

# CSEC 730 ADVANCED FORENSICS

Name : Shriram Karpoora Sundara Pandian ( KP )

Title : Homework 3

## Part 1 – Using AccessData’s Registry Viewer

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

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

Username is “MARK” and the RID number for mark is 1001

The screenshot displays the AccessData's Registry Viewer interface. The left pane shows the tree structure of the SAM registry hive, expanded to SAM > Domains > Account > Users. The right pane shows a list of registry values for the selected user, including F, V, and ForcePassw... (Force Password Change). The bottom pane shows the key properties for the selected user, including Last Written Time, RID unique identifier, User Name, Logon Count, Last Logon Time, Last Password Change, Expiration Time, Invalid Logon Count, Last Failed Login Time, and Account Disabled. The key properties for the user Mark are as follows:

Property	Value
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
Last Failed Login Time	Never
Account Disabled	false

The bottom pane also shows the last password change time and the last time the password was changed.

The bottom pane also shows a hex dump of the registry data, with the user name "Mark" highlighted in blue.

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

From Below we can see that the Last date and time the Mark changed the password is “ 2016-03-08 and 01:59:30 “

000001F5

000003E9

000003EA

Names

iltin

uUpgrade

3/8/2016 4:40:56 UTC

fier1001

Mark

3

3/8/2016 4:40:56 UTC

ange3/8/2016 1:59:30 UTC

Never

unt0

TimeNever

False

ge Time

sword was changed.

00	02	00	01	00	00	00	00	00	00	1E	18	48	B4	F4	78	D1	01	.....H'ôxN'
10	00	00	00	00	00	00	00	00	00	C6	A5	0B	27	DE	78	D1	01	.....EY' 'BxN'
20	00	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	00	00	00	00	01	00	E4	04	00	é.....ä
40	00	00	03	00	01	00	00	00	00	00	00	00	00	00	00	00	00	.....

Checking the

DCode v5.5

FileToolsThemeHelp

Time DecodingTime Encoding

Name	Timestamp
Apple Absolute Time (UTC)	2001-01-01 00:00:00.000000
Apple Absolute Time	2000-12-31 19:00:00.000000
Apple Absolute Time (ns) (UTC)	2005-02-25 10:05:59.703602
Apple Absolute Time (ns)	2005-02-25 05:05:59.703602
Chromium Time Microseconds (UTC)	5752-10-26 19:55:03.602630
Chromium Time Microseconds	5752-10-26 15:55:03.602630
Microsoft Ticks (Local)	0416-03-08 01:59:30.360263
OLE Automation (64-bit) (Local)	1899-12-30 00:00:00.000000
Unix Microseconds (UTC)	6121-10-26 19:55:03.602630
Unix Microseconds	6121-10-26 15:55:03.602630
→ Windows Filetime (UTC)	2016-03-08 01:59:30.360263
Windows Filetime	2016-03-07 20:59:30.360263

Value Input

FormatHexadecimal (Little-Endian)

ValueC6A50B27DE78D101

Decode

Time Zone

Name(UTC-05:00) Eastern Time (US & Canada)

