



# Registry Forensics Cheatsheet

## System info and accounts



### OS Version:

SOFTWARE\Microsoft\Windows NT\CurrentVersion

### Current Control set:

HKLM\SYSTEM\CurrentControlSet  
SYSTEM\Select\Current  
SYSTEM\Select\LastKnownGood

### Computer Name:

SYSTEM\CurrentControlSet\Control\ComputerName  
\ComputerName

### Time Zone Information:

SYSTEM\CurrentControlSet\Control  
\TimeZoneInformation

### Network Interfaces and Past Networks:

SYSTEM\CurrentControlSet\Services\Tcpip  
\Parameters\Interfaces

### Autostart Programs (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

## External/USB device forensics



### 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

## File/folder usage or 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

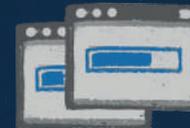
### Open/Save and Last Visited Dialog MRUs:

NTUSER.DAT\Software\Microsoft\Windows  
\CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU  
NTUSER.DAT\Software\Microsoft\Windows  
\CurrentVersion\Explorer\ComDlg32\LastVisitedPidMRU

### Windows Explorer Address/Search Bars:

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

## 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\{Volume GUID}\

### BAM/DAM:

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