CSEC 730 - Advanced Computer Forensics

Practicing Access Data's Registry Viewer
Homework 3

Due Date: Please submit your answers to the Homework 3 dropbox by Sunday midnight 11/25/2018.

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

Do you still remember the *Linux_Financial_Case* from Lab 1? *You are given* the registry hive files acquired from Mark's system. In this activity, you will 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

Download and extract the *Registry files for HW3.zip* from *myCourses > Project and Homework.* The Windows registry hive files are:

- SAM
- SYSTEM
- Mark-NTUSER.DAT

Instructions

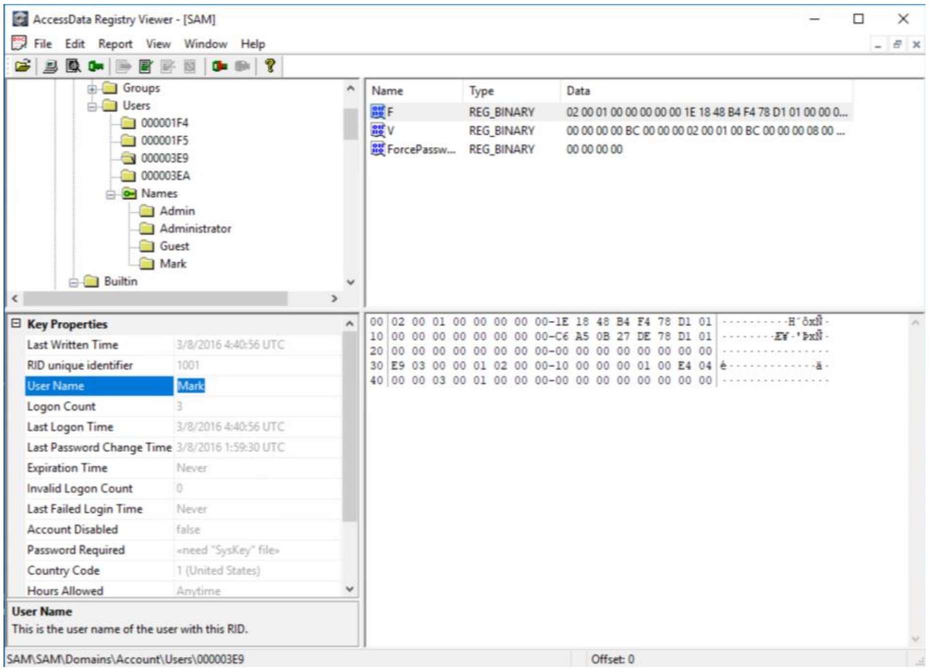
- To open the hive-file you would like to examine, click File > Open.
- Registry Viewer also lets you quickly search keys, values, and dates that were last written to the registry file. To find certain registry data, you will select Edit > Find.

Deliverables:

Examine the SAM, SYSTEM and Mark-NTUSER.DAT hives and **answer all the questions below. Include one screenshot for EACH question as supporting data.**

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, 1001



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 1E 18 48 B4 F4 78 D1 01 00 00 0...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 08 00 ...
ForcePassw...	REG_BINARY	00 00 00 00

```
00 02 00 01 00 00 00 00 00-1E 18 48 B4 F4 78 D1 01  ----------H´ôxÑ-
10 00 00 00 00 00 00 00 00-C6 A5 0B 27 DE 78 D1 01  -------Æ¥-'ÞxÑ-
20 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
30 E9 03 00 00 01 02 00 00-10 00 00 00 01 00 E4 04  é------------ä-
40 00 00 03 00 01 00 00 00-00 00 00 00 00 00 00 00  ----------------
```

