Volatility Overview

https://t.me/learningnets

Volatility

- Advanced memory Forensics Framework written in python
- Runs on multiple platforms
- Open source
- Extensible API
- Coverage of multiple file formats
- Powerful community
- Used in incident response and forensics

Volatility Commands

Installation details:

http://www.volatilityfoundation.org/

Basic commands:

```
python vol.py -h
```

```
python vol.py -f <mem image> --profile=<profile name> plugin [args]
```

Volatility Commands (contd.)

Determining profile:

```
python vol.py -f < mem image > imageinfo
```

```
python vol.py -f < mem image > kdbgscan
```

Volatility Commands (contd.)

Displaying help:

```
python vol.py -h --> gives help for the default profile WinXPSP2x86
```

```
python vol.py --profile=< profile name > -h --> gives the help for specific profile
```

Volatility Commands (contd.)

Running the plugin & Plugin help:

```
python.py vol.py -f < mem image > --profile= < profile name > pslist
```

```
python vol.py -f < mem image > --profile=< profile name > pslist -h
```

Volatility Commands (contd.)

Plugin output:

```
python vol.py pslist > pslist.txt
```

```
python vol.py pslist --output-file=pslist.txt
```