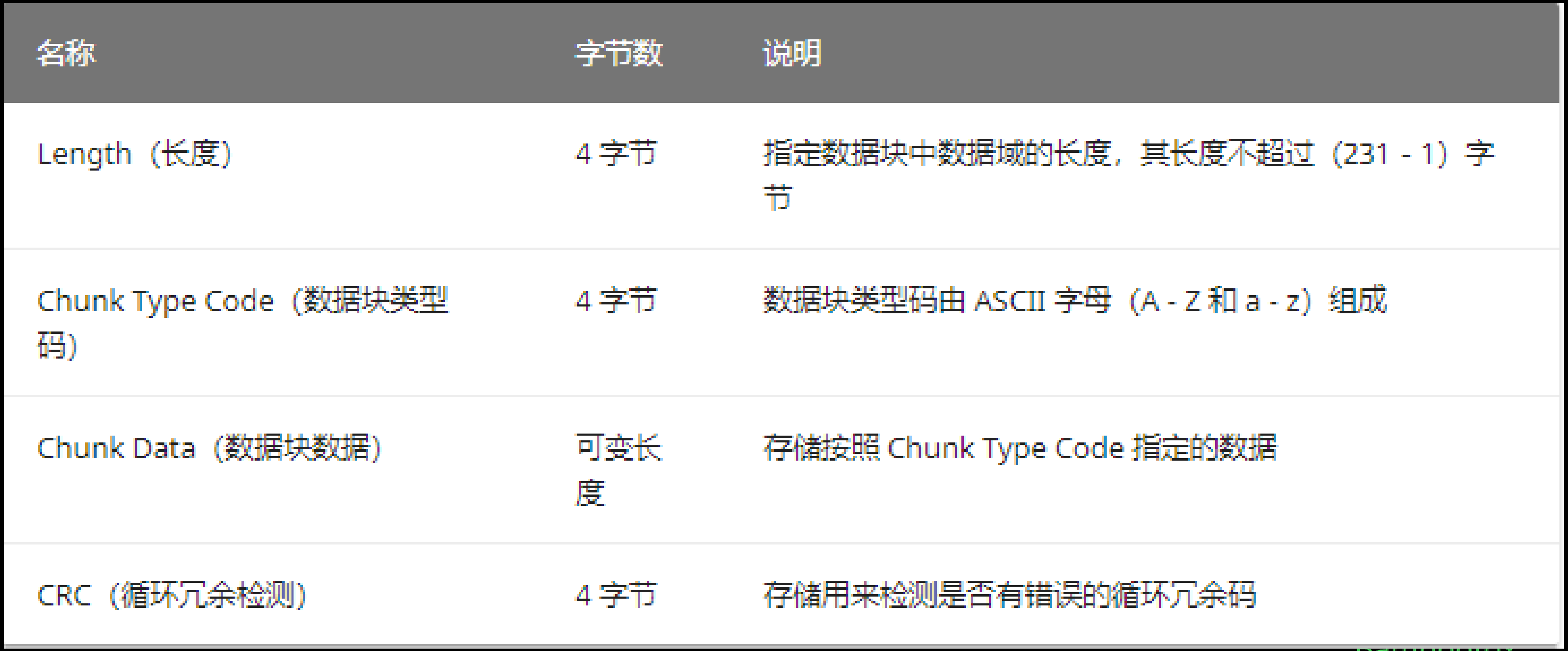
It contains file header + data chunks, where the file header is 89 50 4E 47 0D 0A 1A 0A

