



Intro to Memory Forensics with Volatility

Intro to Memory Forensics

Welcome!!

Let's make a great workshop!

Chicolinux (a.k.a. Miguel Guirao)



Intro to Memory Forensics

Your computer will betray you!

What is Digital Forensics?

“The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting, and possible expert presentation.”

Ken Zatyko

<http://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics>

Digital Forensics Process

- 1) Search Authority
- 2) Chain of Custody
- 3) Imaging/Hashing Function
- 4) Validated Tools
- 5) Analysis
- 6) Repeatability (Quality Assurance)
- 7) Reporting
- 8) Possible Expert Presentation

Ken Zatyko

<http://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics>

LOCARD'S EXCHANGE PRINCIPLE

Locard's exchange principle says that, in the physical world, whenever perpetrators enter or leave a crime scene, they will leave something behind and take something with them. (Saferstein, 2006).



Intro to Memory Forensics

A digital investigator seeks to preserve the state of the digital environment in a manner that allows the investigator to reach reliable inferences through analysis.

Intro to Memory Forensics

IMPORTANT

The course of action is often prioritized based on the order of decreasing volatility.

Intro to Memory Forensics

It is never recommended to dump memory to the target system's local drive.

MEMORY DUMP FORMATS

Volatility automatically identify the file format for you:

crashinfo, hibinfo, hpakinfo (HBGary), machoinfo, vmwareinfo, vboxinfo

- **rawmemorydump - widely supported**
- **windows crash dump**
- **windows hibernation file**
- **vm memory [VMWare: .vmem raw schema; .vmsn snapshots; .vmss saved state] [VBox:]**



WHY IS IMPORTANT?

Each function performed by an operating system or application results in specific modifications to the computer's memory (RAM), which can often persist a long time after the action, essentially preserving them.



WHY IS IMPORTANT?

Critical data often exist exclusively only in memory:

- Disk encryption keys
- Memory-resident injected code fragments
- off-the-record chat messages
- unencrypted e-mail messages



WHY IS IMPORTANT?

It must be loaded in memory to be executed.

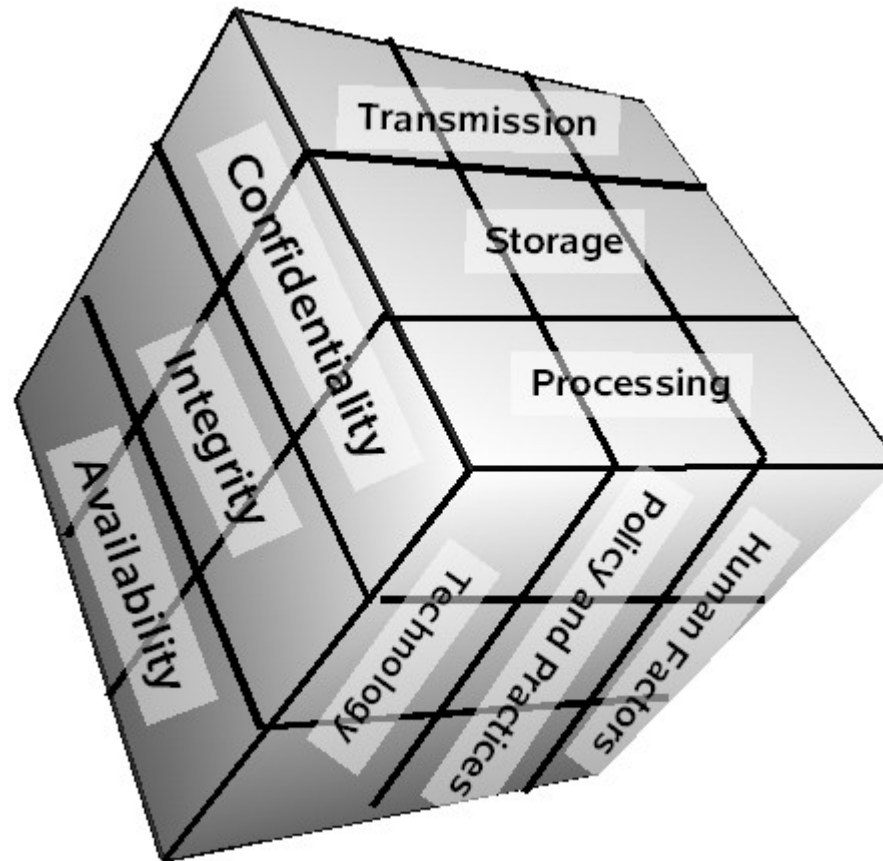
McCumber Cube

In 1991, John McCumber created a model framework for establishing and evaluating information security programs, now known as The McCumber Cube.

