Volatility

```
pipx install volatility3

pipx ensurepath
pipx completions
```

* Install symbols tables from github https://github.com/volatilityfoundation/volatility3

Windows Basics

https://volatility3.readthedocs.io/en/latest/volatility3.plugins.windows.html

```
vol -f <image> windows.info
vol -f <image> windows.pstree
windows.psscan
windows.pslist

vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles --pid <PID>
vol.py -f “/path/to/file” -o “/path/to/dir” windows.memmap --dump --pid
<PID>
vol.py -f “/path/to/file” windows.handles --pid <PID>
vol.py -f “/path/to/file” windows.dlllist --pid <PID>
vol.py -f “/path/to/file” windows.cmdline

vol.py -f “/path/to/file” windows.netscan
vol.py -f “/path/to/file” windows.netstat


vol.py -f “/path/to/file” windows.registry.hivescan
vol.py -f “/path/to/file” windows.registry.hivelist

vol.py -f “/path/to/file” windows.registry.printkey
vol.py -f “/path/to/file” windows.registry.printkey --key
“Software\Microsoft\Windows\CurrentVersion”

vol.py -f “/path/to/file” windows.filescan

filedump

vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles
vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles --virtaddr
<offset>
vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles --physaddr
<offset>
```

```
vol.py -f “/path/to/file” windows.malfind


vol.py -f “/path/to/file” windows.vadyarascan --yara-rules <string>
vol.py -f “/path/to/file” windows.vadyarascan --yara-file
“/path/to/file.yar”
vol.py -f “/path/to/file” yarascan.yarascan --yara-file “/path/to/file.yar”
```