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

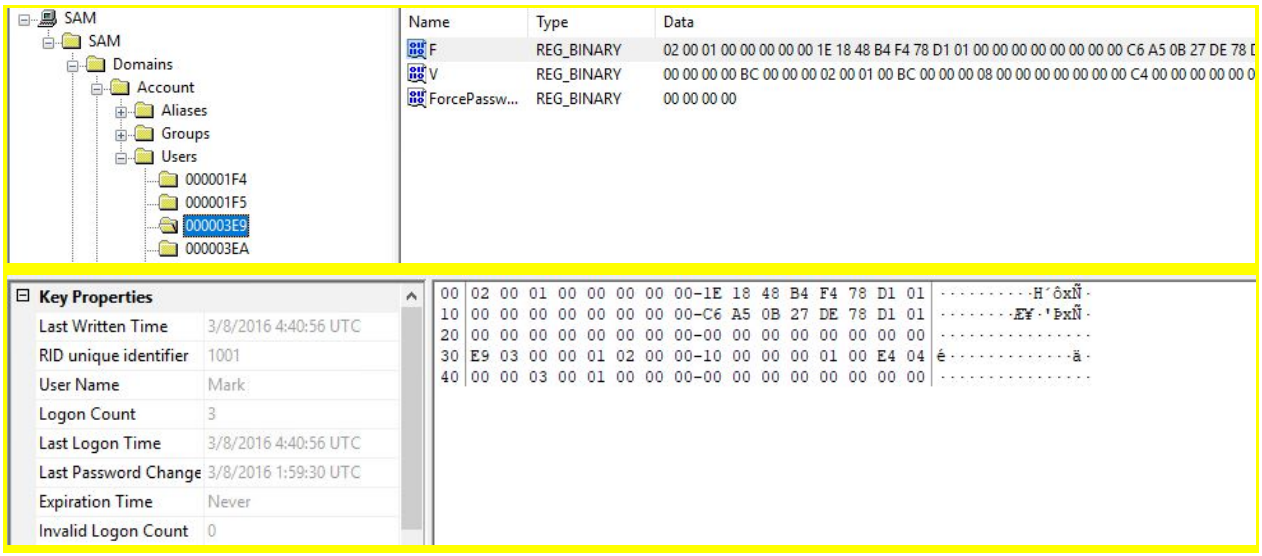
The Windows registry hive files are:

- SAM
- SYSTEM
- Mark-NTUSER.DAT

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

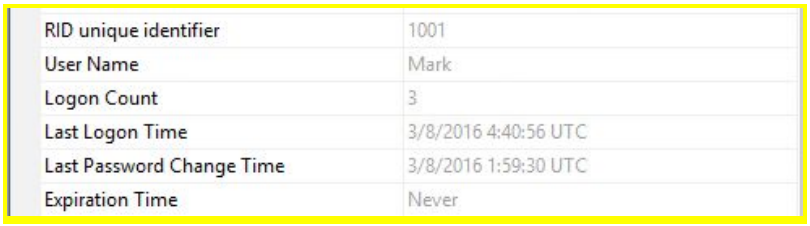
Question 1. Which user name and SID number logged onto the system on 3/8/2016 at 4:40:56 UTC?

Mark 000003E9 1001



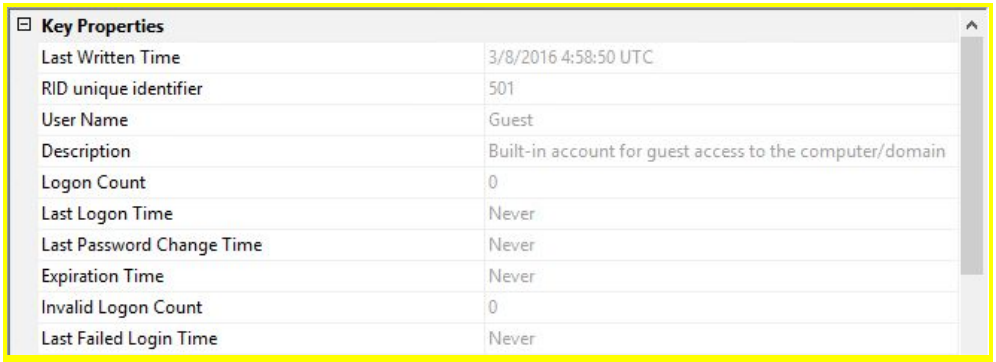
Question 2. When was the last date and time that Mark changed his Windows password?

3/8/2016 1:59:30 UTC



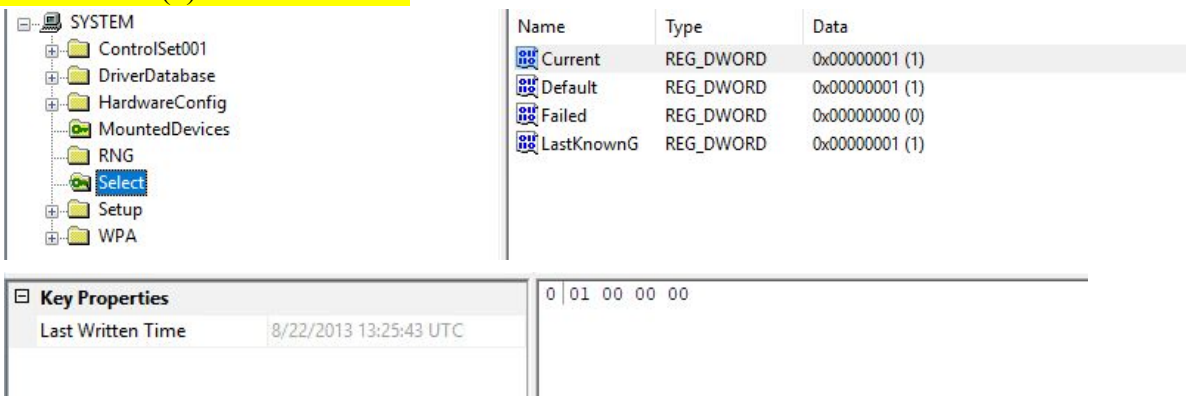
Question 3. Who has never logged onto this Windows system?