No AdjustmentSelect

Date Output

Patternyyyy'-MM'-'dd HH':'mm':'ss'.ffffff

Sample2024-03-22 16:50:21.530555

Default

www.digitaldetective.net

elp

quest

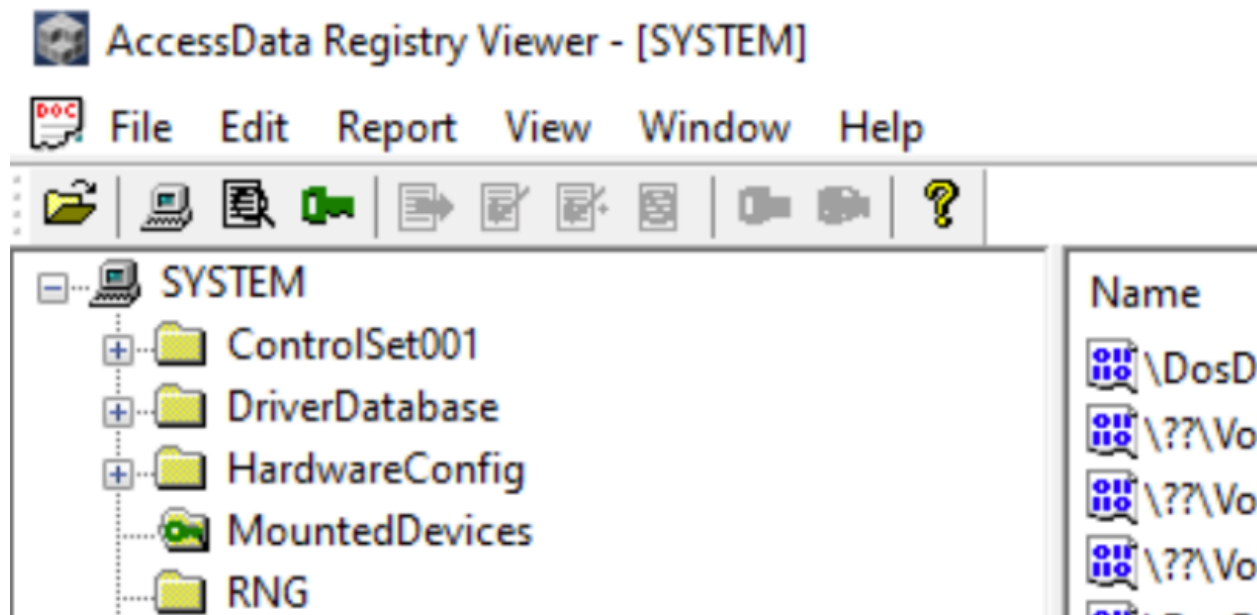
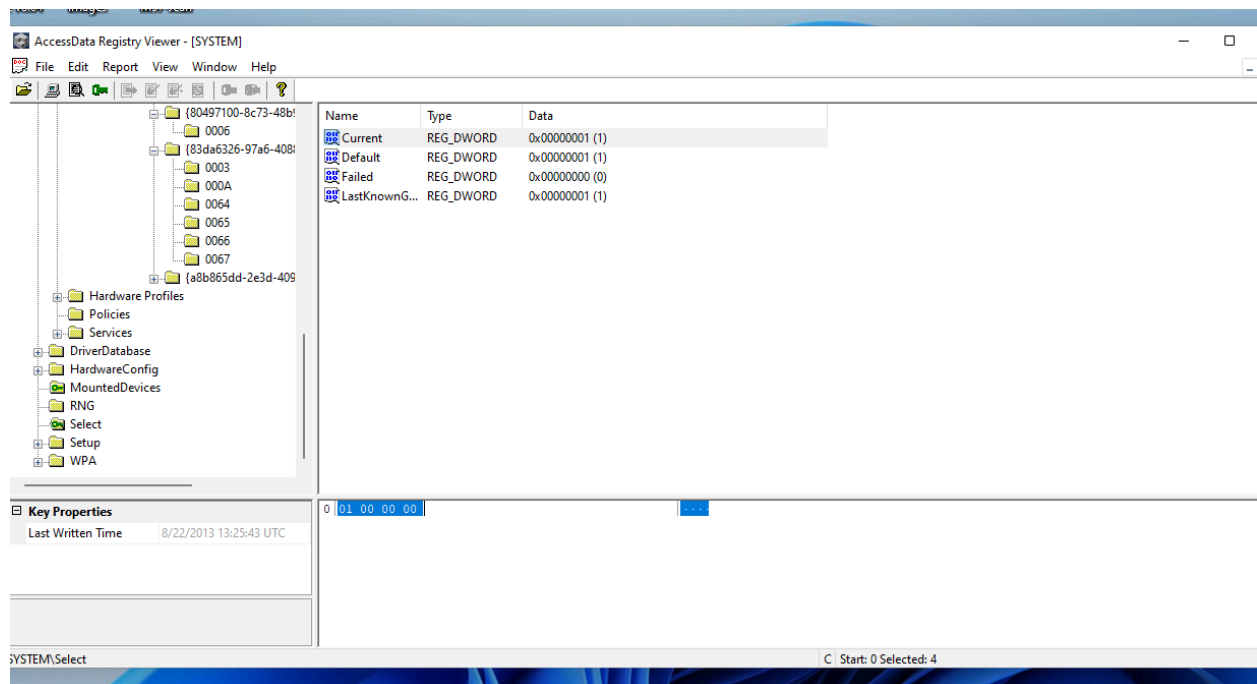
**Last Written Time**  
This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT).

