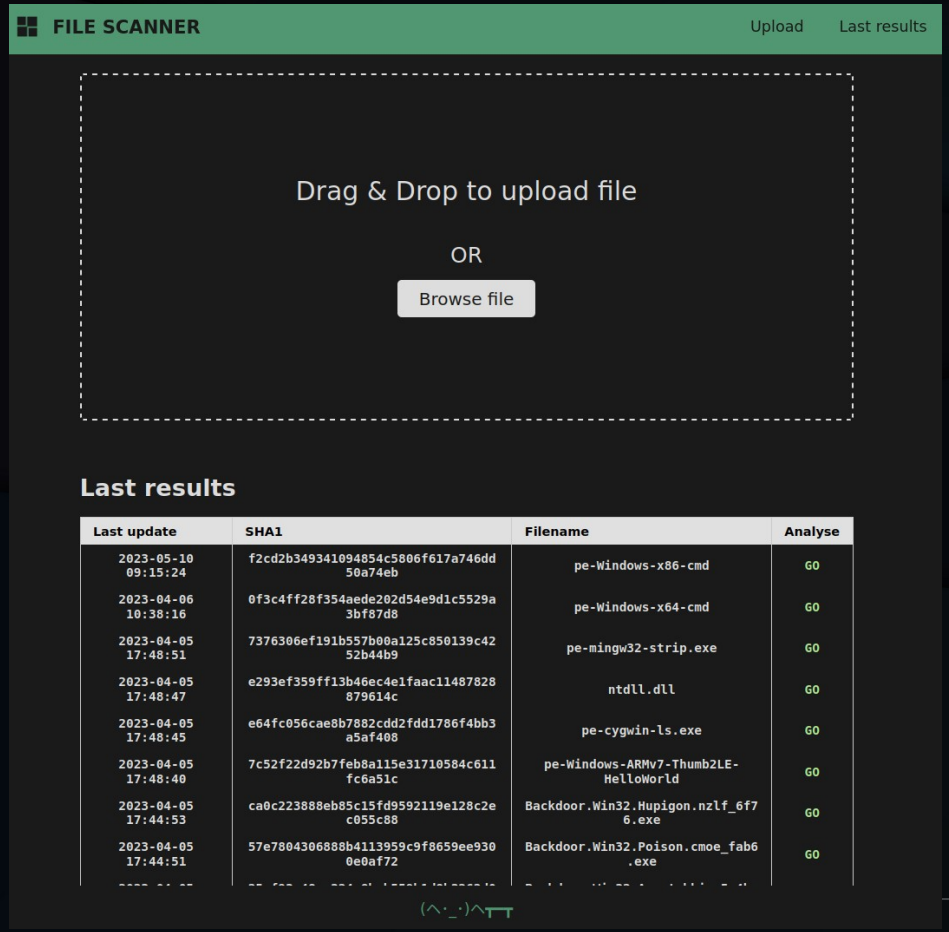
# scanner

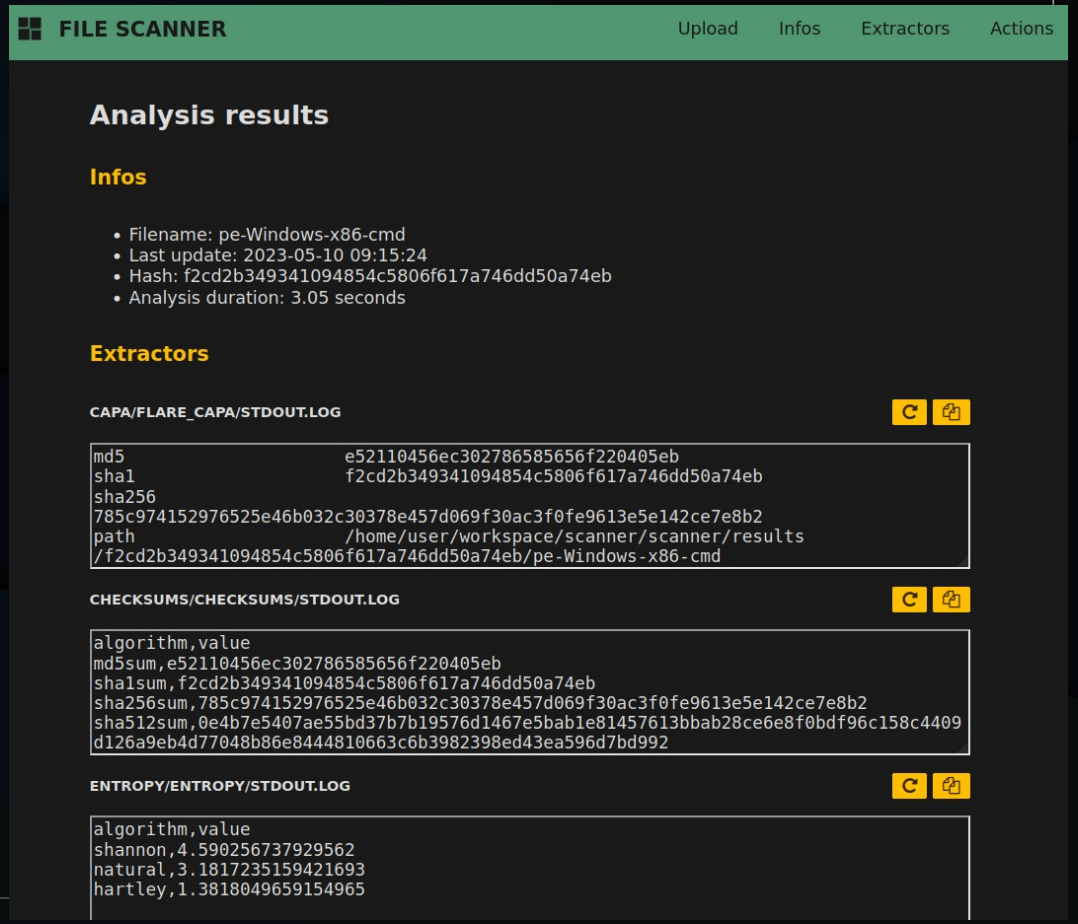
PE static analysis platform

# PE static analysis platform

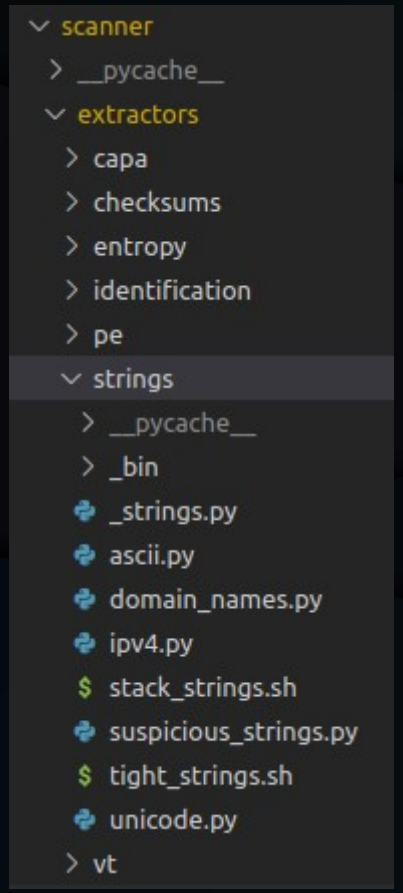
- CLI && GUI
- Plugins
- Analysis database
- Developer oriented

# Show me the ~~code~~ interface



# Extractors




- Drop your exec
- Categorize with folders
- Write to stdout / stderr
- Prefix deps with _

# Extractors full list

| | |
|---|---|
| capa | capa -vv |
| checksums | Md5, sha1, sha256 |
| entropy | Calcul shannon, natural, hartley |
| identification | file (1) |
| pe/authenticode | Authenticode display |
| pe/debug | PE debug infos (e.g. pdb path) |
| pe/exports | Exports listing |
| pe/features | Has suspicious imphash, has native subsystem, ... |
| pe/header | PE header infos (addr of entrypoint, size of code, ...) |
| pe/imports_hash | Imports hash computation (pefile / lief based) |
| pe/imports | Imports listing |
| pe/packers | Packer detection |

| | |
|---|---|
| pe/resources | Rsrc listing |
| pe/rich_header | rich header infos (vs2022 up to date!) |
| pe/sections | Pe section infos |
| pe/stamps | PE timestamps |
| pe/subsystem | PE subsystem output |
| pe/suspicious_imports | Suspicious imports listing (e.g. antidebug) |
| pe/suspicious_modules | Suspicious modules listing (e.g. libraries) |
| pe/suspicious_sections | Suspicious sections listing (e.g. packers) |
| strings/ascii | Ascii strings listing |
| strings/domain_names | Domain names listing |
| strings/ipv4 | Ipv4 listing |

