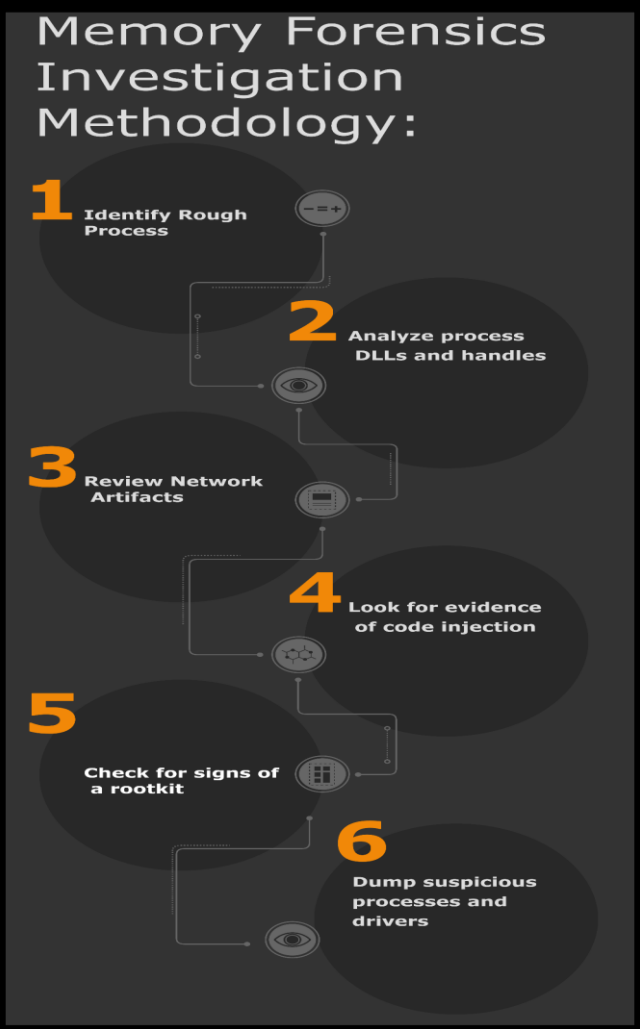
Memory Forensics Cheat-Sheet



Volatile Artifact Collector

Source: https://github.com/cado-security/varc

Varc executed accross

- Windows
- Linux
- OSX
- AWS Lambda
- Cloud environments such as AWS EC2
- Containerised Docker/Kubernetes environments such as AWS ECS/EKS/Fargate and Azure AKS

Cloud Forensics using Varc:

python3 varc.py -h

```
┌──(root㉿kali)-[/home/kali/Desktop/varc]
└─# python3 varc.py -h
usage: varc.py [-h] [--skip-memory] [--skip-open] [--dump-extract] [--yara-scan YARA_SCAN] ...

positional arguments:
  args

optional arguments:
  -h, --help            show this help message and exit
  --skip-memory         Skip collecting process memory, which can be slow
  --skip-open           Skip collecting open files, which can be slow
  --dump-extract        Extract process memory dumps, which can be slow
  --yara-scan YARA_SCAN
                        Scan process memory using compiled YARA rule file, which can be slow.
```

Varc Installation Process:

1. Clone the repository then install with:
python3 setup.py install

2. Then call with:
#from varc import acquire_system
#output_file_path = acquire_system().zip_path

python3 varc.py

(execute command.. To access some data, you will need to run with elevated privileges (i.e. sudo or root on Linux)

```
┌──(root㉿kali)-[/home/kali/Desktop/varc]
└─# python3 varc.py
[2023-10-22 16:58:25,171]:[INFO] - Operating System is: linux
[2023-10-22 16:58:25,181]:[INFO] - Acquiring system: kali, at 2023-10-22 16:58:25
[2023-10-22 16:58:26,580]:[INFO] - Adding Netstat Data
[2023-10-22 16:58:26,581]:[INFO] - Adding open file /usr/share/locale/en/LC_MESSAGES/gtk30-properties.mo
[2023-10-22 16:58:26,581]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libbd_loop.so.2.0.0
[2023-10-22 16:58:26,582]:[INFO] - Adding open file /usr/libexec/gvfs-mtp-volume-monitor
[2023-10-22 16:58:26,587]:[INFO] - Adding open file /usr/share/glib-2.0/schemas/gschemas.compiled
[2023-10-22 16:58:26,592]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libFLAC.so.8.3.0
[2023-10-22 16:58:26,605]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
[2023-10-22 16:58:26,612]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libxvidcore.so.4.3
[2023-10-22 16:58:26,648]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libdbusmenu-gtk3.so.4.0.12
[2023-10-22 16:58:26,655]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libsbc.so.1.3.0
[2023-10-22 16:58:26,659]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/pipewire-0.3/libpipewire-module-rtkit.so
[2023-10-22 16:58:26,659]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libc-2.33.so
[2023-10-22 16:58:26,781]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libgio-2.0.so.0.6600.8
[2023-10-22 16:58:27,046]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libusb-1.0.so.0.3.0
[2023-10-22 16:58:27,061]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libX11.so.6.4.0
[2023-10-22 16:58:27,236]:[INFO] - Adding open file /var/log/lightdm/x-0.log
[2023-10-22 16:58:27,237]:[INFO] - Adding open file /usr/libexec/at-spi-bus-launcher
[2023-10-22 16:58:27,240]:[INFO] - Adding open file /usr/lib/python3/dist-packages/gi/_gi_cairo.cpython-39-x86_64-linux-gnu.so
[2023-10-22 16:58:27,242]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libacl.so.1.1.2301
[2023-10-22 16:58:27,246]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/gio/modules/libdconfsettings.so
[2023-10-22 16:58:27,255]:[INFO] - Adding open file /usr/bin/udevadm
[2023-10-22 16:58:27,410]:[INFO] - Adding open file /usr/local/lib/python3.9/dist-packages/psutil-5.9.6-py3.9-linux-x86_64.egg/psutil/_psutil_posix.abi3.so
[2023-10-22 16:58:27,418]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/ModemManager/libmm-plugin-quectel.so
[2023-10-22 16:58:44,710]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libvdpau.so.1.0.0
[2023-10-22 16:58:44,712]:[INFO] - Adding open file /usr/lib/python3.9/lib-dynload/_queue.cpython-39-x86_64-linux-gnu.so
[2023-10-22 16:58:44,714]:[INFO] - Adding open file /usr/lib/x86_64-linux-gnu/libbz2.so.1.0.4
Process dump progess: 100%|████████████████████████████████████████████████████████| 234/234 [04:26<00:00,  1.14s/ procs]
[2023-10-22 17:03:11,398]:[INFO] - Dumping processing has completed. Output file is located: kali-1697974105.181599.zip
```

Cheat-Sheet for Volatility 2 & Volatility 3

Information about OS

Information About	Plugins for Volatility 2	Plugins for Volatility 3
IMAGEINFO	• vol.py -f “/path/file” imageinfo • vol.py -f “/path/file” kdbgscan	• vol.py -f “/path/file” windows.info