The screenshot shows the Windows Security Center interface. On the left, the 'Users' section is expanded, showing a list of users: '000001F4', '000001F5', '000003E9', '000003EA', and 'Names'. The 'Names' user is selected, showing details: 'Built-in', 'Guest', 'Built-in account for guest', and 'Never' expiration. The 'Users' list on the left also shows 'Guest' as a built-in user.

From the above screenshot, we can see the username is “Guest Built-in account for guest access to the computer / domain “. Never logged on, we can confirm that from the screenshot above.

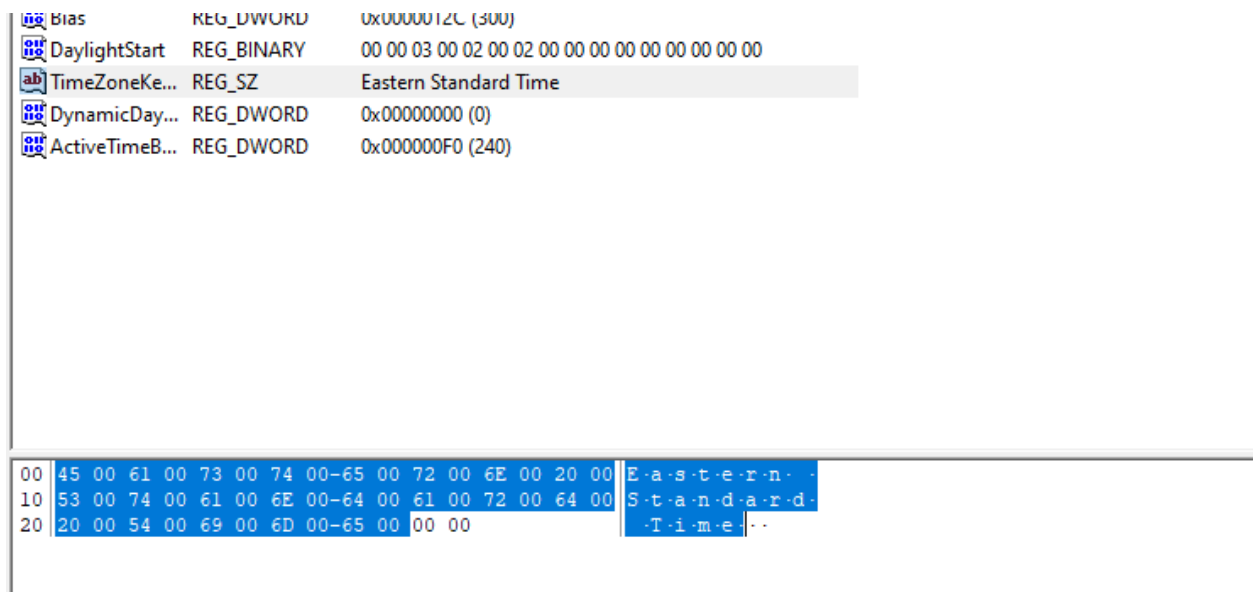
**Question 4. Click on “Select” and check the value of “Current”. What is the current control set?**

The hex values say 01 00 00 00, which means decimal 1, which is ControlSet001 in current use. Also, the second screenshot supports my statement.



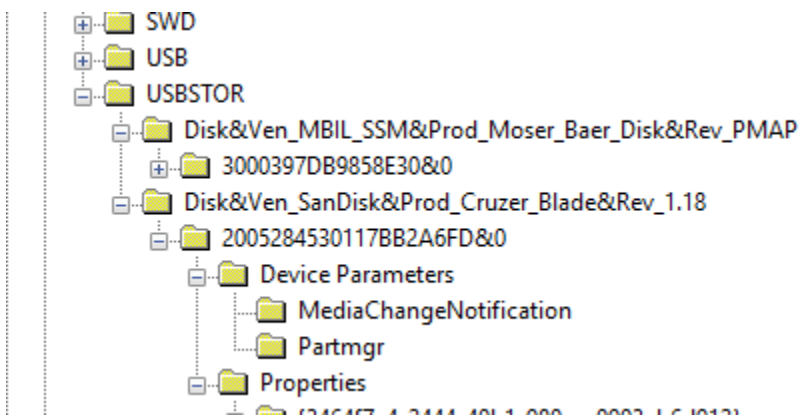
**Question 5. Click ControlSet001 and search for “TimeZone” via “Edit>Find...”  
What is the TimeZoneKeyName?**