0x01 Basis of Forensics

数据块符号	数据块名称	多数据块	可选否	位置限制
IHDR	文件头数据块	否	否	第一块
cHRM	基色和白色点数据块	否	是	在 PLTE 和 IDAT 之前
gAMA	图像γ数据块	否	是	在 PLTE 和 IDAT 之前
sBIT	样本有效位数据块	否	是	在 PLTE 和 IDAT 之前
PLTE	调色板数据块	否	是	在 IDAT 之前
bKGD	背景颜色数据块	否	是	在 PLTE 之后 IDAT 之前
hIST	图像直方图数据块	否	是	在 PLTE 之后 IDAT 之前
tRNS	图像透明数据块	否	是	在 PLTE 之后 IDAT 之前
oFFs	(专用公共数据块)	否	是	在 IDAT 之前
pHYs	物理像素尺寸数据块	否	是	在 IDAT 之前
sCAL	(专用公共数据块)	否	是	在 IDAT 之前
IDAT	图像数据块	是	否	与其他 IDAT 连续
tIME	图像最后修改时间数据块	否	是	无限制
tEXt	文本信息数据块	是	是	无限制
zTXt	压缩文本数据块	是	是	无限制
fRAc	(专用公共数据块)	是	是	无限制
gIFg	(专用公共数据块)	是	是	无限制
gIFt	(专用公共数据块)	是	是	无限制
gIFx	(专用公共数据块)	是	是	无限制
IEND	图像结束数据	否	否	最后一个数据块

0x01 Basis of Forensics



名称	字节数	说明
Length（长度）	4 字节	指定数据块中数据域的长度，其长度不超过（231 - 1）字节
Chunk Type Code（数据块类型码）	4 字节	数据块类型码由 ASCII 字母（A - Z 和 a - z）组成
Chunk Data（数据块数据）	可变长度	存储按照 Chunk Type Code 指定的数据
CRC（循环冗余检测）	4 字节	存储用来检测是否有错误的循环冗余码

0x01 Basis of Forensics

IHDR

(4 bytes) Length : 00 00 00 0D

(4 bytes) Chunk Type Code : 49 48 44 52 (IHDR)

(13 bytes) Chunk Data : length + width + 5 bytes

(4 bytes) CRC : crc32(Length + Chunk Type code + Chunk Data)

0x01 Basis of Forensics

PLTE(palette chunk) : regarding to indexed-color image

IDAT(image data chunk) : contains all of the image's compressed pixel data

IEND(image trailer chunk) : to tell that the chunks are over

length : 00 00 00 00

Chunk type code : 46 45 4E 44

CRC : AE 42 60 82

Do It Yourself !!