Information about Process

Information About	Plugins for Volatility 2	Plugins for Volatility 3
PSLIST	• vol.py -f “/path/file” --profile <profile> pslist • vol.py -f “/path/file” --profile <profile> psscan • vol.py -f “/path/file” --profile <profile> pstree • vol.py -f “/path/file” --profile <profile> psxview	• vol.py -f “/path/file” windows.pslist • vol.py -f “/path/file” windows.psscan • vol.py -f “/path/file” windows.pstree
PROCDUMP	• vol.py -f “/path/file” --profile <profile> procdump -p <PID> --dump-dir=“/path/dir”	• vol.py -f “/path/file” -o “/path/dir” windows.dumpfiles --pid <PID>
MEMDUMP	• vol.py -f “/path/file” --profile <profile> memdump -p <PID> --dump-dir=“/path/dir”	• vol.py -f “/path/file” -o “/path/dir” windows.memmap --dump --pid <PID>
HANDLES	• vol.py -f “/path/file” --profile <profile> handles -p <PID>	• vol.py -f “/path/file” windows.handles --pid <PID>
DLLS	• vol.py -f “/path/file” --profile <profile> dlllist -p <PID>	• vol.py -f “/path/file” windows.dlllist --pid <PID>
CMDLINE	• vol.py -f “/path/file” --profile <profile> cmdline • vol.py -f “/path/file” --profile <profile> cmdscan • vol.py -f “/path/file” --profile <profile> consoles	• vol.py -f “/path/file” windows.cmdline

Information about Network

Information About	Plugins for Volatility 2	Plugins for Volatility 3
NETSCAN	• vol.py -f “/path/file” --profile <profile> netscan • vol.py -f “/path/file” --profile <profile> netstat **For XP/2003** • vol.py -f “/path/file” --profile <profile> connscan • vol.py -f “/path/file” --profile <profile> connections • vol.py -f “/path/file” --profile <profile> sockscan • vol.py -f “/path/file” --profile <profile> sockets	• vol.py -f “/path/file” windows.netscan • vol.py -f “/path/file” windows.netstat

Information about Registry

Information About	Plugins for Volatility 2	Plugins for Volatility 3
HIVELIST	• vol.py -f “/path/file” --profile <profile> hivescan • vol.py -f “/path/file” --profile <profile> hivelist	• vol.py -f “/path/file” windows.registry.hivescan • vol.py -f “/path/file” windows.registry.hivelist
PRINTKEY	• vol.py -f “/path/file” --profile <profile> printkey • vol.py -f “/path/file” --profile <profile> printkey -K “Software\Microsoft\Windows\CurrentVersion”	• vol.py -f “/path/file” windows.registry.printkey • vol.py -f “/path/file” windows.registry.printkey --key “Software\Microsoft\Windows\CurrentVersion”
HIVEDUMP	• vol.py -f “/path/file” --profile hivedump -o <offset>	• vol.py -f “/path/file” -o “/path/dir” windows.dumpfiles --physaddr <offset>

Information about Files

Information About	Plugins for Volatility 2	Plugins for Volatility 3
FILESCAN	• vol.py -f “/path/file” --profile <profile> filescan	• vol.py -f “/path/file” windows.filescan
FILEDUMP	• vol.py -f “/path/file” --profile <profile> dumpfiles --dump-dir=“/path/dir” • vol.py -f “/path/file” --profile <profile> dumpfiles --dump-dir=“/path/dir” -Q <offset> • vol.py -f “/path/file” --profile <profile> dumpfiles --dump-dir=“/path/dir” -p <PID>	• vol.py -f “/path/file” -o “/path/dir” windows.dumpfiles • vol.py -f “/path/file” -o “/path/dir” windows.dumpfiles --virtaddr <offset> • vol.py -f “/path/file” -o “/path/dir” windows.dumpfiles --physaddr <offset>

Information about Miscellaneous Activity

Information About	Plugins for Volatility 2	Plugins for Volatility 3
MALFIND	• vol.py -f “/path/file” --profile <profile> malfind	• vol.py -f “/path/file” windows.malfind
YARASCAN	• vol.py -f “/path/file” yarascan -y “/path/file.yar”	• vol.py -f “/path/file” windows.vadyarascan --yara-rules <string> • vol.py -f “/path/file” windows.vadyarascan --yara-file “/path/file.yar” • vol.py -f “/path/file” yarascan.yarascan --yara-file “/path/file.yar”

Scan to learn more

The course is on 50% Sale now!