intro to forensics

by @a-yun

file formats

what is a file anyway?

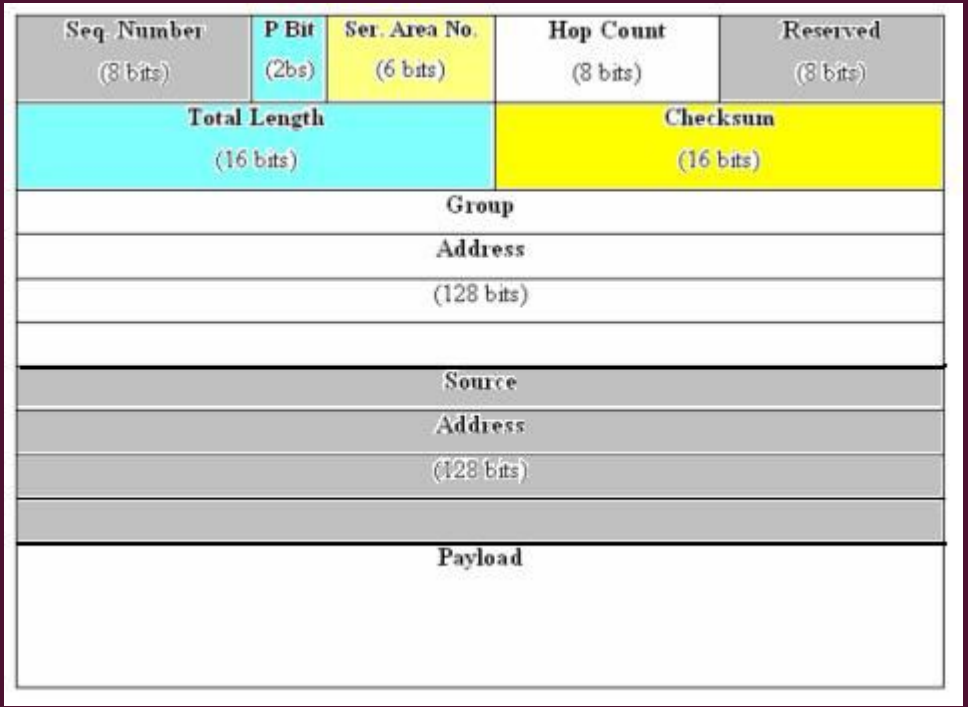
what is a file anyway?

files are just collections of 1’s and 0’s (binary data) stored on your hard drive

files have many different formats (document, image, zip, executable)

programs identify and interact with files based on their metadata

example (jpg)


Seq. Number
(8 bits)
P Bit
(2bs)
Ser. Area No.
(6 bits)
Hop Count
(8 bits)
Reserved
(8 bits)
Total Length
(16 bits)
Checksum
(16 bits)
Group
Address
(128 bits)
Source
Address
(128 bits)
Payload

common file types

ascii text

image (jpg, png, bmp)

audio (wav, mp3)

archive (zip, rar)

MS Office (Word, Excel)

pdf

executable

ascii text

pretty boring

just open it in vim or your favorite text editor

images - png

widely used image format with lossless compression

magic number: 89 50 4e 47 0d 0a 1a 0a

followed by sequence of chunks (IHDR and IEND)