http

Bamboofox

0x01 Basis of Forensics

Zip : A format of compressed file

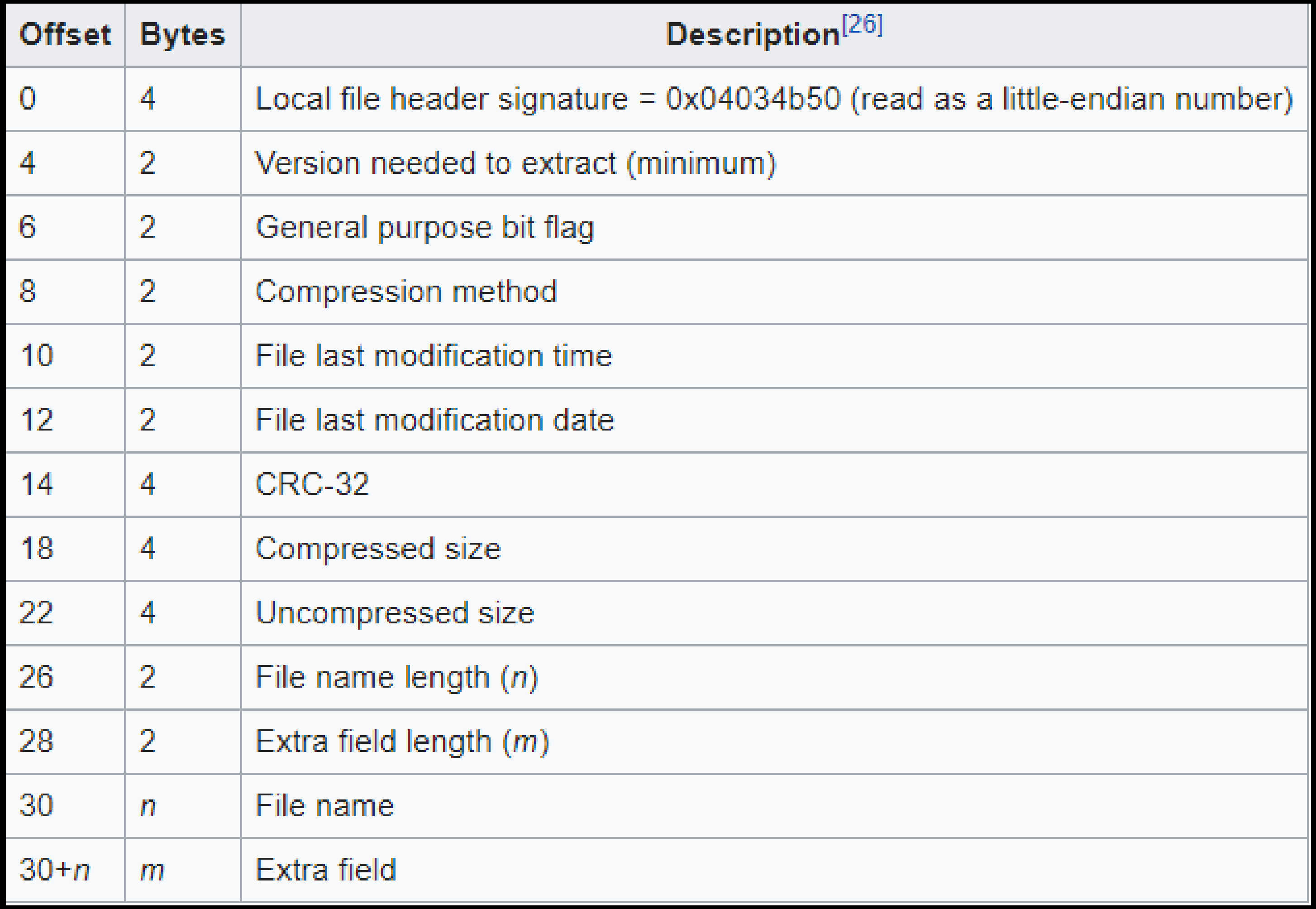
It consists of four parts, which are Local file header, Data descriptor, Central directory file header, and End of central directory record.

Part	Signature
Local file header	50 4b 03 04
Data descriptor	50 4b 01 02
Central directory file header	50 4b 07 08
End of central directory record	50 4b 05 06

