

# Practical Windows Forensics: Cheat Sheet

*Disclaimer: This cheatsheet has been created by Blue Cape Security, LLC to provide students with resources and information related to the Practical Windows Forensic (PWF) course. Please note that this cheatsheet is not intended to be a comprehensive list of all available Windows artifacts that could be relevant to an investigation.*

## Data Collection

Suspend the Virtual Machine before taking memory images.

## Virtual Box

### Memory

- Identify the VM's UUID:  
`vboxmanage list vms`
- Create a snapshot of the VM's memory:  
`vboxmanage debugvm <VM_UUID> dumpvm-core --filename win10-mem.raw`

### Disk

- Identify the VM's UUID:  
`vboxmanage list vms`
- Identify the VM's disk UUID:  
`vboxmanage showvminfo <VM_UUID>`  
Note the UUID of the disk in row IDE Controller
- Export the disk using the disk UUID:  
`vboxmanage clonemedium disk <disk_UUID>`

## VMWare

### Memory

- Collect the .vmem and associated .vmss and .vmsn files if available

### Disk

- Collect all .vmdk files associated with the current snapshot ID
- Alternatively, create a single VMDK from split files:  
`C:\Program Files (x86)\VMware\VMware Player\vmware-vdiskmanager.exe» -r «d:\VMLinux\vmdiskname.vmdk» -t 0 MyNewImage.vmdk`

## Hashing

### Windows

`Get-FileHash -Algorithm SHA1 <file>`

### Mac/Linux

`shasum <file>`

## Data Extraction

Fundamental sources of forensic evidence on Windows systems

### Memory

### Disk



## Registry Hives

### Registry root keys:

Name	Abbreviation
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_CONFIG	HKCC

## Registry Hives:

Registry Path	Hive and Supporting Files
HKLM\SAM	SAM, SAM.LOG
HKLM\SECURITY	SECURITY, SECURITY.LOG
HKLM\SOFTWARE	SOFTWARE, SOFTWARE.LOG, SOFTWARE.sav
HKLM\SYSTEM	SYSTEM, SYSTEM.LOG, syst SYSTEM em.sav
HKLM\HARDWARE	(Dynamic/Volatile Hive)
HKU\DEFAULT	Default, Default.LOG, Default.sav
HKU\SID	NTUSER.DAT
HKU\SID_CLASSES	UsrClass.dat, UsrClass.dat.LOG

## Registry Hives Location:

### System-specific Hives

```
\Windows\System32\config\DEFAULT
\Windows\System32\config\SAM
\Windows\System32\config\SECURITY
\Windows\System32\config\SOFTWARE
\Windows\System32\config\SYSTEM
```

### User-specific Hives

```
\Users\<user>\AppData\Local\Microsoft\Windows\UsrClass.dat
\Users\<user>\NTUSER.DAT
```

## Registry file types:

File Extension	Description
No extension	Registry Hive File
.alt extension	Backup copy of hive, used in Windows 2000, not XP
.log extension	Transaction log of changes to a hive
.sav extension	Backup copy of hive created at the end of text-mode (console) phrase during Windows XP setup

## Registry Analysis

### System Information

#### Computername:

*HKLM\System\CurrentControlSet\Control\Computername\*

#### Windows Version:

*HKLM\Software\Microsoft\Windows NT\Currentversion\*

#### Timezone:

*HKLM\System\CurrentControlSet\Control\Time-ZoneInformation\*

#### Network Information:

*HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{interface-name}*

#### Shutdown time:

*HKLM\System\CurrentControlSet\Control\Windows\ShutdownTime*

#### Defender settings:

*HKLM\Software\Microsoft\Windows Defender\*

#### User Profiles:

*HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\{SID}*

## User Information

#### UserAssist

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}*

In Vista and Windows 7:

- {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} – A list of applications, files, links, and other objects that have been accessed.