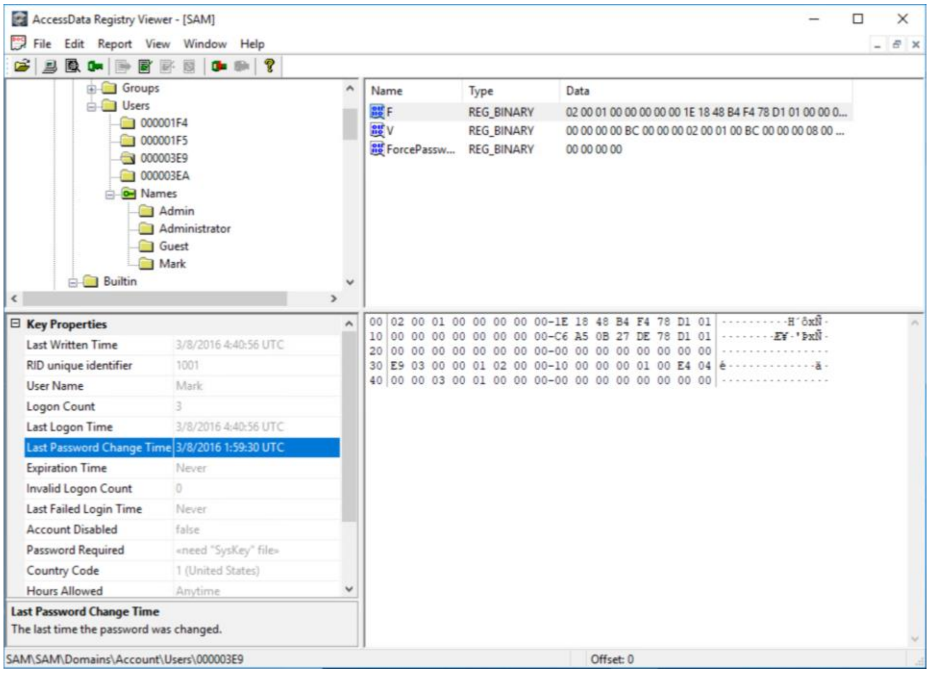
Key Properties	
Last Written Time	3/8/2016 4:40:56 UTC
RID unique identifier	1001
User Name	Mark
Logon Count	3
Last Logon Time	3/8/2016 4:40:56 UTC
Last Password Change Time	3/8/2016 1:59:30 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	«need "SysKey" file»
Country Code	1 (United States)
Hours Allowed	Anytime

User Name

This is the user name of the user with this RID.

SAM\SAM\Domains\Account\Users\000003E9 Offset: 0

Question 2. When was the last date and time that Mark changed his Windows password? 3/8/2016 1:59:30 UTC



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 1E 18 48 B4 F4 78 D1 01 00 00 0...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 08 00 ...
ForcePassw...	REG_BINARY	00 00 00 00

```
00 02 00 01 00 00 00 00 00-1E 18 48 B4 F4 78 D1 01  ----------H´ôxÑ-
10 00 00 00 00 00 00 00 00-C6 A5 0B 27 DE 78 D1 01  -------Æ¥-'ÞxÑ-
20 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
30 E9 03 00 00 01 02 00 00-10 00 00 00 01 00 E4 04  é------------ä-
40 00 00 03 00 01 00 00 00-00 00 00 00 00 00 00 00  ----------------
```

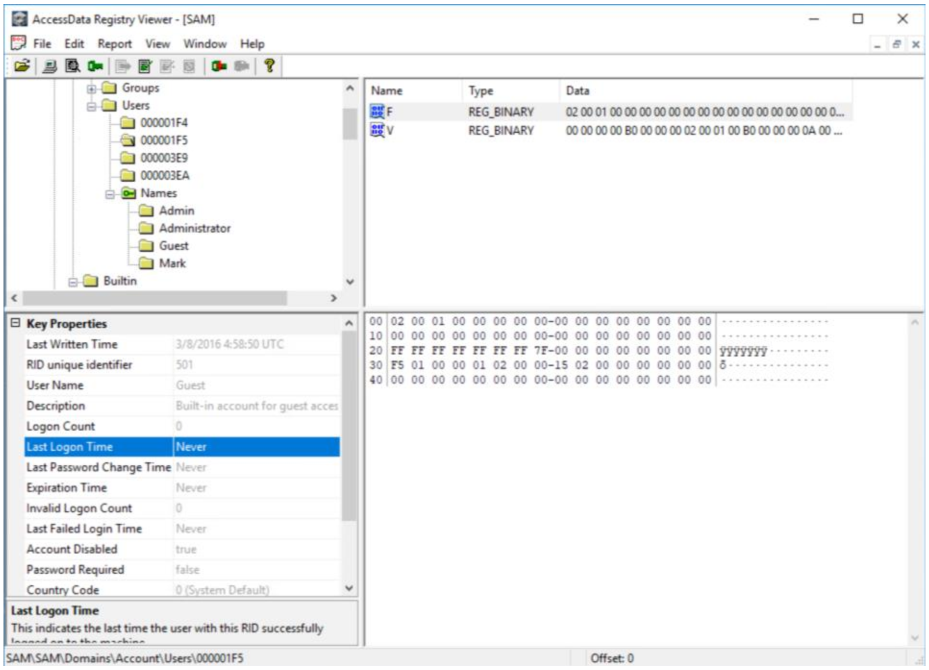
Key Properties	
Last Written Time	3/8/2016 4:40:56 UTC
RID unique identifier	1001
User Name	Mark
Logon Count	3
Last Logon Time	3/8/2016 4:40:56 UTC
Last Password Change Time	3/8/2016 1:59:30 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	«need "SysKey" file»
Country Code	1 (United States)
Hours Allowed	Anytime

Last Password Change Time

The last time the password was changed.

SAM\SAM\Domains\Account\Users\000003E9 Offset: 0

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



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
V	REG_BINARY	00 00 00 00 B0 00 00 00 02 00 01 00 B0 00 00 00 0A 00 ...