Eastern Standard Time



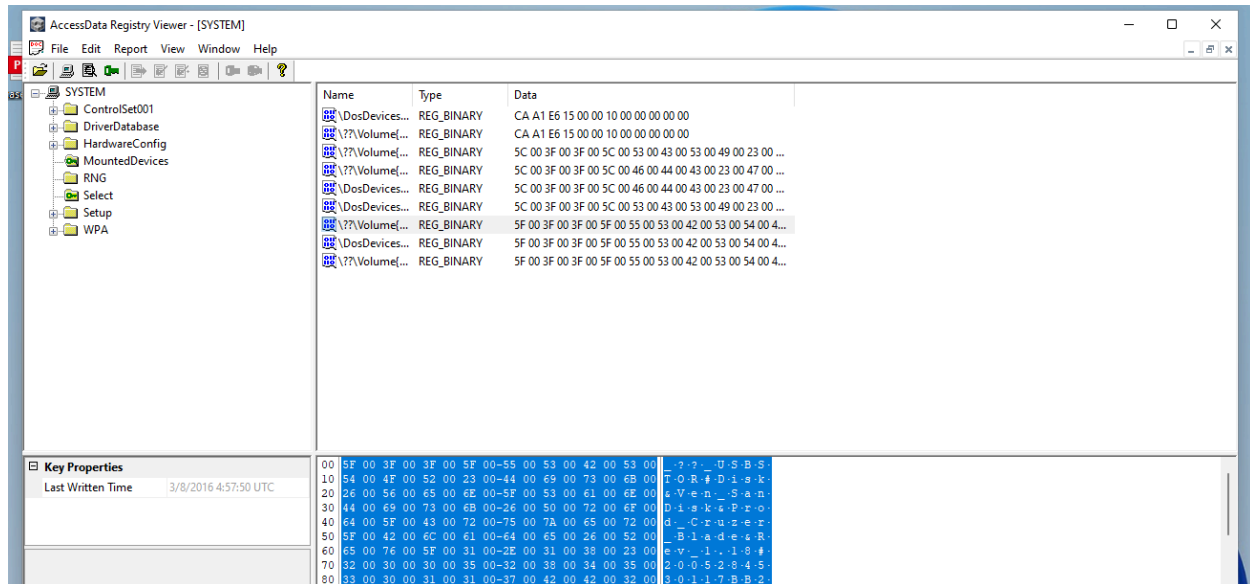
**Question 6. Expand ControlSet001>Enum>USBSTOR. How many USBs were plugged into the system and what are the USB’s friendly names? (Hint: expand each device entry and click on the unique instance ID, for example “2005284530117BB2A6FD&0”)**

We have two entries below under USBSTOR, Moser\_Baer and Cruzer\_Blade.

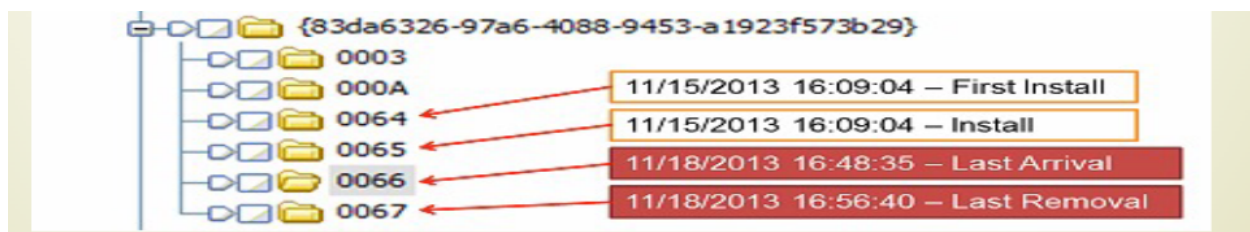


**Question 7. Select SYSTEM> MountedDevices. Search the USB instance ID “2005284530117BB2A6FD&0.” Which Windows Volume had this USB device mounted to?**

We can see from the screenshot below that is USBSTOR and the Disk name is Cruzer Blade.