This security model is depicted as a three-dimensional Rubik's Cube-like grid.

https://en.wikipedia.org/wiki/McCumber_cube

McCumber Cube



https://en.wikipedia.org/wiki/McCumber_cube

Intro to Memory Forensics

PART I:

Intro to Volatility

<http://www.volatilityfoundation.org/>

Intro to Volatility



Extraction of digital artifacts from RAM samples.



Intro to Volatitlity

WHAT YOU NEED?

- **Volatility v2.5 (latest version right now!)**
- **Python 2.7**
- **Memory Adquisition Tools**
- **YARA**
- **Recommended plugins**



Intro to Volatility

There are many way that you can install Volatility,
I recommend the following two:

- Source code packages. Just unpack the archive and you are done!
- Clone it from the github repository

Intro to Volatitlity

Sadly!!



Intro to Volatility

What is a profile?

Is a collection of VTypes, overlays and object classes for a specific operating system version and hardware architecture (x86, x64, ARM).

- a. Metadata
- b. system call information
- c. constant values
- d. native types
- e. system map

Intro to Volatility

What is a profile?

Each profile has a unique name:

[OS Name][version][SP][architecture]

For example: Windows 7 SP1 x64 --> Win7SP1x64

Volatility supports memory dumps from:

- Windows
- Linux
- Mac
- Android



Plugins every where!

You can use plugins other than those that come with Volatility.

Or you can create your own.

--plugins Linux/Mac dir1:dir2:dir3 Win dir1;dir2;dir3

It must come right after vol.py!

It comes with 200 plugins (--info)

Intro to Volatility

Basic command:

```
python vol.py -f FILENAME --profile=PROFILE PLUGIN [ARGS]
```



Intro to Volatility

Who asked for help?

-h / --help either be global help or plugin based





Hola --profile!

What type of system your memory dump came from!

Default: WinXPSP2x86

ha, profile? **imageinfo**, **kdbgscan** to the rescue!

Antiforensics

- a. Modifying values in the data structure
- b. recently applied patches or a cold boot

Intro to Volatility

To be aware:

Some plugins use by default, the first kdbg data structure found.

But, we can specify which one to use with: --kdbg=





Ease my life!

Environment variables and configuration files:

- a. `export VOLATILITY_PROFILE=Win7SP1x64`
`export VOLATILITY_LOCATION=file:///tmp/myimage.img`
- b. `pwd`, `~` or `----conf-file` and a file named `.volatitlityrc`

[DEFAULT]
PROFILE=Win7SP1x64
LOCATION=file:///tmp/myimage.img

Hands on!

From the memory samples, tell me to which OS they belong to.



Intro to Memory Forensics

PART II:

First steps with Volatility

PROCESS, HANDLES & TOKENS.

LAB # 1

Please, turn to the sheet titled “LAB # 1”, and perform each one of the sections.

45 min.



Intro to Memory Forensics

PART III:



NETWORKING

LAB # 2

Please, turn to the sheet titled “LAB # 2”, and perform each one of the sections.

30 min.



PART IV:



MALWARE

LAB # 3

Please, turn to the sheet titled “LAB # 3”, and perform each one of the sections.

30 min.