Bamboofox

0x01 Basis of Forensics

Local file header

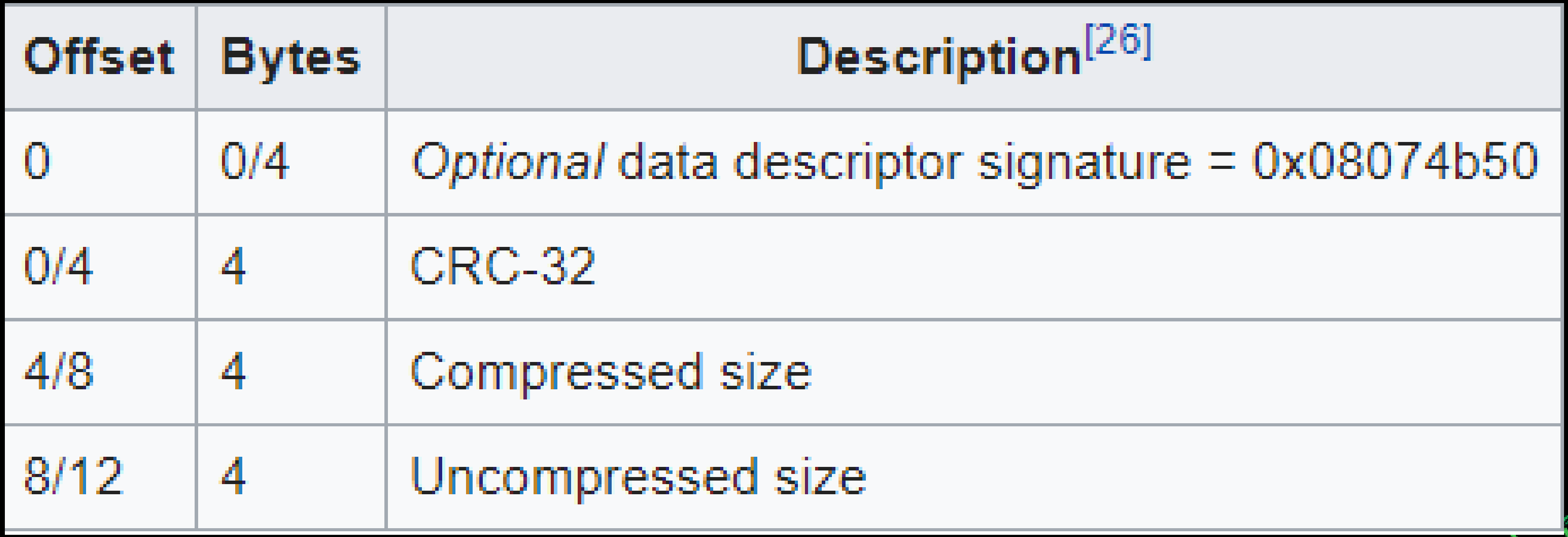


Offset	Bytes	Description[26]
0	4	Local file header signature = 0x04034b50 (read as a little-endian number)
4	2	Version needed to extract (minimum)
6	2	General purpose bit flag
8	2	Compression method
10	2	File last modification time
12	2	File last modification date
14	4	CRC-32
18	4	Compressed size
22	4	Uncompressed size
26	2	File name length (*n*)
28	2	Extra field length (*m*)
30	*n*	File name
30+*n*	*m*	Extra field