**Question 8.** When was the USB with the instance ID of “2005284530117BB2A6FD&0” last inserted into the system, and when was it last removed? (Hint: See Registry Lecture PowerPoint slides)



From the slides, I understood that 0067 says about the last inserted time and 0068 says about last removed

Below is hex values of 0066 and its time values and we can see the time is 04:10:17

AccessData Registry Viewer - [SYSTEM]

File Edit Report View Window Help

MediaChangeNotification  
Partmgr  
Properties  
(3464f7a4-2444-40b1-980a-e0)  
000A  
(540b947e-8b40-45bc-a8a2-6)  
0004  
0007  
(80497100-8c73-48b9-aad9-c)  
0006  
(83da6326-97a6-4088-9453-a1)  
0003  
000A  
0064  
0065  
0066  
0067  
(a8b865dd-2e3d-4094-ad97-e

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- 16x3

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_SanDisk&Prod\_Cruzer\_Blade&Rev\_1.18\{2005284530117BB2A6FD&0}\Properties\83

DCode v5.5

File Tools Theme Help

Time Decoding Time Encoding

Name	Timestamp
Apple Absolute Time (UTC)	2001-01-01 00:00:00.000 Z
Apple Absolute Time	2000-12-31 19:00:00.000 -05:00
Apple Absolute Time (ns) (UTC)	2005-02-25 10:07:18.172 Z
Apple Absolute Time (ns)	2005-02-25 05:07:18.172 -05:00
Chromium Time Microseconds (UTC)	5752-10-27 17:42:52.600 Z
Chromium Time Microseconds	5752-10-27 13:42:52.600 -04:00
Microsoft Ticks (Local)	0416-03-08 04:10:17.260
OLE Automation (64-bit) (Local)	1899-12-30 00:00:00.000
Unix Microseconds (UTC)	6121-10-27 17:42:52.600 Z
Unix Microseconds	6121-10-27 13:42:52.600 -04:00
Windows Filetime (UTC)	2016-03-08 04:10:17.260 Z
Windows Filetime	2016-03-07 23:10:17.260 -05:00

Value Input  
Format Hexadecimal (Little-Endian)  
Value 9888296CF078D101  
Decode

Time Zone  
Name (UTC-05:00) Eastern Time (US & Canada)  
No Adjustment Select

Date Output  
Pattern yyyy'-MM'-'dd HH':'mm':'ss'.fff K  
Sample 2024-03-22 16:12:01.236 -04:00  
Default



Below is hex of 0067 and its time values, it says removed it 04:13:12.

AccessData Registry Viewer - [SYSTEM]

File Edit Report View Window Help

MediaChangeNotification  
Partmgr  
Properties  
{34647a4-2444-40b1-980a-e0  
000A  
{540b947e-8b40-45bc-a8a2-6  
0004  
0007  
{80497100-8c73-48b9-aad9-cr  
0006  
{83da6326-97a6-4088-9453-a1  
0003  
000A  
0064  
0065  
0066  
0067  
{a8b865dd-2e3d-4094-ad97-e

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

DCode v5.5

File Tools Theme Help

Time Decoding Time Encoding

Name	Timestamp
Apple Absolute Time (UTC)	2001-01-01 00:00:00.000 Z
Apple Absolute Time	2000-12-31 19:00:00.000 -05:00
Apple Absolute Time (ns) (UTC)	2005-02-25 10:07:19.928 Z
Apple Absolute Time (ns)	2005-02-25 05:07:19.928 -05:00
Chromium Time Microseconds (UTC)	5752-10-27 18:12:08.927 Z
Chromium Time Microseconds	5752-10-27 14:12:08.927 -04:00
Microsoft Ticks (Local)	0416-03-08 04:13:12.892
OLE Automation (64-bit) (Local)	1899-12-30 00:00:00.000
Unix Microseconds (UTC)	6121-10-27 18:12:08.927 Z
Unix Microseconds	6121-10-27 14:12:08.927 -04:00
Windows Filetime (UTC)	2016-03-08 04:13:12.892 Z
Windows Filetime	2016-03-07 23:13:12.892 -05:00

Value Input

Format Hexadecimal (Little-Endian)

Value 7AF5D8D4F078D101

Decode

Time Zone

Name (UTC-05:00) Eastern Time (US & Canada)

No Adjustment Select

Date Output

Pattern yyyy'-MM'-'dd HH':'mm':'ss'.fff K

Sample 2024-03-22 16:12:01.236 -04:00

These are two URL Mark visited “ Url1 and Url2 “

AccessData Registry Viewer - [Mark-NTUSER.DAT]

