CYBER_FORENSIC ANALYSIS FOR WINDOWS

Cheat sheet

1.8.3

World Cybernetics House 33, 18th floor, 29th door

ÍNDEX

REGEDIT.EXE

Structure of the Registry:

The registry on any Windows system contains the following five root keys:

1. HKEY_CURRENT_USER
2. HKEY_HKEY_USERS
3. HKEY_LOCAL_MACHINE
4. HKEY_CLASSES_ROOT
5. HKEY_CURRENT_CONFIG

WINDOWS + R => "regedit.exe"

HKEY_HKEY_USERS (HKU)

All actively loaded user profiles.

HKCU is a subkey of HKU.

HKEY_CURRENT_USER (HKCU)

User who is currently logged on.

Info on:

> User's folders
>
> User's screen colors
>
> User's Control Panel settings

HKEY_LOCAL_MACHINE (HKLM)

Computer configuration info.

For any user == Not specific

It is a type of default info.

HKEY_CLASSES_ROOT(HKCR)

It is a subkey of **HKEY_LOCAL_MACHINE\Software**

Its job is to execute the correct program to open a certain file that you request through Windows Explorer.

This key can be found divided on two other keys.

HKEY_CLASSES_ROOT provides a merged view of the two infos.

(HKCR also provides this merged view for programs that are designed for earlier versions of Windows.)

- HKEY_LOCAL_MACHINE\Software\Classes

  Which states the default settings that apply for all users.

- HKEY_CURRENT_USER\Software\Classes

  Which states the settings particular to the running user. These, always override the default ones.

Default settings CHANGE

To change the default settings, which are registered inside HKCR, it is required to be done under **HKEY_LOCAL_MACHINE\Software\Classes** and NOT! under HKCR

Current User settings CHANGE

To change the settings on the current user, which are registered inside HKCR it is needed to be done under **HKEY_CURRENT_USER\Software\Classes** and NOT! under HKCR

!!![1] If you make changes under any HKCR subkey (with an exception) the changes will be saved on *HKEY_LOCAL_MACHINE\Software\Classes*.

!!![2] If you make changes under HKCR and the key that you are editing info on, already exists under *HKEY_CURRENT_USER\Software\Classes* the system will then save it in *HKEY_CURRENT_USER\Software\Classes* and NOT! in *HKEY_LOCAL_MACHINE\Software\Classes*.

HKEY_CURRENT_CONFIG

Saved information on the hardware profile used at system startup

OFFLINE HIVES ACCESS

Knowledge needed to analyze registry hives on an "image" instead of a live system

First HIVES

Most of the top important hives are saved under **C:\Windows\System32\Config** these are:

- DEFAULT (HKEY_USERS\Default)
- SAM (HKEY_LOCAL_MACHINE\SAM)
- SECURITY (HKEY_LOCAL_MACHINE\Security)
- SOFTWARE (HKEY_LOCAL_MACHINE\Software)
- SYSTEM (HKEY_LOCAL_MACHINE\System)

User HIVES

This **HIDDEN** hives files can be found under the user profile directory -> C:\Users\<username>\ (For W7 and above)

- NTUSER.DAT (HKEY_CURRENT_USER when a user logs in)

Under C:\Users\<username>\AppData\Local\Microsoft\Windows we find:

- USRCLASS.DAT (HKEY_CURRENT_USER\Software\CLASSES)

Amcache HIVE

Saves info on what programs where recently run on the system and it can be found on:

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

Transaction Logs

Transaction logs next to backups are a fundamental and strategic piece of information for an accurate analysis. Transaction logs are “CHANGELOGS” of the Registry Hive.

The way Windows uses Transaction Logs can lead to a Transaction Log having information on the latest changes on the Registry Hive and the Registry Hive in question not yet containing them. These files are saved in the same directory as their hive and have the same name as the hive they refer to but end with .LOG instead of .HVE

If there are more than one Transaction log they will be named in the following sequence:

<tlog1>.LOG1   <tlog1>.LOG2   <tlog1>.LOG3   <···>

Backups

Contains the backups located at C:\Windows\System32\Config and they are saved every ten days to C:\Windows\System32\Config\RegBack.