- {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} – Lists the shortcut links used to start programs

#### RecentDocs

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*

#### ShellBags

*USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags*

*USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU*

#### OpenSavePidIMRU

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU*

#### Last-Visited MRU

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPIDIMRU*

## New Technology File System (NTFS)

### Files

- C:\\$MFT – Master File Table stores records of every file and directory

- C:\\$LogFile – Tracks MFT metadata changes

- C:\\$Extend\\$UsnJrnl:\$J (Alternate Data Stream) – Tracks file changes

## MFT File Record Structure

### Important headers, attributes and values:

MFT Record header

- Headers include entry number, Flags (InUse), etc.

\$STD\_INFO attribute

- MACB timestamps 0x10 – user level

\$FILE\_NAME attribute

- File name
- MACB timestamps 0x30 – system level

\$DATA attribute

- Resident (True or False)
- Data or DataRun if not resident

## MACB Timestamps:

Timestamp	Notation	Description
Modified	m...	File modified
Accessed	.a..	File accessed
Changed (\$MFT record)	..c.	MFT record modified
Birth (Created)	...b	File created

## Execution

### Background Activity Moderator (BAM)

#### Registry:

HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings

### AmCache

#### Registry:

C:\Windows\AppCompat\Programs\Amcache.hve

### Prefetch

#### Path:

C:\Windows\Prefetch\\*.pf

### Shortcut (LNK) Files

#### Path:

C:\users\\AppData\Roaming\Microsoft\Windows\Recent

#### Path:

C:\users\\AppData\Roaming\Microsoft\Office\Recent

## Persistence

### Auto-Run keys:

#### Registry:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

## Startup Folders

### File Paths:

C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

## Windows Services

### Registry:

HKLM\SYSTEM\CurrentControlSet\Services\Windows\Start Menu\Programs\Startup

## Tasks

### Registry:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree

### File Path:

C:\Windows\System32\Tasks

## Event Logs

### Path:

C:\Windows\System32\winevt\logs

Source	Event IDs	Description
Microsoft-Windows-Defender	5000	Defender enabled
Microsoft-Windows-Defender	5001	Defender disabled
System	7045	A new service was installed
Security	4624	An account was successfully logged on
Windows PowerShell	400	Engine state is changed from None to Available
Microsoft-Windows-Sysmon	1	Process creation
Microsoft-Windows-Sysmon	3	Network connection
Microsoft-Windows-Sysmon	11	File create
Microsoft-Windows-Sysmon	12, 13	Registry events
Microsoft-Windows-Sysmon	22	DNS query

## Memory Analysis

### Additional memory related artifacts:

hiberfil.sys	Hibernation system file
pagefile.sys	Paging file
swapfile.sys	Special type pagefile

## Volatility

<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>

### Command:

*vol-fwin10-memory.raw windows.info*

Plugins	Description
Windows.info	Show operating system information
Windows.pstree	List processes in tree structure
Windows.pslist	List processes
Windows.pslist --pid <PID> --dump	Dump process
Windows.dlllist --pid <PID> --dump	Dump DLLs associated with a process
Windows.getsids --pid <PID>	SIDs associated with a process
Windows.registry.hivelist	Show registry hives and offsets
Windows.registry.printkey --offset <hive_offset> --key <key_name>	Show registry key

## Super Timelines

### QEMU

Convert VHD to RAW disk:

*Qemu-img convert -O raw disk.vhd disk.raw*

### Volatility

Create timeline from memory:

*Vol -f memory.raw timeliner --create-bodyfile*

### Log2Timeline

<https://plaso.readthedocs.io/en/latest/index.html>

Create plaso file from raw disk:

*Log2timeline.py --storage-file disk.plaso disk.raw*

Show plaso file info:

*Pinfo.py disk.plaso*

Merge body with plaso file:

*Log2timeline.py --parser=mactime --storage-file=disk.plaso volatility.body*

Create CSV timeline from date:

*Psort.py -o l2tcsv -w super-timeline.csv disk.plaso "date" > '2022-03-01 00:00:00*