Windows Forensics Cheat Sheet

System Info & Accounts

OS Version:

- SOFTWARE\Microsoft\WindowsNT\CurrentVersion

Current Control Set:

- SOFTWARE\Microsoft\WindowsNT\CurrentVersion
- SYSTEM\Select\Current
- SYSTEM\Select\LastKnownGood

Computer Name:

- SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Time Zone Information:

- SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Autostart Proccess (Autoruns):

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
- SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run

SAM hive and user information:

- SAM\Domains\Account\Users

File/Folder Usage & Knowledge

Recent Files:

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

Office Recent Files:

- NTUSER.DAT\Software\Microsoft\Office\VERSION
- NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

ShellBags:

- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

Open/Save and LastVisited Dialog MRUs:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Windows Explorer Address/Search Bars:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer WordWheelQuery

File/Folder Search Bar

- NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/WordWheelQuery

USB Device

Device identification:

- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SYSTEM\CurrentControlSet\Enum\USB

First/Last Times:

- SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####
  - 0o64=first connection
  - 0066=last connection
  - 0067=last removal

USB device Volume Name:

- SOFTWARE\Microsoft\Windows Portable Devices\Devices

Evidence Of Execution

UserAssist:

NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

ShimCache:

SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

AmCache:

Amcache.hve\Root\File\{VolumeGUID}\

BAM/DAM:

SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}

SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Command Execution:

NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/RunMRU