Digital Forensics
KOREA UNIVERSITY

LDFS
CLDFS
REGA
WEFA
JPEGViewer
P.F.P
LNK Parser
Volafox

Volafox

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)
Contact	rapfer@gmail.com
License	GPL Version 2
Source code	Volafox is open source project. site: http://code.google.com/p/volafox
Download	Volafox(0.9)
Hash(SHA1)	1383c667c7d2e65387aa48875466f3a7d40a2b76

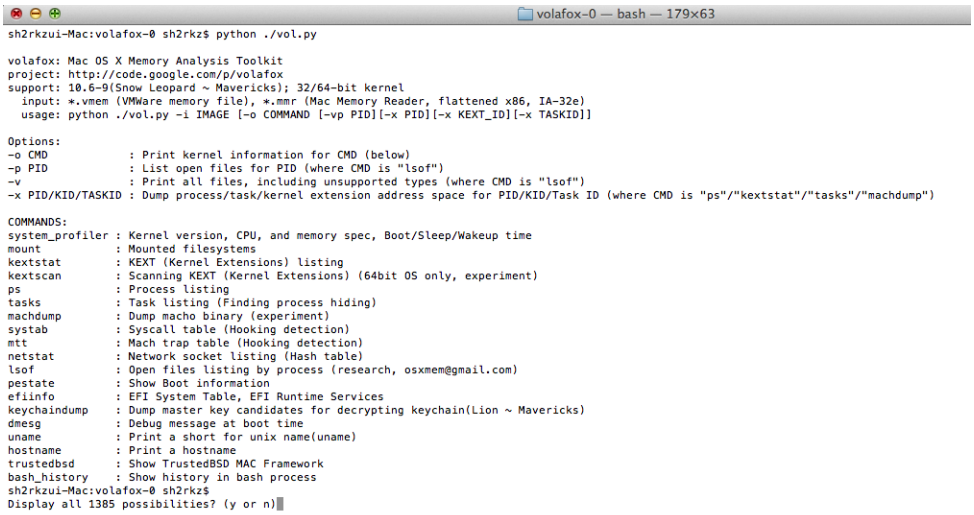
Introduction

- 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.)

Information



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

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