

File analysis and forensics

What is file forensics?

Often in CTFs some challenges give us an anonymous file, we need to understand how to use it and gather as much information possible about it

Sometimes the file can be corrupted or can have the extension changed, so we need to look at it directly at byte level

Sometimes steganalysis techniques required to recover the flag

Tools for file analysis

Linux is already bundled with some useful analysis tools.

Covered tools:

- **file**
- **strings**

file

Detects most file types reading both file extension and header bytes

For binary executables gives also other useful information about the architecture and compilation details

file <filename>

strings

Performs a scan of the given file looking for long sequences of printable characters

- Can be configured to look for sequences with a minimum given length
- Often combined with other tools like **grep** in order to filter the output

Useful to detect strings written directly in the code of compiled binaries, like password or secret keys

```
strings <filename> [-n <min_length>]
```

binwalk

Swiss army knife for file analysis.

- Performs scan of binary images looking for files or executable code hidden inside them. The scan is based mainly upon ***magic numbers***
- Capable of extracting automatically all detected files *[option -e]*
- Allows to print the hexdump of a file *[option -W]*
- Can be used as a quick view binary disassembler *[option -Y]*

Not already bundled in many linux distributions

Install (on debian/ubuntu):

```
15:33:07 in ~  
⚡ sudo apt install binwalk
```