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 acces
Logon Count	0
Last Logon Time	Never
Last Password Change Time	Never
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	false
Country Code	0 (System Default)

```
00 02 00 01 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
10 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
20 FF FF FF FF FF FF FF 7F-00 00 00 00 00 00 00 00  ÿÿÿÿÿÿÿ---------
30 F5 01 00 00 01 02 00 00-15 02 00 00 00 00 00 00  õ---------------
40 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ----------------
```

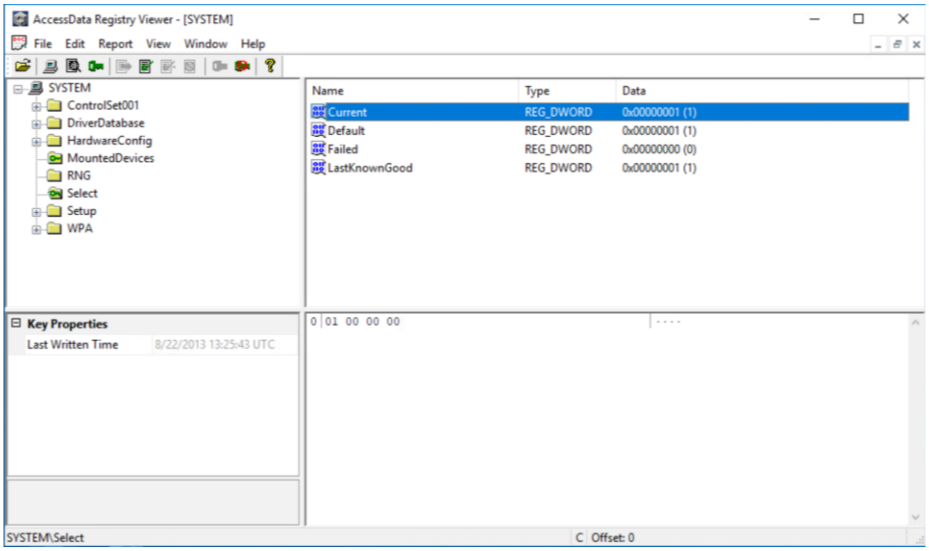
Last Logon Time

This indicates the last time the user with this RID successfully logged on to the machine

SAM\SAM\Domains\Account\Users\000001F5   Offset: 0

2. Examine the SYSTEM registry hive.

Question 4. Click on "Select" and check the value of "Current". What is the current ControlSet? 0 01 00 00 00



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

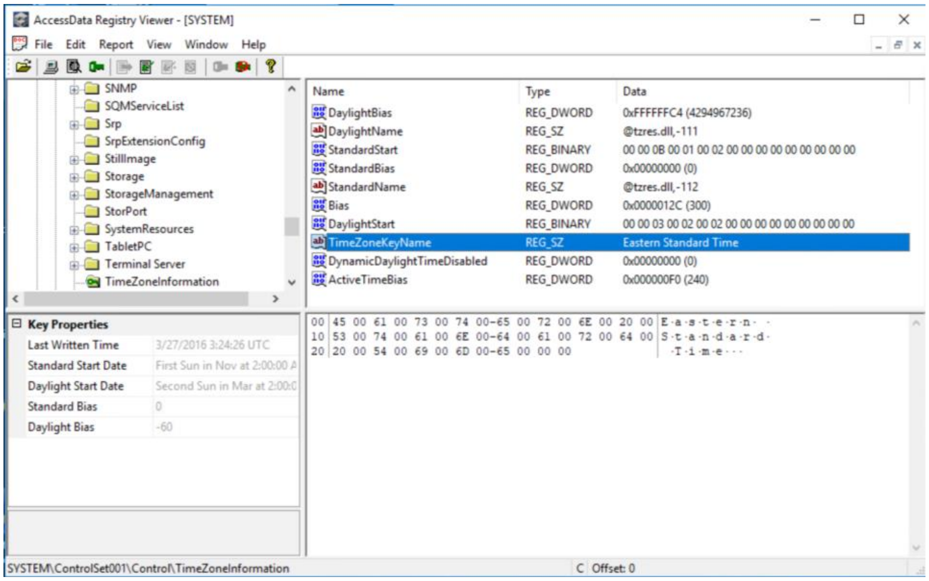
Key Properties

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

```
0 01 00 00 00    ----
```

SYSTEM\Select   C Offset: 0

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



Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
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)

Key Properties	
Last Written Time	3/27/2016 3:24:26 UTC
Standard Start Date	First Sun in Nov at 2:00:00 A
Daylight Start Date	Second Sun in Mar at 2:00:0
Standard Bias	0
Daylight Bias	-60

```
00 45 00 61 00 73 00 74 00-65 00 72 00 6E 00 20 00 E·a·s·t·e·r·n· ·
10 53 00 74 00 61 00 6E 00-64 00 61 00 72 00 64 00 S·t·a·n·d·a·r·d·
20 20 00 54 00 69 00 6D 00-65 00 00 00              ·T·i·m·e···
```

