forensics, files, and stuff

by @a-yun, some slides stolen from @alex-bellon

file formats

what is a file anyway?

what is a file anyway?

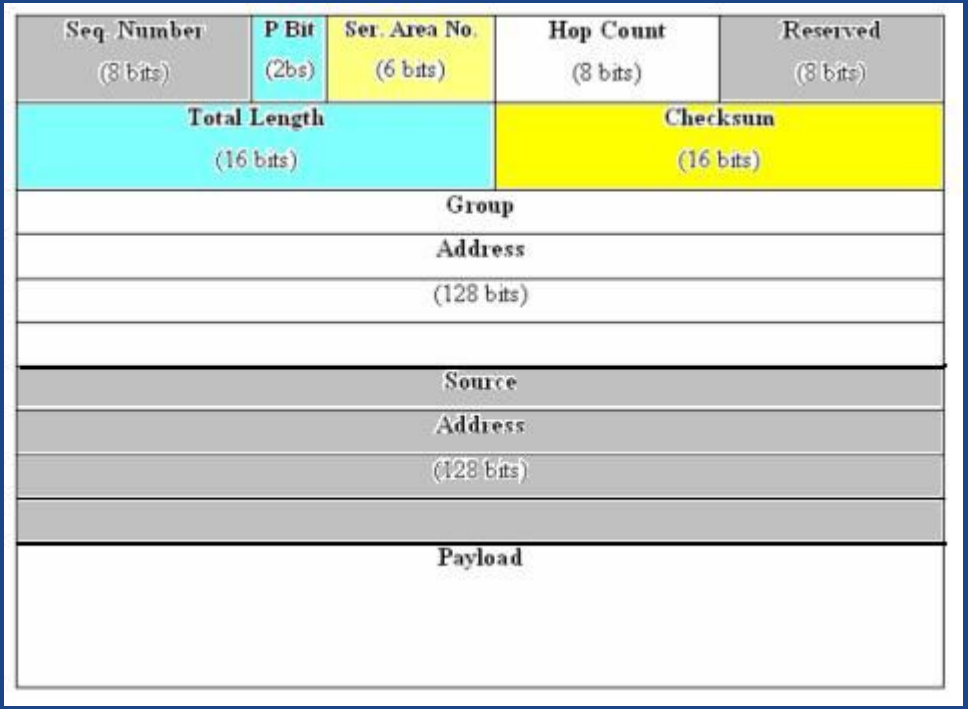
files are just collections of 1’s and 0’s (binary data) stored on your hard drive

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

programs identify and interact with files based on their metadata

file types often determined by “magic numbers” in the header

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) -
XML + zip file

pdf

executable - see binary talk

tools

tools

strings

dd

binwalk

file

hexdump / xxd / hex editor (Bless)

Exiftool

john the ripper

strings <file> - shows all strings in that file

xxd <file> - shows a hexdump of that file

binwalk <file> - find embedded files and executable code in binaries

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

dd

Unix utility for manipulating files

useful for file carving, among other things

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

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

steganography

by @alex-bellon

crypto - hiding information

steganography - hiding information AND hiding the fact that you hid information

usually done in audio and image files

least significant bits

one common tactic (with images) is to use least significant bit (or LSB)

embed the message in the least *x* significant bits of the image

the more bits you use, the more obvious it is that you are hiding a message

	red	green	blue
	10001001	11001111	10001001
	10001000	11001110	10001000
	10001000	11001111	10001010

original

steg

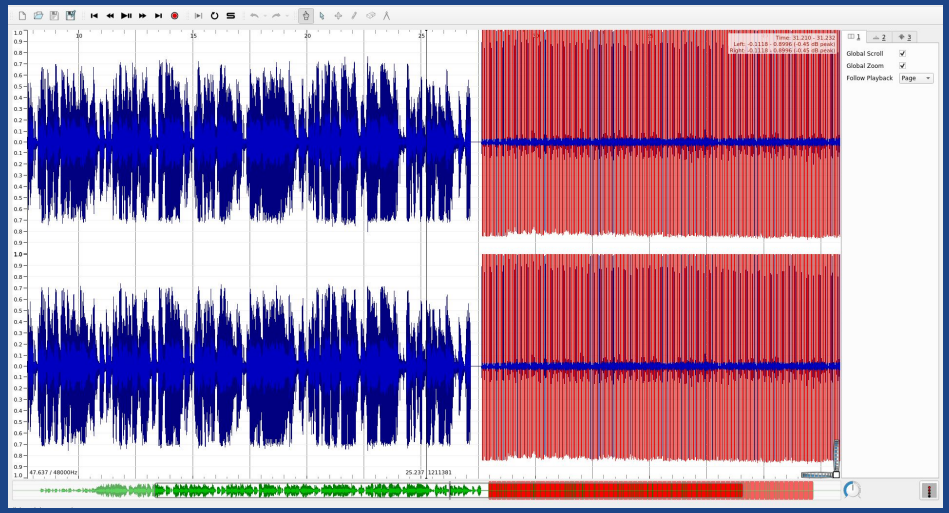
demo:

https://www.incoherency.co.uk/image-steganography/#unhide

spectrograms

used to hide text or images in audio files that can only be seen by looking at the spectrogram

you can use a tool like Sonic Visualizer or Audacity (both work on win, *nix, mac) to view the spectrogram



waveform (default)

pane > add spectrogram

spectrogram

resources

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

https://asecuritysite.com/forensics/magic

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