# Digital Forensics | Commands

## Useful Bash Commands

**sudo <command>**
Run as user root

**strings <file>**
Extract all strings from a file

**<command> | grep <parameters>**
Search the output of the pipelined command

**<command> | less**
Send output to a scrollable form

**gpg -d <in file> > <out file>**
Decrypt and/or verify file

## Hashing

**sha256sum <file>**
Calculate the sha256 hash of a file

**md5sum <file>**
Calculate the md5 hash of a file

## Volatility

In Linux we use the command volatility, while in Windows, we usually use vol.exe and then the rest of the line. Getting the image information to enable use of advanced tools:
**volatility imageinfo -f <imagefile.vmem>**

Prefix for most commands:
**volatility --profile=<profile from imageinfo's output> -f <imagefile.vmem> <volatility command>**

For example:
**volatility --profile=WinXPSP3x86 -f dump.vmem pslist**

## Processes

**pslist**
List the processes found

**pstree**
Display the processes found in a tree form

**cmdline**
Getting command-line parameters information

```
procdump -p <PID> --dump-dir <directory for dumped files>
```

This dumps the code of the process from the host’s memory

```
memdump -p <PID> --dump-dir <directory for dumped files>
```

This dumps the memory used by the process

## Networking

```
connscan
```

Display information about network connections

```
sockets
```

Display information about network sockets

```
netscan
```

This command finds TCP endpoints, TCP listeners, UDP endpoints, and UDP listeners

## Registry

```
Hivelist
```

List existing registry hives

```
printkey -K <registry key>
```

Print a specific key and the information it holds

```
malfind --dump-dir <directory for dumped files>
```

Find malicious activities

## Scalpel

Scalpel is a file carving and indexing application.

It has a configuration file (/etc/scalpel/scalpel.conf) that should be edited before execution.

Usage:

```
scalpel <binary file> -o <output folder>
```

```
scalpel -c /etc/scalpel/scalpel.conf -o <binary file>
```

## Binwalk

Binwalk is an open-source firmware extraction tool that extracts embedded file systems from firmware images.

**binwalk -Y <binary file>**
Identify the CPU architecture of a binary file

**binwalk -E <binary file>**
Entropy analysis of a binary file

**binwalk --extract <binary file>**
Extract files from a binary file

**binwalk -B <binary file>**
Signature analysis