OS Information

imageinfo

Volatility 2

```
        vol.py -f "filename" imageinfo
        vol.py -f "filename" kdbgscan
```

Volatility 3

```
        vol3 -f "filename" windows.info
```

Process Information

process list

Volatility 2

```
        vol.py -f "filename" --profile <profile> pslist
        vol.py -f "filename" --profile <profile> psscan
        vol.py -f "filename" --profile <profile> pstree
        vol.py -f "filename" --profile <profile> psxview
```

Volatility 3

```
        vol3 -f "filename"  windows.pslist
        vol3 -f "filename"  windows.psscan
        vol3 -f "filename"  windows.pstree
```

procdump

Volatility 2

```
        vol.py -f "filename" --profile <profile> procdump -p <PID> --dump-dir="output/dir"
```

Volatility 3

```
        vol3 -f "filename" -o "output/dir" windows.dumpfiles --pid <PID>
```

memdump

Volatility 2

```
        vol.py -f "filename" --profile <profile> memdump -p <PID> --dump-dir="output/dir"
```

Volatility 3

```
        vol3 -f "filename" -o "output/dir" windows.memmap --dump --pid <PID>
```

handles

Volatility 2

```
        vol.py -f "filename" --profile <profile> handles -p <PID>
```

Volatility 3

```
        vol3 -f "filename" windows.handles --pid <PID>
```

dlls

Volatility 2

```
        vol.py -f "filename" --profile <profile> dlllist -p <PID>
```

Volatility 3

```
        vol3 -f "filename" windows.dlllist --pid <PID>
```

cmdline

Volatility 2

```
        vol.py -f "filename" --profile <profile> netscan
        vol.py -f "filename" --profile <profile> netstat
```

XP/2003 SPECIFIC

```
        vol.py -f "filename" --profile <profile> connscan
        vol.py -f "filename" --profile <profile> connections
        vol.py -f "filename" --profile <profile> sockscan
        vol.py -f "filename" --profile <profile> sockets
```

Volatility 3

```
        vol3 -f "filename" windows.netscan
        vol3 -f "filename" windows.netstat
```

Network Information

netscan

Volatility 2

```
        vol.py -f "filename" --profile <profile> dlllist -p <PID>
```

Volatility 3

```
vol3 -f "filename" windows.dlllist --pid <PID>
```

Registry

hivelist

Volatility 2

```
vol.py -f "filename" --profile <profile> hivescan
vol.py -f "filename" --profile <profile> hivelist
```

Volatility 3

```
vol3 -f "filename" windows.registry.hivescan
vol3 -f "filename" windows.registry.hivelist
```

printkey

Volatility 2

```
vol.py -f "filename" --profile <profile> printkey
vol.py -f "filename" --profile <profile> printkey -K Software\Microsoft\Windows\CurrentVersion”
```

Volatility 3

```
vol3 -f "filename" windows.registry.printkey
vol3 -f "filename" windows.registry.printkey --key “Software\Microsoft\Windows\CurrentVersion”
```

hivedump

Volatility 2

```
vol.py -f "filename" --profile <profile> hivedump -o <offset>
```

Volatility 3(not sure if this capability exists in Vol3; however, you may be able to extract registry hives using filedump with the offset)

Files

filescan

Volatility 2

```
vol.py -f "filename" --profile <profile> filescan
```

Volatility 3

```
vol3 -f "filename" windows.filescan
```

filedump

Volatility 2

```
vol.py -f "filename" --profile <profile> dumpfiles --dump-dir="output/dir"
vol.py -f "filename" --profile <profile> dumpfiles --dump-dir="output/dir" -Q <offset>
vol.py -f "filename" --profile <profile> dumpfiles --dump-dir="output/dir" -p <PID>
```

Volatility 3

```
vol3 -f -o "output/dir"  "filename" windows.dumpfiles
vol3 -f -o "output/dir"  "filename" windows.dumpfiles --virtaddr <offset>
vol3 -f -o "output/dir"  "filename" windows.dumpfiles --physaddr <offset>
```