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\vm-ware-vdiskmanager.exe» -r «d:\VMLinux\vmd-kname.vmdk» -t 0 MyNewImage.vmdk

Hashing

Windows

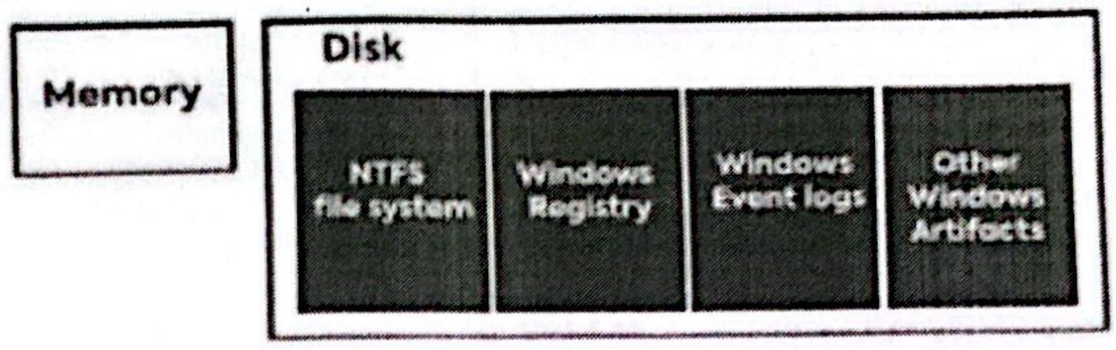
Get-FileHash -Algorithm SHA1 <file>

Mac/Linux

shasum <file>

Data Extraction

Fundamental sources of forensic evidence on Windows systems



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.
\Users\<user>\NTUSER.DAT

Windows Directories

Directory	Description
C:\Windows\System32\drivers\etc\hosts	DNS file
C:\Windows\System32\drivers\etc\networks	Network Config file
C:\Windows\System32\config\SAM	Usernames and Password
C:\Windows\System32\config\SECURITY	Security Log
C:\Windows\System32\config\SOFTWARE	Software Log
C:\Windows\System32\config\SYSTEM	System Log
C:\Windows\System32\winevt\	Windows Event Logs
C:\Windows\repair\SAM	Backup of User and Password
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\	Windows XP All User Startup
C:\Documents and Settings\User\Start Menu\Programs\Startup	Windows XP User Startup
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp	Windows All User Startup
C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	Windows User Startup
C:\Windows\Prefetch	Prefetch files
C:\Windows\AppCompat\Programs\Amcache.hve	Amcache.hve
C:\Windows\Users*\NTUSER.dat	NTUSER.dat