WINDOWS REGISTRY LOCATIONS AND DETAILS

Windows Registry Locations

Tools:

- Registry Explorer.
- RegRipper.
- ShellBags Explorer.

OS Version

SOFTWARE\Microsoft\Windows NT\CurrentVersion

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

The past networks a given machine was connected to can be found in the following locations:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

Autostart Programs (Autoruns):

The following registry keys include information about programs or commands that run when a user logs on.

`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`

The following registry key contains information about services:

`SYSTEM\CurrentControlSet\Services`

SAM hive and user information:

The SAM hive contains user account information, login information, and group information. This information is mainly located in the following location:

`SAM\Domains\Account\Users`

Recent Files:

Windows maintains a list of recently opened files for each user. As we might have seen when using Windows Explorer, it shows us a list of recently used files. This information is stored in the NTUSER hive and can be found on the following location:

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

Office Recent Files:

Similar to the Recent Docs maintained by Windows Explorer, Microsoft Office also maintains a list of recently opened documents. This list is also located in the NTUSER hive. It can be found in the following location:

NTUSER.DAT\Software\Microsoft\Office\VERSION

The version number for each Microsoft Office release is different. An example registry key will look like this:

NTUSER.DAT\Software\Microsoft\Office\15.0\Word

Here, the 15.0 refers to Office 2013. A list of different Office releases and their version numbers can be found on this link.

Starting from Office 365, Microsoft now ties the location to the user's live ID. In such a scenario, the recent files can be found at the following location.

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

In such a scenario, the recent files can be found at the following location. This location also saves the complete path of the most recently used files.

ShellBags:

When any user opens a folder, it opens in a specific layout. Users can change this layout according to their preferences. These layouts can be different for different folders. This information about the Windows *'shell'* is stored and can identify the Most Recently Used files and folders. Since this setting is different for each user, it is located in the user hives. We can find this information on the following locations:

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:

When we open or save a file, a dialog box appears asking us where to save or open that file from. It might be noticed that once we open/save a file at a specific location, Windows remembers that location. This implies that we can find out

recently used files if we get our hands on this information. We can do so by examining the following registry keys

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

Windows Explorer Address/Search Bars:

Another way to identify a user's recent activity is by looking at the paths typed in the Windows Explorer address bar or searches performed using the following registry keys, respectively.

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

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

Evidence Of Execution:

UserAssist:

Windows keeps track of applications launched by the user using Windows Explorer for statistical purposes in the User Assist registry keys. These keys contain information about the programs launched, the time of their launch, and the number of times they were executed. However, programs that were run using the command line can't be found in the User Assist keys. The User Assist key is present in the NTUSER hive, mapped to each user's GUID. We can find it at the following location:

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

ShimCache:

ShimCache is a mechanism used to keep track of application compatibility with the OS and tracks all applications launched on the machine. Its main purpose in Windows is to ensure backward compatibility of applications. It is also called Application Compatibility Cache (AppCompatCache). It is located in the following location in the SYSTEM hive:

```
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
```

ShimCache stores file name, file size, and last modified time of the executables.

We can use the following command to run the AppCompatCache Parser Utility:

```
AppCompatCacheParser.exe --csv <path to save output> -f <path to SYSTEM hive for data parsing> -c <control set to parse>
```

The output can be viewed using EZviewer, another one of Eric Zimmerman's tools.

AmCache:

The AmCache hive is an artifact related to ShimCache. This performs a similar function to ShimCache, and stores additional data related to program executions. This data includes execution path, installation, execution and deletion times, and SHA1 hashes of the executed programs. This hive is located in the file system at:

`C:\Windows\appcompat\Programs\Amcache.hve`

Information about the last executed programs can be found at the following location in the hive:

`Amcache.hve\Root\File\{Volume GUID}\`

BAM/DAM:

Background Activity Monitor or BAM keeps a tab on the activity of background applications. Similar Desktop Activity Moderator or DAM is a part of Microsoft Windows that optimizes the power consumption of the device. Both of these are a part of the Modern Standby system in Microsoft Windows.

In the Windows registry, the following locations contain information related to BAM and DAM. This location contains information about last run programs, their full paths, and last execution time.

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

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

Device identification:

The following locations keep track of USB keys plugged into a system. These locations store the vendor id, product id, and version of the USB device plugged in and can be used to identify unique devices. These locations also store the time the devices were plugged into the system.

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

`SYSTEM\CurrentControlSet\Enum\USB`

First/Last Times:

Similarly, the following registry key tracks the first time the device was connected, the last time it was connected and the last time the device was removed from the system.

SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####

In this key, the #### sign can be replaced by the following digits to get the required information:

Value	Information
0064	First Connection time
0066	Last Connection time
0067	Last removal time

Although we can check this value manually, as we have seen above, Registry Explorer already parses this data and shows us if we select the USBSTOR key.