As @umairalizafar highlights, backups can be helpful if the registry is presumed to have been recently manipulated, modified, or deleted.

DATA ACQUISITION

As the files in %WINDIR%\System32\Config are RESTRICTED, a tool is needed to be able to acquire these files.

KAPE

Umairalizafar's Kroll Artifact Parser and Extractor room

- KAPE

Autopsy

Has the option to acquire data from live systems and disk images.

- Autopsy

FTK Imager

Similar to Autopsy but mounts the disk image or drive in FTK Imager.

- FTK Imager

REGISTRY VIEW

To view the extracted hives as they would be shown through the Windows Registry Editor, a different tool is needed for this purpose.

AccessData's Registry Viewer

- Loads ONE hive at a time
- DOES NOT consider Transaction Logs

AccessData R.V.

Zimmerman's Registry Explorer

- Loads MULTIPLE hives at a time
- DOES consider Transaction Logs
- Includes BOOKMARKS menu

Z's R.E.

RegRipper

Takes a Hive, extracts its data, and outputs it as a report in text format.

- DOES NOT consider Transaction Logs

SYS INFO & ACCOUNTS

In forensic analysis you may come across many situations where the only recovered information is “triage data”. Therefore, you must know how to extract and determine basic information such as the computer name, OS version, Startup config, Time Zones, Network Interface, Autoruns, SAM, and User info.

Computer Name

The computer’s name can be found under:

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

OS version

Found under:

SOFTWARE\Microsoft\Windows NT\CurrentVersion

Current Control Set (CCT – Startup config info)

It is common to find two different Control Sets: ControlSet001, and ControlSet002,

- ➢ ControlSet001 states the config with which the computer run StartUp (booted with).
  - ▪ SYSTEM\ControlSet001
- ➢ ControlSet002 states the last known GOOD config
  - ▪ SYSTEM\ControlSet002

There is also a <u>volatile</u> Control Set that Windows creates while it is running called: CurrentControlSet, found under:

- ➢ HKLM\SYSTEM\CurrentControlSet

This control set is the one to look at when trying to determine the most accurate information. To acquire data on the Control Set that is being used as the CurrentControlSet you may look at:

- ➢ SYSTEM\Select\Current

In the same way as we had ControlSet001 and <···>.002, being this last one the last known config, the CCT has it to. To find the last known configuration to the CCT, you may look at:

- SYSTEM\Select\LastKnownGood

Time Zone info

Time zone data can be crucial to understand the chronology of events. Information on Time Zones is found at:

- SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Network Interface and Past Networks

Network Interface

The list of Network Interfaces used on the machine can be found at:

- SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interface

Every interface is named by a GUID a unique identifier. It is related to de TCP/IP configuration particular to that interface it names.
This GUID key gives info on these main aspects:

- IP address
- DHCP IP address
- Subnet Mask
- DNS Servers

Past Networks

Accessible at:

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

Here you will also find when these networks were used for the last time. a.k.a. the last time they were connected. This intel is found under the last write time of the registry key of the past network in question.

AutoStart Programs (Autoruns)

These are keys regarding info on programs or commands active when any user logs on the computer:

- 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

This is the key responsible for saving information on services:

- SYSTEM\CurrentControlSet\Services

(If the value of the subkey "Start" on this key is set to 0x02 the service starts at boot)

SAM Hive & User Info

The SAM Hive contains:

- Account Info
- Login Info
- Group Info

You may find this under:

- SAM\Domains\Account\Users

This registry key holds information on:

- User RID
- Number of "Log-ins"
- Last Log-in
- Last Failed Log-in
- Last Password Change
- Password expiry date
- Password policy
- Password Hint
- Groups the user is part of