images - bmp

bitmap image file

magic number: 42 4D

header stores file size

images - jpg

lossy compression for images usually used by cameras

magic number: FF D8 FF

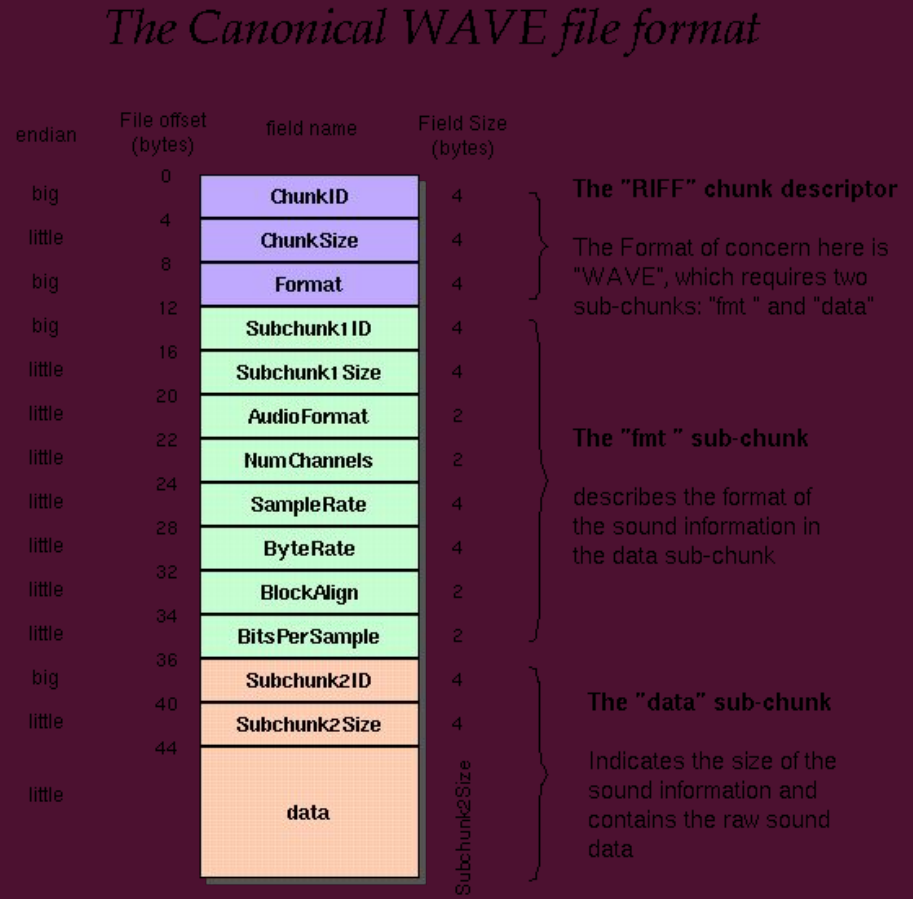
trailer: FF D9

audio - wav

stores raw and typically uncompressed audio bitstream

header: 52 49 46 46

trailer: FF D9



archive - zip

lossless data compression

can be password secured

magic number: 50 4B 03 04, 50 4B 05 06, or 50 4B 07 08 (all start with PK)

MS Office

everything is just a zip file lol

contains XML (marked up files) and assets

executable

varies per operating systems

consists ELF header, program header, .text and .data sections

look at the binary presentation

tools

tools

file

hexdump

hex editor (Bless)

Exiftool

dd

john the ripper

file

Unix program for determining file type

useful for renamed files or finding metadata

DEMO!

hexdump and hex editors

binary (0-1) can also be represented as hexadecimal (0-9, A-F)

command line tools like hexdump and editors like Bless help you read and modify raw file data

DEMO!

exiftool

some media file types (jpep, tiff, wav) support additional metadata tags

information can include: date/time, camera details, location

DEMO!

dd

Unix utility for manipulating files

useful for file carving, among other things

DEMO!

john the ripper

password cracking tool (dictionary attack, brute force, and others)

can be used on /etc/passwd (encrypted password file) or password protected archives (rar/zip, with jumbo utilities)

PLEASE COMPILE BEFOREHAND

DEMO!

common problems

common problems

changed file type

corrupted file header

file carving and hidden files within pdfs/archives

steganography (concealing messages in images/audio)

encrypted or corrupted archives

memory dump

filesystems

resources

https://trailofbits.github.io/ctf/forensics/

https://asecuritysite.com/forensics/magic

https://en.wikipedia.org/wiki/List_of_file_signatures