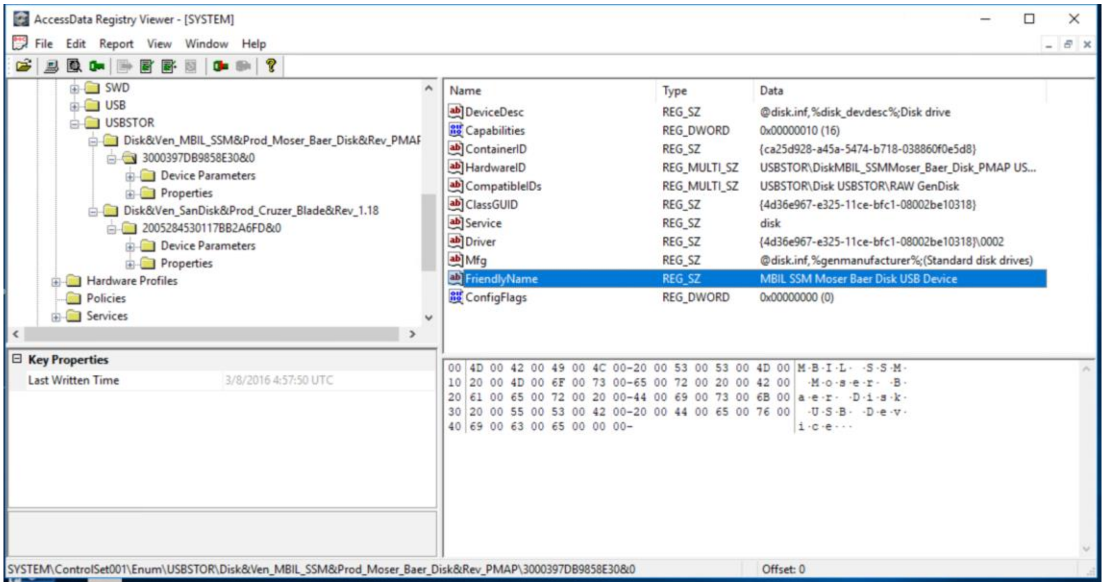
SYSTEM\ControlSet001\Control\TimeZoneInformation C Offset: 0

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”)

There are 2 USB plugged in the system.

The Friendly names:

- MBIL SSM Moser Baer Disk USB Device
- SanDisk Cruzer Blade USB device

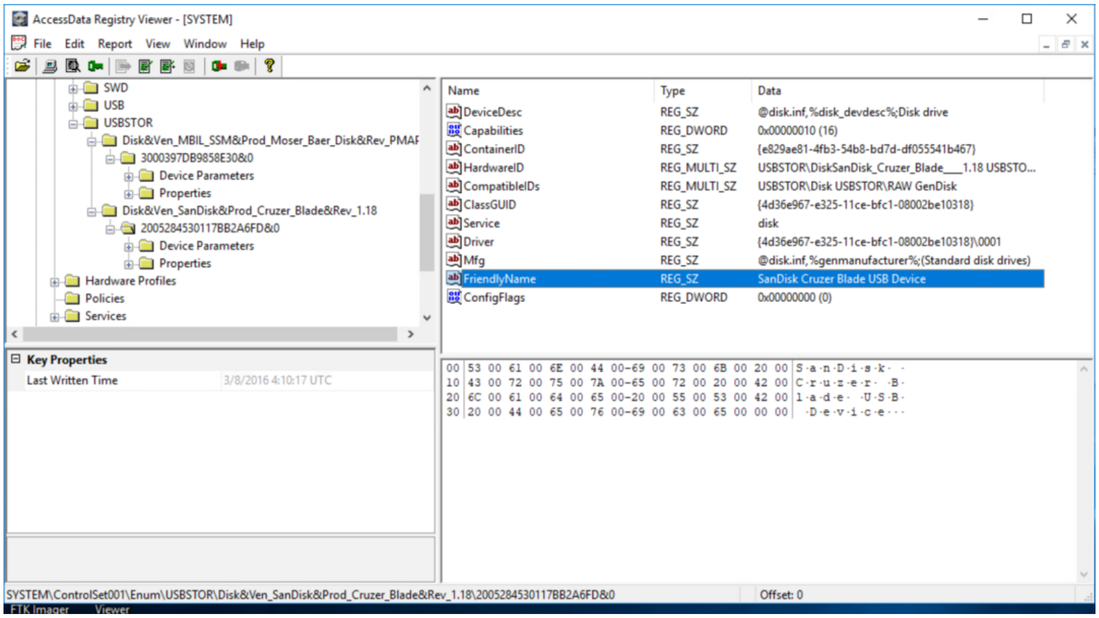

AccessData Registry Viewer - [SYSTEM]
File Edit Report View Window Help
SWD
USB
USBSTOR
Disk&Ven_MBIL_SSM&Prod_Moser_Baer_Disk&Rev_PMAF
3000397DB9858E30&0
Device Parameters
Properties
Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.18
2005284530117BB2A6FD&0
Device Parameters
Properties
Hardware Profiles
Policies
Services

