

[Home](#)[About Us](#)[Publication](#)[Tools](#)[Project](#)[Guideline](#)[Workshop](#)[Data Search](#)

## Volafox

### LDFS

**Tool Desc** Mac OS X Memory Analysis Toolkit  
**Using Env** 10.6-9(Snow Leopard ~ Mavericks); 32/64-bit kernel input: \*.mem (osxpmem or virtualmachine raw memory file), \*.mmr (Mac Memory Reader, flattened x86)

### CLDFS

**Contact** rapfer@gmail.com

**License** GPL Version 2

### REGA

**Source code** Volafox is open source project. site: <http://code.google.com/p/volafox>

**Download** [Volafox\(0.9\)](#)

**Hash(SHA1)** 1383c667c7d2e65387aa48875466f3a7d40a2b76

### WEFA

#### Introduction

- volafox a.k.a 'Memory Analyzer for Mac OS X' is developed on python 2.5

- volafox is memory forensics tool for gathering system information and finding rootkit. it need to get two image.

- kernel image(mach\_kernel)
- Memory Image(firewire, '/dev/mem' or any other operation to dump physical memory.)

### JPEGViewer

### P.F.P

#### Information

### LNK Parser

### Volafox

```

sh2rkzui-Mac:volafox-0 sh2rkz$ python ./vol.py
volafox: Mac OS X Memory Analysis Toolkit
project: http://code.google.com/p/volafox
support: 10.6-9(Snow Leopard ~ Mavericks); 32/64-bit kernel
input: *.vmem (VMware memory file), *.mmr (Mac Memory Reader, flattened x86, IA-32e)
usage: python ./vol.py -i IMAGE [-o COMMAND [-vp PID][--x KEXT_ID][--x TASKID]]

Options:
-o CMD          : Print kernel information for CMD (below)
-d PID          : List open files for PID (where CMD is "lsot")
-v             : Print all files, including unsupported types (where CMD is "lsot")
-x PID/KID/TASKID : Dump process/task/kernel extension address space for PID/KID/Task ID (where CMD is "ps"/"kextstat"/"tasks"/"machdump")

COMMANDS:
system_profiler : Kernel version, CPU, and memory spec, Boot/Sleep/Wakeup time
mount           : Mounted filesystems
kextstat       : KEXT (Kernel Extensions) listing
kextscan       : Scanning KEXT (Kernel Extensions) (64bit OS only, experiment)
ps             : Process listing
tasks          : Task listing (Finding process hiding)
machdump       : Dump macho binary (experiment)
systab         : Syscall table (Hooking detection)
mtt           : Mach trap table (Hooking detection)
netstat       : Network socket listing (Hash table)
lsdf          : Open files listing by process (research, osxmem@gmail.com)
pestate       : Show Boot information
efiinfo       : EFI System Table, EFI Runtime Services
keychaindump  : Dump master key candidates for decrypting keychain(Lion ~ Mavericks)
dmesg         : Debug message at boot time
uname         : Print a short for unix name(uname)
hostname      : Print a hostname
trustedbsd    : Show TrustedBSD MAC Framework
bash_history  : Show history in bash process
sh2rkzui-Mac:volafox-0 sh2rkz$
Display all 1385 possibilities? (y or n)

```

- Machine Information - Darwin Kernel Version, CPU, Physical Memory, etc

- Mounted Filesystem - Like command 'df', you can show mounted device information.

- Process List - Volafox show process list at time on Imaging Physical Memory.

- KEXT information/dump - volafox show kext information, and dump kext in memory image.

- System call list/hooks detection - volafox analysis kernel symbol, and find system call table. In Additional, it can detect system call hooking using writer's technique.

Center for information Security Technologies. Anam-dong 5-ga Seongbu-gu, Seoul, Korea. / TEL +82-2-3290-4738 / FAX +82-2-928-9109

COPYRIGHT. 2013 Digital Forensic Research Center in KOREA UNIV. All right Reserved. forensic@cist.korea.ac.kr