KNOWLEDGE OF FILES & FOLDERS

Recent Files

Windows does save a record on what files were opened recently and the last time it was opened. It can be found at:

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

There are registry keys for specific file extensions. You can access the registry key for .PNG files at:

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

Office specific recent files

Microsoft Office keeps an alternate record of recently opened Office files, found at:

- 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

Office Version equivalents

Office 365	>	16.0
Microsoft 365	>	16.0
Office LTSC 2021	>	16.0
Office 2021	>	16.0
Office 2019	>	16.0
Office 2016	>	16.0
Office 2013	>	15.0

With Office 365 and above, Windows now saves the records using the users Live ID[1] following this structure:

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

*[1] A Windows Live ID is your e-mail address and a password that you choose. After you've signed up for a Windows Live ID, you can use it on Windows Live sites like Windows Live Hotmail, Windows Live Messenger, Office Live, Xbox Live, and more.

ShellBags

Shellbags are set of registry keys which contain details about a user's viewed folder, its layout and the changes they have done according to their preferences.

Because ShellBags are particular to each user they are stored under it.

- 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

A useful tool to view ShellBags is Eric Zimmerman's ShellBag-Explorer

- EZ's SB-Explorer

Open/Save & Last Visited Dialog MRUs

When we open and save a file in Windows, telling where to specifically save or open it, Windows saves that information too. Therefore, by looking at these locations and when were they accessed, we can infer what were some files that were opened recently. Here are the keys to look at:

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

EVIDENCE OF EXECUTION

UserAssist

Windows collects that data on what programs are launched by the user using Windows Explorer this collection of data can be found under the User Assist key. They contain:

- Info on programs launched
- Time of launch
- Times executed

Location:

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

ShimCache (AppCompatCache)

It is a mechanism that tracks ALL applications launched on the system. Windows uses it under claiming its necessity for backwards compatibility of applications and it records each application's compatibility with the OS running. It stores the following information:

- File name
- File size
- Last modified time of every ".exe" registered

Located at:

- SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

For this data to be human readable another of Eric Zimmerman' tool is needed. AppCompatCache-Parser which outputs a CSV file when given the system hive as input.

- EZ's AppCompatCache-Parser

As at the time this document is being written, AppCompatCache-Parser is a CLI based program you may know the command to execute it on the Windows Console:

AppCompatCacheParser.exe --csv <path to output> -f <path to SYSTEM hive> -c <control set to parse>

AmCache

Artifact related to ShimCache that stores information on program executions, including:

- Execution Path
- Installation
- Execution time
- Deletion time
- SHA1 hash of the program

It can be found at:

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

To look at the last executed programs head to:

- [···]\Amcache.hve\Root\File\{Volume GUID}\

BAM/DAM

Background Activity Monitor and Desktop Activity Moderator. BAM keeps track of background applications activity. DAM is a power consumption optimizer. These two are part of Modern Standby system of Windows, keeping information on:

- Last run programs
- Full path to program
- Last execution time

Found at:

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

EXTERNAL/USB DEVICES FORENSICS

Device Identification

USBSTOR & USB keys keep track of every USB key plugged into the system, storing:

- Vendor ID
- Product ID
- Version of USB device (can be used to identify unique devices)

Found at:

- 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}\####

At this key it is found:

- First time the device was connected.
- Last time it was connected
- Last time the device was removed from the system

The "####" sign can be replaced by the following digits to get the required information:

0064 --------	First Connection time
0066 --------	Last Connection time
0067 --------	Last removal time

USB device Volume Name

Device name of the connected drive:

- SOFTWARE\Microsoft\Windows Portable Devices\Devices

We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification to correlate the names with unique devices.

Combining all this information, we can create a fair picture of any USB devices that were connected to the machine we're investigating.

The end.

Synthesis of @umairalizafar's Windows Forensic 1 room

By:

!.8.3