Name	Type	Data
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
ContainerID	REG_SZ	{ca25d928-a45a-5474-b718-038860f0e5d8}
HardwareID	REG_MULTI_SZ	USBSTOR\DiskMBIL_SSMMoser_Baer_Disk_PMAP US...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	REG_SZ	disk
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0002
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
FriendlyName	REG_SZ	MBIL SSM Moser Baer Disk USB Device
ConfigFlags	REG_DWORD	0x00000000 (0)

Key Properties	
Last Written Time	3/8/2016 4:57:50 UTC

```
00 4D 00 42 00 49 00 4C 00-20 00 53 00 53 00 4D 00 M·B·I·L· ·S·S·M·
10 20 00 4D 00 6F 00 73 00-65 00 72 00 20 00 42 00  ·M·o·s·e·r· ·B·
20 61 00 65 00 72 00 20 00-44 00 69 00 73 00 6B 00 a·e·r· ·D·i·s·k·
30 20 00 55 00 53 00 42 00-20 00 44 00 65 00 76 00  ·U·S·B· ·D·e·v·
40 69 00 63 00 65 00 00 00-                         i·c·e···
```

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_MBIL_SSM&Prod_Moser_Baer_Disk&Rev_PMAP\3000397DB9858E30&0 Offset: 0


AccessData Registry Viewer - [SYSTEM]
File Edit Report View Window Help
SWD
USB
USBSTOR
Disk&Ven_MBIL_SSM&Prod_Moser_Baer_Disk&Rev_PMAF
3000397DB9858E30&0
Device Parameters
Properties
Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.18
2005284530117BB2A6FD&0
Device Parameters
Properties
Hardware Profiles
Policies
Services
FTK Imager
Viewer

Name	Type	Data
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
ContainerID	REG_SZ	{e829ae81-4fb3-54b8-bd7d-df055541b467}
HardwareID	REG_MULTI_SZ	USBSTOR\DiskSanDisk_Cruzer_Blade___1.18 USBSTO...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	REG_SZ	disk
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
FriendlyName	REG_SZ	SanDisk Cruzer Blade USB Device
ConfigFlags	REG_DWORD	0x00000000 (0)

Key Properties

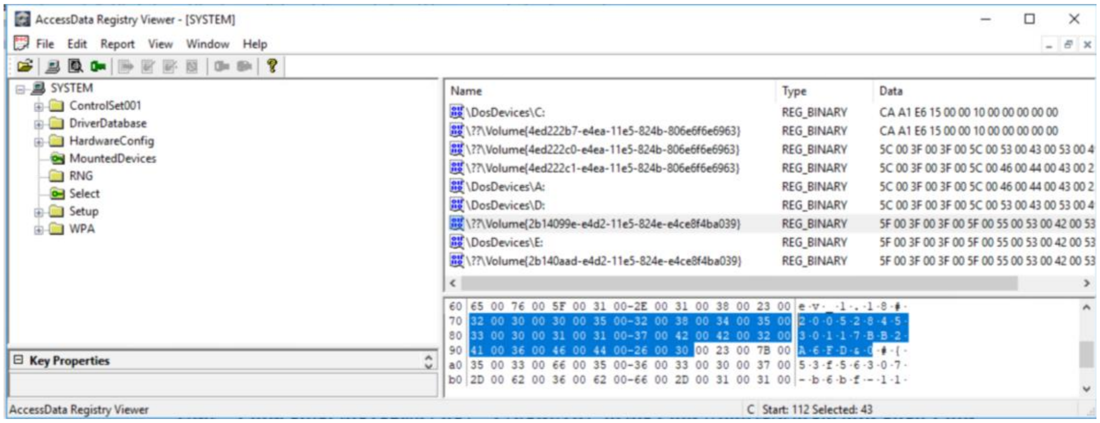
Last Written Time	3/8/2016 4:10:17 UTC

```
00 53 00 61 00 6E 00 44 00-69 00 73 00 6B 00 20 00 S·a·n·D·i·s·k· ·
10 43 00 72 00 75 00 7A 00-65 00 72 00 20 00 42 00 C·r·u·z·e·r· ·B·
20 6C 00 61 00 64 00 65 00-20 00 55 00 53 00 42 00 l·a·d·e· ·U·S·B·
30 20 00 44 00 65 00 76 00-69 00 63 00 65 00 00 00  ·D·e·v·i·c·e···
```

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.18\2005284530117BB2A6FD&0   Offset: 0