File Edit Report View Window Help

IntelliForms  
 International  
 InternetRegistry  
 LinksBar  
 LowRegistry  
 Main  
 MINIE  
 New Windows  
 PageSetup  
 PhishingFilter  
 Recovery  
 SearchScopes  
 Security  
 Services  
 Settings  
 Setup  
 SQM  
 Suggested Sites  
 TabbedBrowsing  
 Toolbar  
 TypedURLs

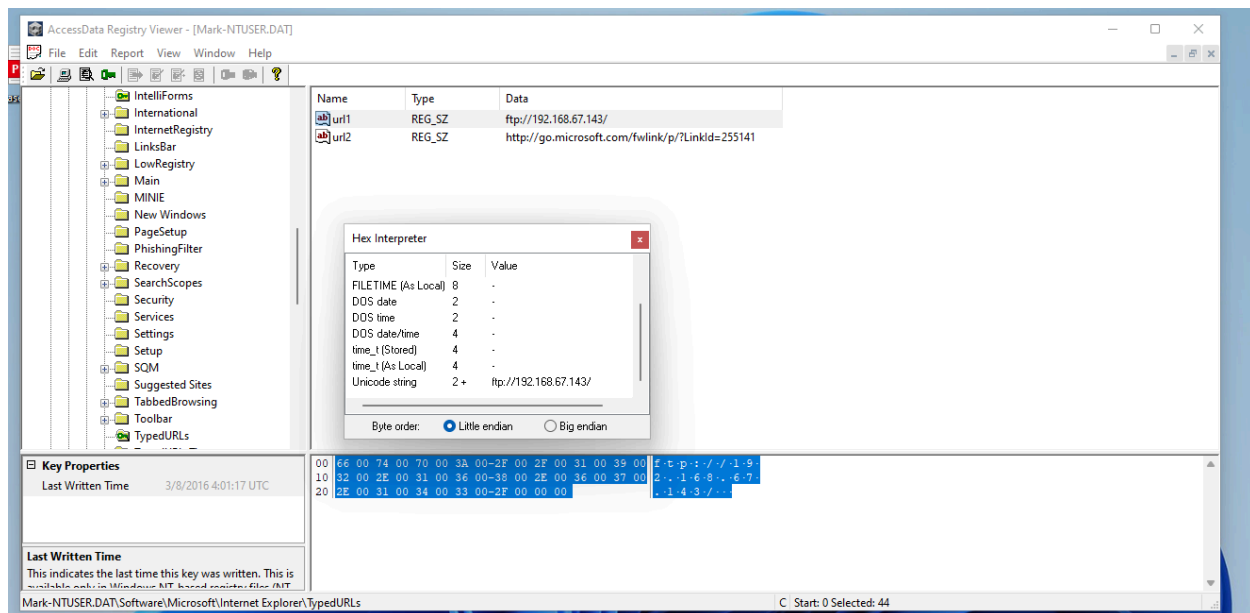
Name	Type	Data
url1	REG_SZ	ftp://192.168.67.143/
url2	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

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

00 66 00 74 00 70 00 3A 00-2F 00 2F 00 31 00 39 00 f . t . p : / . / . 1 . 9 .  
 10 32 00 2E 00 31 00 36 00-38 00 2E 00 36 00 37 00 2 . . . 1 . 6 . 8 . . . 6 . 7 .  
 20 2E 00 31 00 34 00 33 00-2F 00 00 00 . . 1 . 4 . 3 . / . . .

