

Practicing Access Data's Registry Viewer

Goal

Windows registry is a system-defined hierarchical database containing Windows hardware, user information and preferences, application, and network configuration information. Examining the Windows registry is one of the most important steps for Windows forensic analysis.

Case Scenario

Use Access Data's Registry Viewer to examine the files, and to extract and correlate information to obtain evidence.

Software and registry files

Registry Viewer is installed on the virtual machine *Windows 10 w/ FTK 6 & EnCase 8* on RLES. User Guide download link: https://ad-pdf.s3.amazonaws.com/RegistryViewer_UG.pdf

The Windows registry hive files are:

- SAM
- SYSTEM
- Mark-NTUSER.DAT

1. Examine the SAM registry hive by expanding SAM>Domains>Account>Users.

Question 1. Which user name and SID number logged onto the system on 3/8/2016 at 4:40:56 UTC?

Mark 000003E9 1001

The screenshot shows the Windows Security console with the SAM database selected. The left pane shows the hierarchy: SAM > Domains > Account > Users > 000003E9. The right pane shows the details for user Mark.

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 1E 18 48 B4 F4 78 D1 01 00 00 00 00 00 00 00 C6 A5 0B 27 DE 78 D1 01
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 08 00 00 00 00 00 00 C4 00 00 00 00 00
ForcePassw...	REG_BINARY	00 00 00 00

Key Properties	
Last Written Time	3/8/2016 4:40:56 UTC
RID unique identifier	1001
User Name	Mark
Logon Count	3
Last Logon Time	3/8/2016 4:40:56 UTC
Last Password Change	3/8/2016 1:59:30 UTC
Expiration Time	Never
Invalid Logon Count	0

Question 2. When was the last date and time that Mark changed his Windows password?

3/8/2016 1:59:30 UTC

RID unique identifier	1001
User Name	Mark
Logon Count	3
Last Logon Time	3/8/2016 4:40:56 UTC
Last Password Change Time	3/8/2016 1:59:30 UTC
Expiration Time	Never

Question 3. Who has never logged onto this Windows system?

Guest

Key Properties	
Last Written Time	3/8/2016 4:58:50 UTC
RID unique identifier	501
User Name	Guest
Description	Built-in account for guest access to the computer/domain
Logon Count	0
Last Logon Time	Never
Last Password Change Time	Never
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never

2. Examine the SYSTEM registry hive.

Question 4. Click on “Select” and check the value of “Current”. What is the current ControlSet?
0x00000001(1) Controlset001

Name	Type	Data
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownG	REG_DWORD	0x00000001 (1)

Key Properties
 Last Written Time: 8/22/2013 13:25:43 UTC

Question 5. Click ControlSet001 and search for “TimeZone” via “Edit>Find...” What is the TimeZoneKeyName?
Eastern standard time

Name	Type	Data
Bias	REG_DWORD	0x0000012C (300)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000000F0 (240)

Question 6. Expand ControlSet001>Enum>USBSTOR. How many USBs were plugged into the system and what are the USB’s friendly names? (Hint: expand each device entry and click on the unique instance ID, for example “2005284530117BB2A6FD&0”)

2 USB’s

Disk&Ven_MBIL_SSM&Prod_Moser_Baer_Disk&Rev_PMAP
Disk&Ven_sanSanDisk&Prod_CRruzer_Blade&Rev_1.18

FriendlyName ⇒ SanDisk Cruzer Blade USB Device

FriendlyName ⇒ MBIL SSM Moser Baer Disk USB Device

Question 7. Select SYSTEM> MountedDevices. Search the USB instance ID
 “2005284530117BB2A6FD&0.” Which Windows Volume had this USB device mounted to?

USBSTOR Disk&Ven_SanDisk&Prod_CRruzer_Blade&Rev_1.18

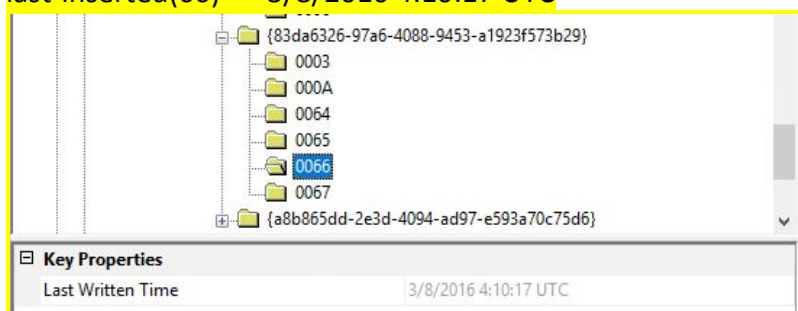
volume ⇒ \??\Volume{2b14099e-e4d2-11e5-824e-e4ce8f4ba039}

\\DosDevices\\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 45 00 4E 00 4...
\\DosDevices\\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 49 00 23 00 43 00 64 00 5...
\\?\\Volume{2b14099e-e4d2-11e5-824e-e4ce8f4ba039}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23...
\\DosDevices\\E:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23...
\\?\\Volume{2b140aad-e4d2-11e5-824e-e4ce8f4ba039}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23...