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

Volume{2b14099e-e4d2-11e5-824e-e4ce8f4ba039}



Name	Type	Data
\DosDevices\C:	REG_BINARY	CA A1 E6 15 00 00 10 00 00 00 00 00
\??\Volume{4ed222b7-e4ea-11e5-824b-806e6f6e6963}	REG_BINARY	CA A1 E6 15 00 00 10 00 00 00 00 00
\??\Volume{4ed222c0-e4ea-11e5-824b-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 4
\??\Volume{4ed222c1-e4ea-11e5-824b-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 2
\DosDevices\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 2
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 4
\??\Volume{2b14099e-e4d2-11e5-824e-e4ce8f4ba039}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53
\DosDevices\E:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53
\??\Volume{2b140aad-e4d2-11e5-824e-e4ce8f4ba039}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53

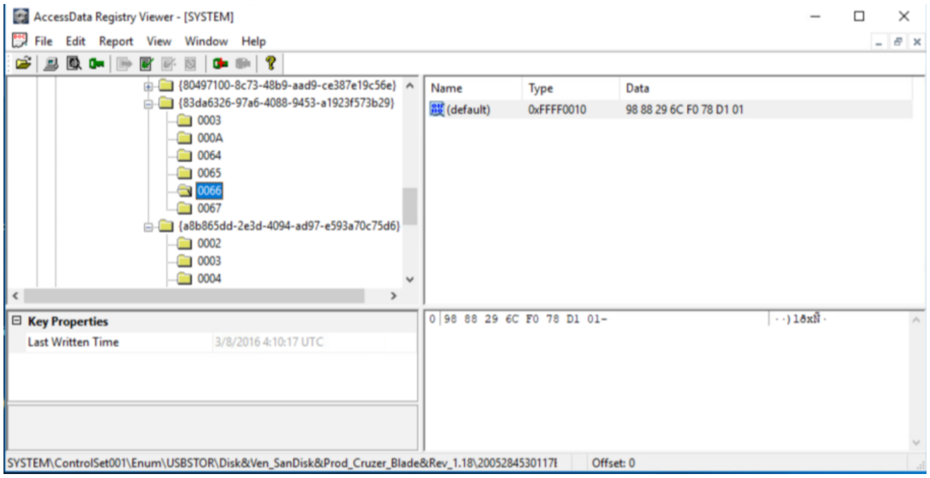
```
60 65 00 76 00 5F 00 31 00-2E 00 31 00 38 00 23 00 e·v·_·1·.·1·8·#·
70 32 00 30 00 30 00 35 00-32 00 38 00 34 00 35 00 2·0·0·5·2·8·4·5·
80 33 00 30 00 31 00 31 00-37 00 42 00 42 00 32 00 3·0·1·1·7·B·B·2·
90 41 00 36 00 46 00 44 00-26 00 30 00 23 00 7B 00 A·6·F·D·&·0·#·{·
a0 35 00 33 00 66 00 35 00-36 00 33 00 30 00 37 00 5·3·f·5·6·3·0·7·
b0 2D 00 62 00 36 00 62 00-66 00 2D 00 31 00 31 00 -·b·6·b·f·-·1·1·
```

AccessData Registry Viewer   C Start: 112 Selected: 43

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: 3/8/2016 4:10:17 UTC

Last removed: 3/8/2016 4:13:12 UTC



```
{80497100-8c73-48b9-aad9-ce387e19c56e}
{83da6326-97a6-4088-9453-a1923f573b29}
    0003
    000A
    0064
    0065
    0066
    0067
{a8b865dd-2e3d-4094-ad97-e593a70c75d6}
    0002
    0003
    0004
```

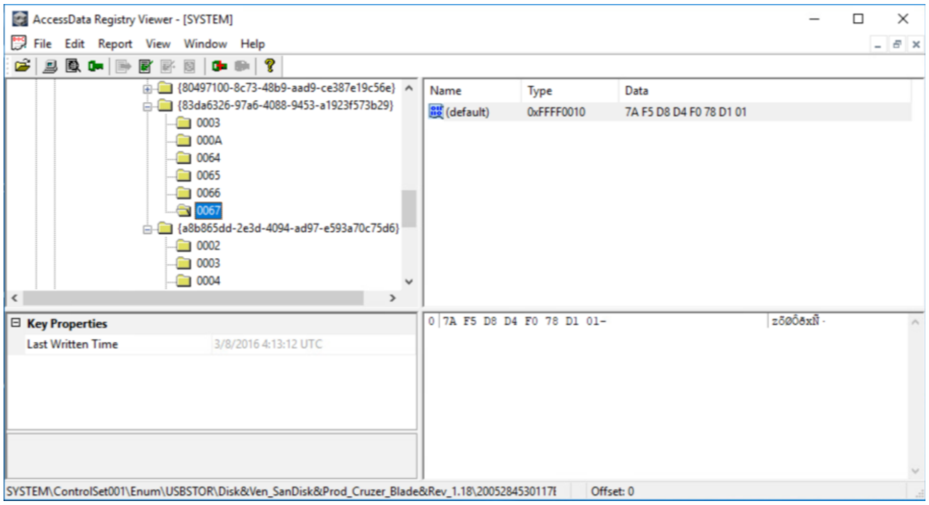
Name	Type	Data
(default)	0xFFFF0010	98 88 29 6C F0 78 D1 01