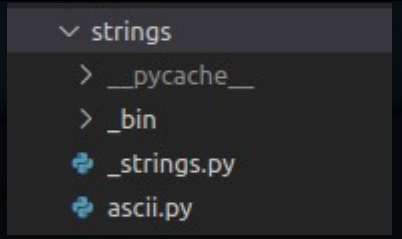
| | |
|---|---|
| strings/stack_strings | Stack strings listing |
| strings/suspicious_strings | Suspicious strings (e.g. cmd.exe) |
| strings/tight_strings | Tight strings listing |
| strings/unicode | Utf16le strings listing |
| vt/by_hash | VT hash report download |

# Example

## Write extractor ...

```python
#!/u

impo

from _strings import get_description, get_strings

if __name__ == "__main__":
    """/usr/bin/strings -es $1"""
    if (
        strings_infos := get_strings(
            sys.argv[1], ascii=True, unicode=False, offsets=True
        )
    ) == []:
        sys.exit(1)

    print("offset,string,description")
    for offset, content in strings_infos:
        string = content.decode("ascii")
        print(f"{offset:#08x}", string, get_description(string), sep=",")

    sys.exit(0)
```

## ... under extractors/ ...




## ... run the scanner ...

```
user@user:~/workspace/scanner$ poetry run scanner cli --file files/pe-Windows-x64-cmd
Handle files/pe-Windows-x64-cmd
pe-Windows-x64-cmd -- 0f3c4ff28f354aede202d54e9d1c5529a3bf87d8
[OK] Process ascii.py ran in 0.12 second(s)
[OK] Process unicode.py ran in 0.13 second(s)
[OK] Process ipv4.py ran in 0.13 second(s)
[OK] Process file.sh ran in 0.01 second(s)
[OK] Process checksums.sh ran in 0.05 second(s)
[OK] Process imports_hash.py ran in 0.23 second(s)
[OK] Process suspicious_strings.py ran in 0.4 second(s)
[OK] Process domain_names.py ran in 0.45 second(s)
[KO] Process packers.py ran in 0.33 second(s)
[OK] Process sections.py ran in 0.3 second(s)
[KO] Process suspicious_modules.py ran in 0.28 second(s)
[KO] Process suspicious_sections.py ran in 0.28 second(s)
[KO] Process exports.py ran in 0.24 second(s)
[OK] Process rich_header.py ran in 0.25 second(s)
[OK] Process subsystem.py ran in 0.24 second(s)
[KO] Process suspicious_imports.py ran in 0.28 second(s)
[OK] Process stamps.py ran in 0.49 second(s)
[OK] Process resources.py ran in 0.31 second(s)
[OK] Process authenticode.py ran in 0.25 second(s)
[OK] Process features.py ran in 2.87 second(s)
[OK] Process tight_strings.sh ran in 45.45 second(s)
[OK] Process stack_strings.sh ran in 48.69 second(s)
[OK] Process flare_capa.py ran in 68.91 second(s)
Extractors ran in 69.06 second(s) for 0f3c4ff28f354aede202d54e9d1c5529a3bf87d8
```

## ... collect output.

**STRINGS/ASCII/STDOUT.LOG**

```
offset,string,description
0x00004d,!This program cannot be run in DOS mode.,string in dos stub
0x0001d0,.text,
0x0001f7,`.data,
0x000220,.rsrc,
0x000247,@.reloc,
0x0002a8,msvcrt.dll,
```

# Installation

- Python -m venv .env
- . .env/bin/activate
- Pip install scanner.tar.gz
- Poetry run scanner