Common Tools

pip

pip is an installer for Python libraries

Install OSX

```
sudo easy_install pip
```

Memory Analysis

Volatility

Volatility uses Python 2.6 or higher not Python 3

Download using the repository

```
git clone
https://github.com/volatilityfoundation/volatility
.git
```

Setup volatility

```
sudo python setup.py install
```

Libraries you may need (see Common Tools for pip)

```
sudo pip install Distorm3
sudo pip install Yara
sudo pip install PyCrypto
sudo pip install PIL
sudo pip install OpenPyxl
sudo pip install ujson
```

List all profiles, plugins, and other things currently installed

```
python vol.py --info
```

Convert pagefile.sys/hiberfile.sys to raw images

```
python vol.py -f <memory file> --profile<profile>
imagecopy -O <new_file_location>
```

Save volatility output to a file

```
python vol.py -f <memory file> --profile=<profile>
<volatility command> > <file>
```

List general info and possible profiles of memory file

```
python vol.py -f <memory file> imageinfo
```

Check profile

```
python vol.py -f <memory file> --profile=<profile>
kdbgscan
```

Check for more than 0 processes in *PsActiveProcessHead*

List processes

```
python vol.py -f <memory file> --profile=<profile>
psscan
```

List network connections

```
python vol.py -f <memory file> --profile=<profile>
netlist
```

Find potential malware

```
python vol.py -f <memory file> --profile=<profile>
malfind --dump-dir <directory>
```

Volatility Plugins

Recreate Ethernet traffic

Download the source from
https://code.google.com/archive/p/jamaal-re-tools/

Put the ethscan.py file into volatility/volatility/plugins

```
python vol.py -f <memory file> --profile=<profile>
ethscan > capture.pcap
```

Get Chrome history

Download the source from

https://github.com/superponible/volatility-plugins

Put the chromehistory.py and sqlite_help.py files into volatility/volatility/plugins

```
python vol.py -f <memory file> --profile=<profile>
chromehistory
```

File Analysis

Hashing

Get MD5

Linux

```
md5sum <file>
```

OSX

```
md5 <file>
```

Malware Checking

VirusTotal.com

Check hash

Use the search tab