Key Properties

Last Written Time	3/8/2016 4:10:17 UTC

```
0 98 88 29 6C F0 78 D1 01-                    ··)1ðxÑ·
```

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.18\2005284530117I Offset: 0



```
{80497100-8c73-48b9-aad9-ce387e19c56e}
{83da6326-97a6-4088-9453-a1923f573b29}
    0003
    000A
    0064
    0065
    0066
    0067
{a8b865dd-2e3d-4094-ad97-e593a70c75d6}
    0002
    0003
    0004
```

Name	Type	Data
(default)	0xFFFF0010	7A F5 D8 D4 F0 78 D1 01

Key Properties

Last Written Time	3/8/2016 4:13:12 UTC

```
0 7A F5 D8 D4 F0 78 D1 01-                    zõØÔðxÑ·
```

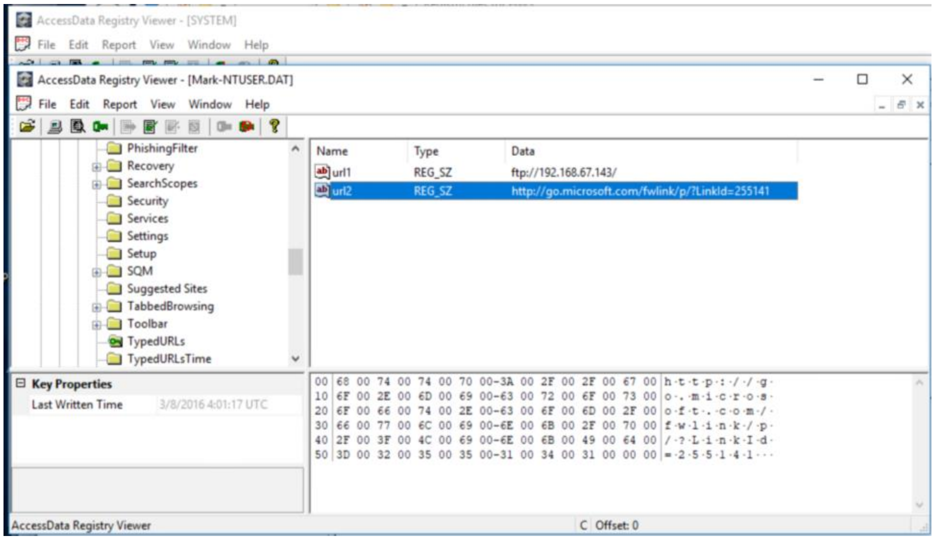
SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.18\2005284530117I Offset: 0

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?

url1:ftp://192.168.67.143

url2: http://go.microsoft.com/fwlink/p/?Linkld=255141


AccessData Registry Viewer - [SYSTEM]
File Edit Report View Window Help
AccessData Registry Viewer - [Mark-NTUSER.DAT]
File Edit Report View Window Help
PhishingFilter
Recovery
SearchScopes
Security
Services
Settings
Setup
SQM
Suggested Sites
TabbedBrowsing
Toolbar
TypedURLs
TypedURLsTime
AccessData Registry Viewer
C Offset: 0