Bamboofox

0x01 Basis of Forensics

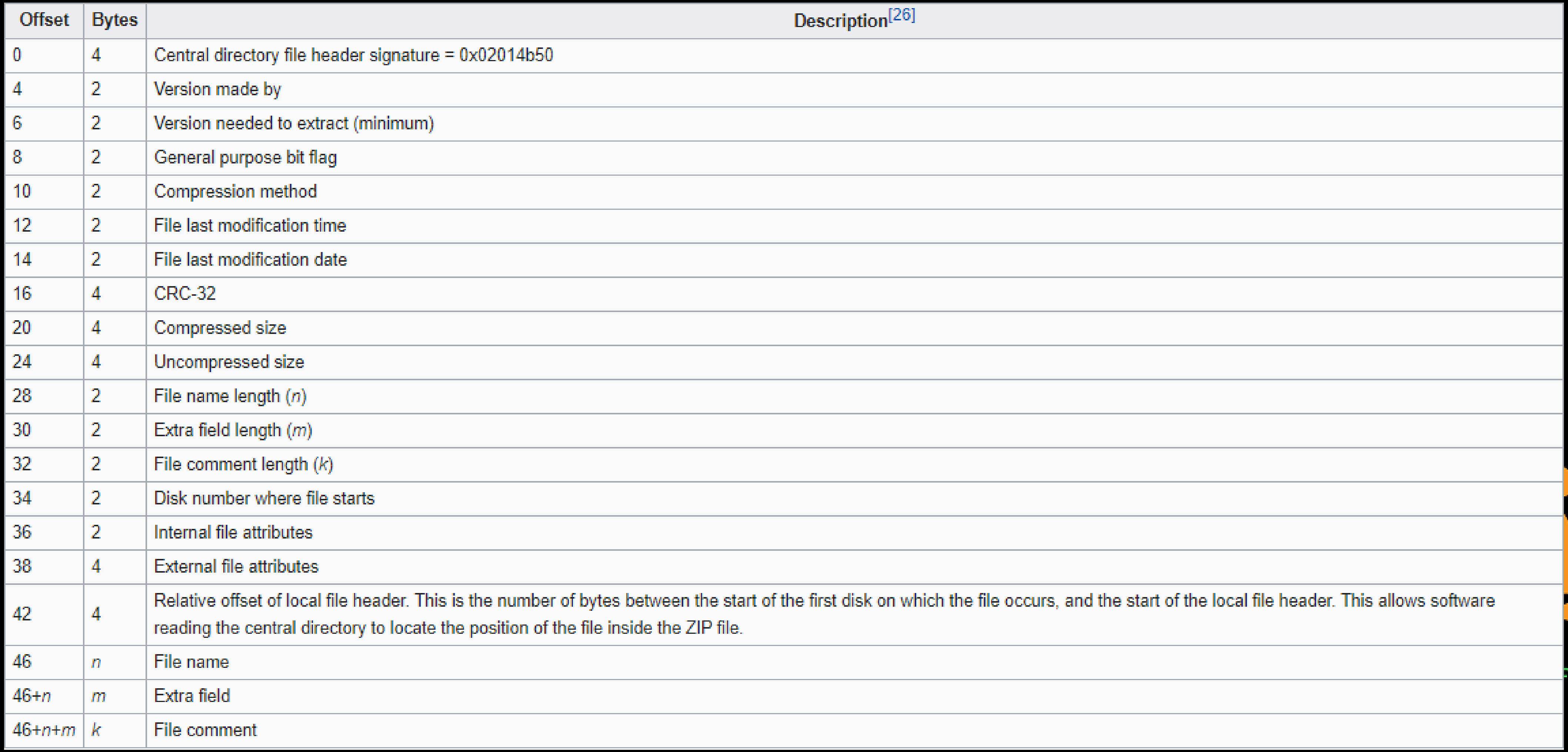
Data descriptor



Offset	Bytes	Description[26]
0	0/4	*Optional* data descriptor signature = 0x08074b50
0/4	4	CRC-32
4/8	4	Compressed size
8/12	4	Uncompressed size