Guest

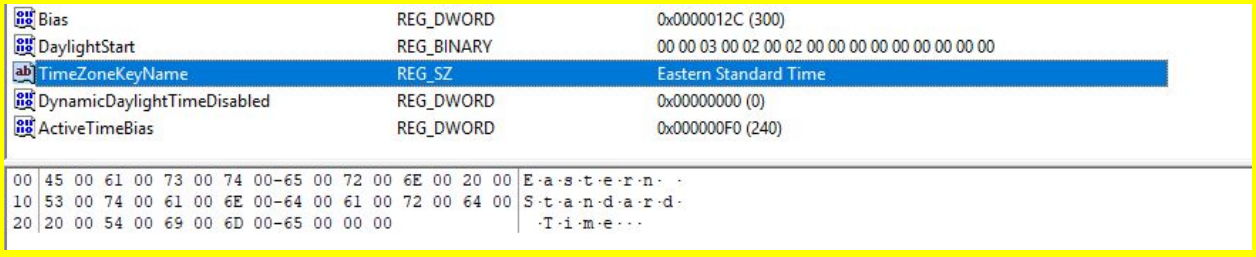


2. **Examine the SYSTEM registry hive.**

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



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

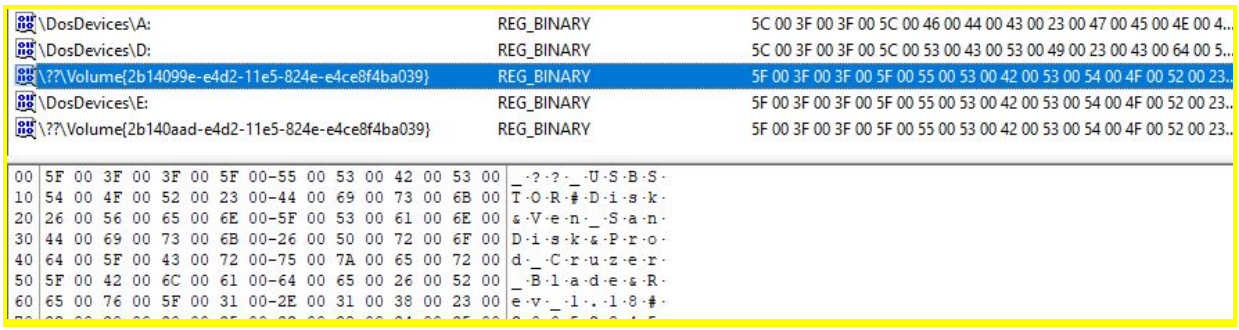


Question 6. Expand ControlSet001>Enum>USBSTOR. How many USBs were plugged into the system and what are the USB's friendly names? (Hint: expand each device entry and click on the unique instance ID, for example "2005284530117BB2A6FD&0")

2 USB's
Disk&Ven_MBIL_SSM&Prod_Moser_Baer_Disk&Rev_PMAP
Disk&Ven_sanSanDisk&Prod_CRruzer_Blade&Rev_1.18

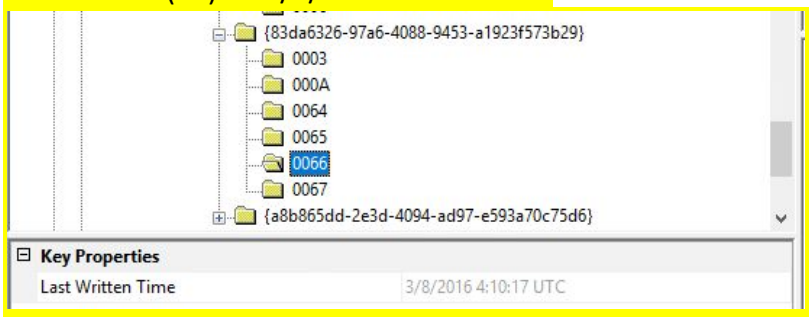
FriendlyName ⇒ SanDisk Cruzer Blade USB Device
FriendlyName ⇒ MBIL SSM Moser Baer Disk USB Device

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)

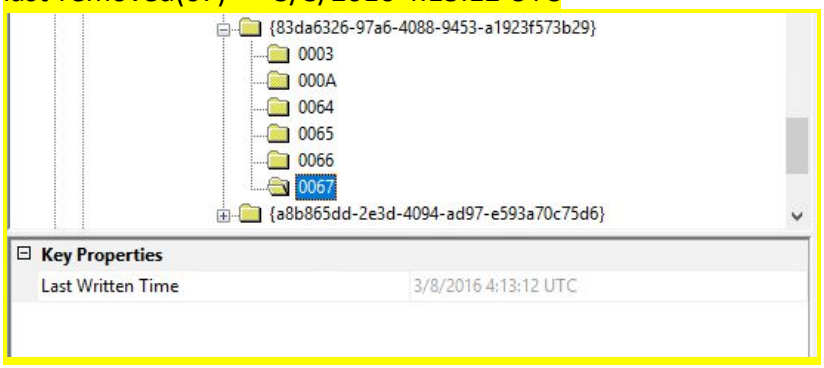


Question 8. When was the USB with the instance ID of "2005284530117BB2A6FD&0" last-inserted to the system, and when was it last-removed? (Hint: See lecture ppt slides #17)

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