Intro to Memory Forensics

PART V:

ROOT KIT

ROOT/ADMIN ACCESS SET OF TOOLS

ROOTKITS

LAB # 4

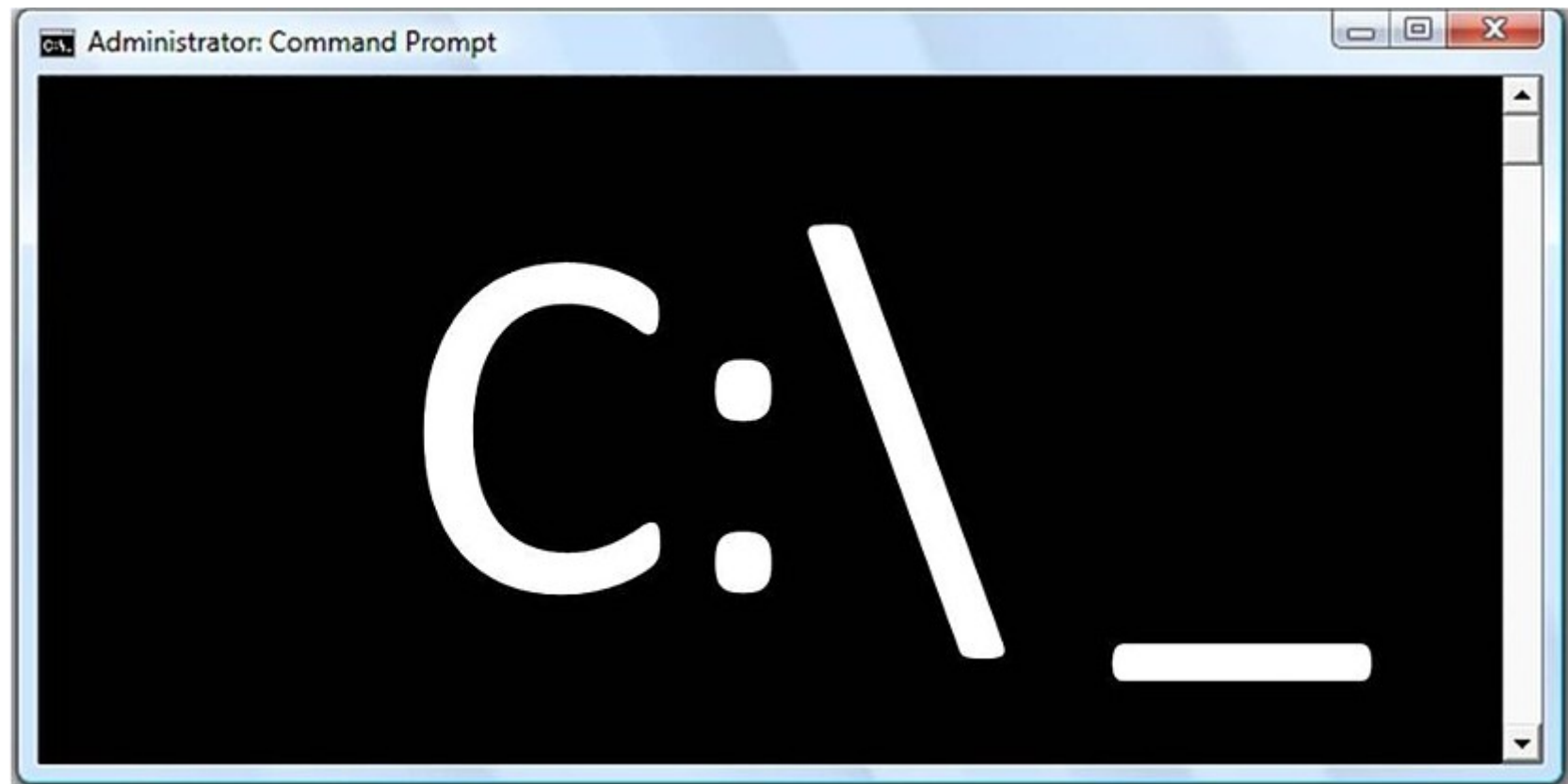
Please, turn to the sheet titled “LAB # 4”, and perform each one of the sections.

30 min.



Intro to Memory Forensics

PART VI:



COMMAND LINE

LAB # 5

Please, turn to the sheet titled “LAB # 5”, and perform each one of the sections.

30 min.



INTRO TO MEMORY FORENSICS WITH VOLATILITY