0x01 Basis of Forensics

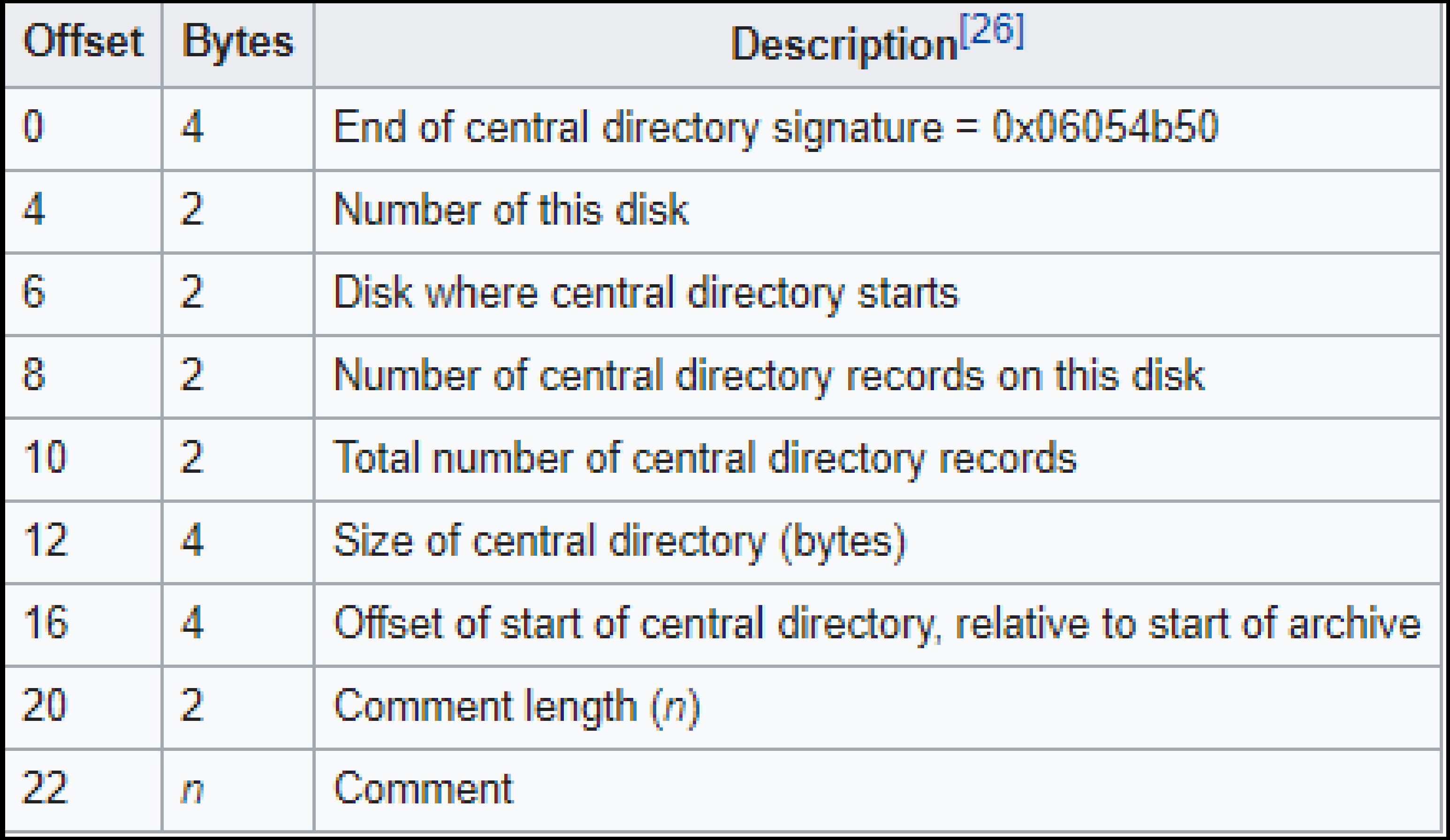
Central directory file header



Offset	Bytes	Description[26]
0	4	Central directory file header signature = 0x02014b50
4	2	Version made by
6	2	Version needed to extract (minimum)
8	2	General purpose bit flag
10	2	Compression method
12	2	File last modification time
14	2	File last modification date
16	4	CRC-32
20	4	Compressed size
24	4	Uncompressed size
28	2	File name length (*n*)
30	2	Extra field length (*m*)
32	2	File comment length (*k*)
34	2	Disk number where file starts
36	2	Internal file attributes
38	4	External file attributes
42	4	Relative offset of local file header. This is the number of bytes between the start of the first disk on which the file occurs, and the start of the local file header. This allows software reading the central directory to locate the position of the file inside the ZIP file.
46	*n*	File name
46+*n*	*m*	Extra field
46+*n*+*m*	*k*	File comment

0x01 Basis of Forensics

End of central directory record



Offset	Bytes	Description[26]
0	4	End of central directory signature = 0x06054b50
4	2	Number of this disk
6	2	Disk where central directory starts
8	2	Number of central directory records on this disk
10	2	Total number of central directory records
12	4	Size of central directory (bytes)
16	4	Offset of start of central directory, relative to start of archive
20	2	Comment length (*n*)
22	*n*	Comment

Bamboofox

Do It Yourself !!

http

0x01 Basis of Forensics

Other examples : pdf, sound files(wav, mp3), ……

pdf forensics tools : pdf2txt, pdftohtml, pdf_parser,

Sound files forensics tools : Sonic Visualiser, ……

Bamboofox

0x02 Recall C, assembly, gdb

Bamboofox

0x03 Basis of Pwn

Bamboofox