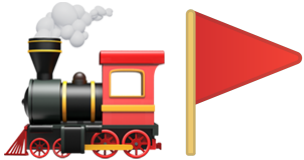
Forensics: a CTF handbook

Introduction to the forensics category of capture the flags

DaVinciCode

30/11/2021



Forensics: a CTF handbook

- Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. (litteraly wikipedia)
- It's finding stuff hidden in files during CTF. (me)
- A ne pas confondre avec la stégano :v
- Ca se fait sous windows c:

Intro

First of all: low hanging fruits

```
# Get a better idea of the file:
file $(file)
strings $(file)
exiftool $(file)
grep
binwalk --dd='.*' $(file)
```

Common challenges

Archives

- File carving
- Filesystem/Images and logs

Specific file

- PCAP
- PDF
- Corrupted files
- Memory forensics
- Honorable mentions

File carving

Finding info from a dd image, a system dump, a .EO1

- FTK Imager
- Autopsy
- FindAES

Example: *ECW2020, Lord of War*

Filesystem/Images and Log analysis

Windows:

- EVTX parsers, MFT explorer, File cache parsers, etc... => https://ericzimmerman.github.io

Example: ECW2021 Response Team 3

Linux:

- grep?

Example: ECW2021 Response Team 1

PCAP

Ressources

- Scapy
- Wireshark
- NetworkMiner
- Many others!

MS Docs

What are we tring to do, what are we trying to find?

- Deobfuscate VBA macros
- Hidden text, media in unzipped

Ressources

- Oletools: VBA analysis
- ViperMonkey: VBA emulation+deobfuscation+analysis

PDF Analysis

Ressources

- Corkami by Ange Albertini
- qpdf
- peepdf
- Pdf-parser, only on kali

Corrupted files

Corrupted PNG

```
pngcheck $image
PCRT $image
```

PNG Check & Repair Tool or Pixrecovery

Memory forensics

Volatility:

```
# Get basic info for a dump, including recommended profiles.
volatility -f $DUMP imageinfo

# For this example, let's use the Win7SP0x64 profile
volatility -f $DUMP --profile=Win7SP0x64 $(plugin command)
```

Windows memory analysis

Some useful plugins:

```
# View processes; see also pslist and psscan.
volatility -f $DUMP --profile=Win7SP0x64 pstree

# Dump the memory of a specific process.
volatility -f $DUMP --profile=Win7SP0x64 memdump -p <PID> -D dump/

# View commands run in the command prompt.
volatility -f $DUMP --profile=Win7SP0x64 connections
```

Windows memory analysis

Some useful plugins:

```
# View network connections; use `consoles` to also get command prompt output.
volatility -f $DUMP --profile=Win7SP0x64 cmdscan

# View environment variables.
volatility -f $DUMP --profile=Win7SP0x64 envars

# View internet explorer history.
volatility -f $DUMP --profile=Win7SP0x64 iehistory
```

Linux dumps

Wait, what do I do if it's not a windows memory dump?

Linux dumps

Short answer, you're f*cked

Linux dumps

Long answer, it's gonna be longer, be there's options

Linux dumps

```
grep -ai "linux version" $DUMP | uniq
grep -ai "Linux release" $DUMP | uniq
grep -ai "BOOT_IMAGE" $DUMP | uniq
grep -ai "distrib_description=" $DUMP | uniq
```

Generate a profile: https://illuad.fr/2020/11/26/writeup-dga-ctf-bwing.html

Honorable mentions

To go deeper... Forensics is a vast subject!

Everything can be searched deeped down, everything is a file, and everything is bruteforceable.

- Mozilla passwords
- BMCs
- Ducky bin
- Android patterns
- Keepass