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

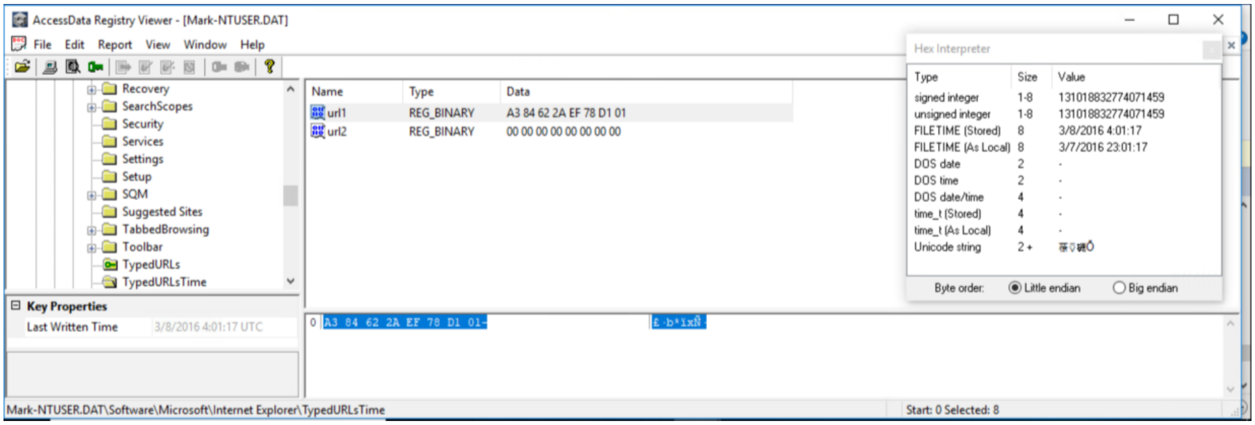
Key Properties

Last Written Time 3/8/2016 4:01:17 UTC

```
00 68 00 74 00 74 00 70 00-3A 00 2F 00 2F 00 67 00 h·t·t·p·:·/·/·g·
10 6F 00 2E 00 6D 00 69 00-63 00 72 00 6F 00 73 00 o·.·m·i·c·r·o·s·
20 6F 00 66 00 74 00 2E 00-63 00 6F 00 6D 00 2F 00 o·f·t·.·c·o·m·/·
30 66 00 77 00 6C 00 69 00-6E 00 6B 00 2F 00 70 00 f·w·l·i·n·k·/·p·
40 2F 00 3F 00 4C 00 69 00-6E 00 6B 00 49 00 64 00 /·?·L·i·n·k·I·d·
50 3D 00 32 00 35 00 35 00-31 00 34 00 31 00 00 00 =·2·5·5·1·4·1···
```

Question 10. Checking the value of "TypedRULsTime", 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.)

3/8/2016 4:01:17 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

Key Properties

Last Written Time 3/8/2016 4:01:17 UTC

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	-
time_t (Stored)	4	-
time_t (As Local)	4	-
Unicode string	2 +	[illegible]

Byte order: ● Little endian ○ Big endian

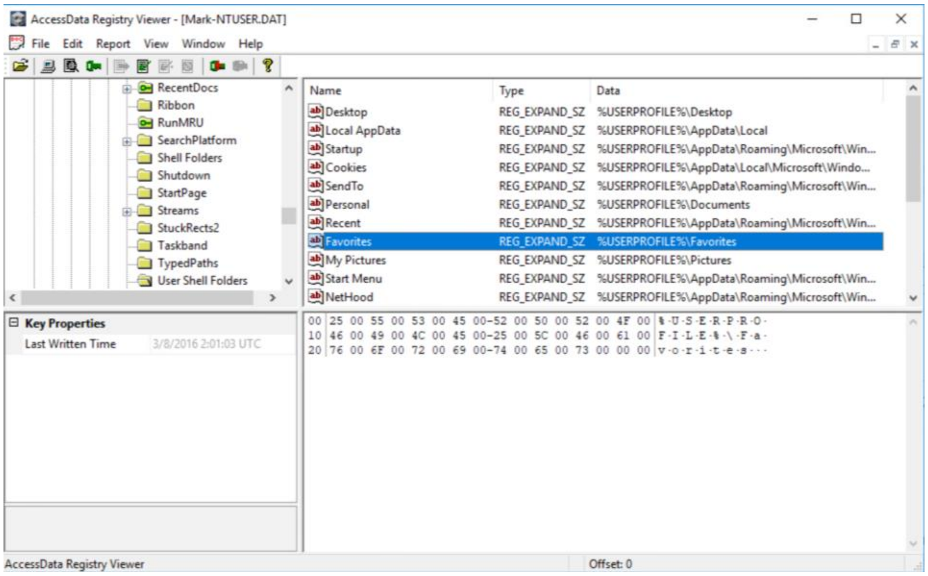
```
0 A3 84 62 2A EF 78 D1 01-          £·b*ïxÑ·
```

Mark-NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLsTime

Start: 0 Selected: 8

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



Name	Type	Data
Desktop	REG_EXPAND_SZ	%USERPROFILE%\Desktop
Local AppData	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local
Startup	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
Cookies	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Microsoft\Windo...
SendTo	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
Personal	REG_EXPAND_SZ	%USERPROFILE%\Documents
Recent	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
Favorites	REG_EXPAND_SZ	%USERPROFILE%\Favorites
My Pictures	REG_EXPAND_SZ	%USERPROFILE%\Pictures
Start Menu	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...
NetHood	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Win...

⊟ Key Properties

Last Written Time 3/8/2016 2:01:03 UTC

```
00 25 00 55 00 53 00 45 00-52 00 50 00 52 00 4F 00 %·U·S·E·R·P·R·O·
10 46 00 49 00 4C 00 45 00-25 00 5C 00 46 00 61 00 F·I·L·E·%·\·F·a·
20 76 00 6F 00 72 00 69 00-74 00 65 00 73 00 00 00 v·o·r·i·t·e·s···
```

ENJOY!