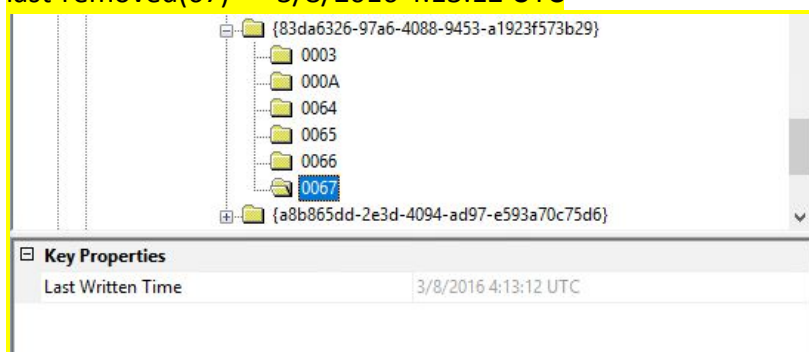
00	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00	_ . ? . ? . _ . U . S . B . S .
10	54 00 4F 00 52 00 23 00 44 00 69 00 73 00 6B 00	T . O . R . # . D . i . s . k .
20	26 00 56 00 65 00 6E 00 5F 00 53 00 61 00 6E 00	s . V . e . n . _ . S . a . n .
30	44 00 69 00 73 00 6B 00 26 00 50 00 72 00 6F 00	D . i . s . k . s . P . r . o .
40	64 00 5F 00 43 00 72 00 75 00 7A 00 65 00 72 00	d . _ . C . r . u . z . e . r .
50	5F 00 42 00 6C 00 61 00 64 00 65 00 26 00 52 00	_ . B . l . a . d . e . R .
60	65 00 76 00 5F 00 31 00 2E 00 31 00 38 00 23 00	e . v . _ . l . _ . l . 8 . # .

Question 8. When was the USB with the instance ID of “2005284530117BB2A6FD&0” last-inserted to the system, and when was it last-removed? (Hint: See lecture ppt slides #17)

last-inserted(66) ⇒ 3/8/2016 4:10:17 UTC



last-removed(67) ⇒ 3/8/2016 4:13:12 UTC



3. Examine Mark_NTUSER.DAT registry hive.

Question 9. Click on “Mark-NTUSER.DAT”. To find the URLs Mark visited, you select Edit > Find, enter the registry key “TypedURL” in the Find what: text area, and click Find Next. Check the data of “TypedURL”, What URLs did Mark visit?

<ftp://192.168.67.143>

<http://go.microsoft.com/fwlink/p/?LinkId=255141>

Name	Type	Data
url1	REG_SZ	ftp://192.168.67.143/
url2	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

Question 10. Checking the value of “TypedURLsTime”, when was the last date and time that Mark visited <ftp://192.168.67.143/>? (Hint: the date and time are shown in the key properties pane. It can also be determined by selecting the data in hex at the right bottom pane, right click and use “Show Hex Interpreter Window...” function.)

stored ⇒ 3/8/2016 4:01:17 UTC

local ⇒ 3/7/2016 23:01:17 UTC

Name	Type	Data
url1	REG_BINARY	A3 84 62 2A EF 78 D1 01
url2	REG_BINARY	00 00 00 00 00 00 00 00

Hex Interpreter		
Type	Size	Value
signed integer	1-8	131018832774071459
unsigned integer	1-8	131018832774071459
FILETIME (Stored)	8	3/8/2016 4:01:17
FILETIME (As Local)	8	3/7/2016 23:01:17
DOS date	2	-
DOS time	2	-
DOS date/time	4	-

Question 11. Checking the value of “User Shell Folders” by Clicking on “Mark-NTUSER.DAT” and using Edit > Find. What is the path to Mark’s “Favorites” fold?

%USERPROFILE%\Favorites

Shell Folders	ab Cookies	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Microsoft\Windo...
Shutdown	ab SendTo	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
StartPage	ab Personal	REG_EXPAND_SZ	%USERPROFILE%\Documents
Streams	ab Recent	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
StuckRects2	ab Favorites	REG_EXPAND_SZ	%USERPROFILE%\Favorites
Taskband	ab My Pictures	REG_EXPAND_SZ	%USERPROFILE%\Pictures
TypedPaths	ab Start Menu	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
User Shell Folders	ab NetHood	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
UserAssist	ab My Music	REG_EXPAND_SZ	%USERPROFILE%\Music
VisualEffects	ab My Video	REG_EXPAND_SZ	%USERPROFILE%\Videos
Ext			