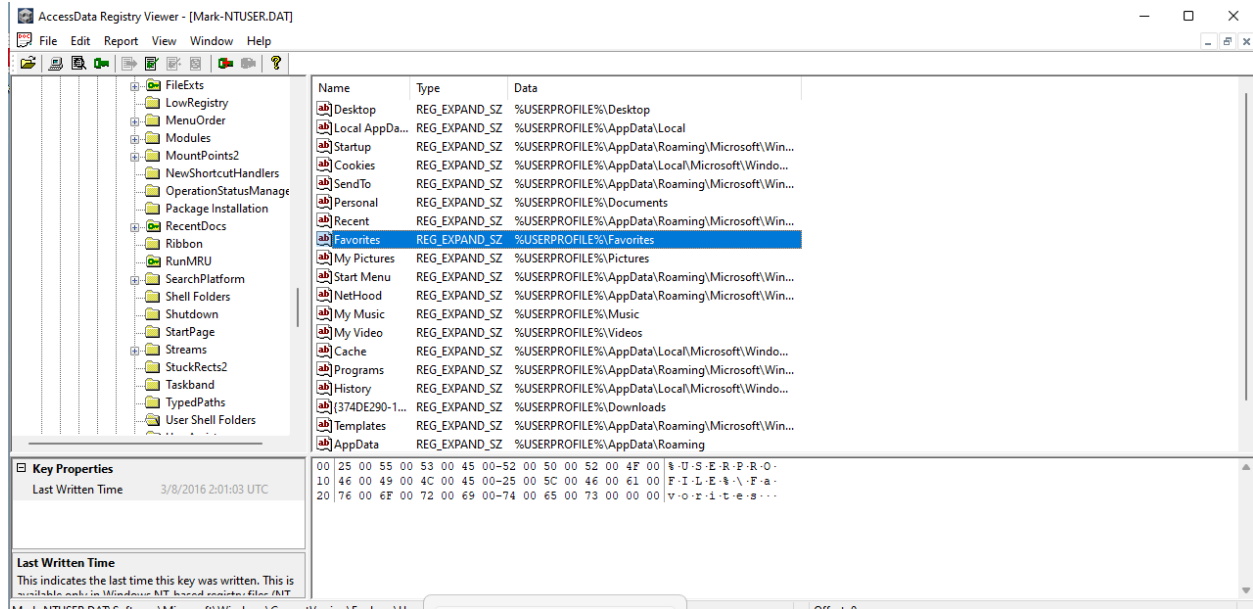
**Question 10. Checking the value of “TypedRULsTime”, when were the last date and time that Mark visited ftp://192.168.67.143? (Hint: the date and time are shown in the key properties pane. It can also be determined by selecting the data in hex at the right bottom pane, right-clicking, and using the “Show Hex Interpreter Window...” function.**

From the Key Properties window we can it is “04:01:17”



**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?**

From the screenshot below %USERPROFILE%\Favorites



## Part 2 – Using RegRipper 3.0

I unzipped the RegRipper3.0 and added this file to my Registry folder to do the analysis.

Below to show the available plugins in RegRipper.

```
C:\Users\Student\Downloads\RegRipper3.0-master\RegRipper3.0-master>rip.exe -l
1. adobe v.20200522 [NTUSER.DAT]
   - Gets user's Adobe app cRecentFiles values
2. allowedenum v.20200511 [NTUSER.DAT, Software]
   - Extracts AllowedEnumeration values to determine hidden special folders
3. amcache v.20200515 [amcache]
   - Parse AmCache.hve file
4. amcache_tln v.20180311 [amcache]
   - Parse AmCache.hve file
5. appassoc v.20200515 [NTUSER.DAT]
   - Gets contents of user's ApplicationAssociationToasts key
6. appcertdlls v.20200427 [System]
   - Get entries from AppCertDlls key
7. appcompatcache v.20220921 [System]
   - Parse files from System hive AppCompatCache
8. appcompatcache_tln v.20220921 [System]
   - Parse files from System hive AppCompatCache
9. appcompatflags v.20200525 [NTUSER.DAT, Software]
   - Extracts AppCompatFlags for Windows.
10. appinitdlls v.20200427 [Software]
```

```
C:\Windows\System32\cmd.exe
245. winscp v.20201227 [NTUSER.DAT]
   - Gets user's WinSCP 2 data
246. winver v.20200525 [Software]
   - Get Windows version & build info
247. winzip v.20200526 [NTUSER.DAT]
   - Get WinZip extract and filemenu values
248. wordwheelquery v.20200823 [NTUSER.DAT]
   - Gets contents of user's WordWheelQuery key
249. wordwheelquery_tln v.20200824 [NTUSER.DAT]
   - Gets contents of user's WordWheelQuery key
250. wow64 v.20200515 [Software]
   - Gets contents of WOW64\x86 key
251. wpdbusenum v.20200515 [System]
   - Get WpdBusEnum subkey info
252. wsh_settings v.20200517 [Software]
   - Gets WSH Settings

C:\Users\Student\Downloads\RegRipper3.0-master\RegRipper3.0-master>
```

1. This Plugin is used to get the info about the USB that may be recorded on the registry and we got some information about the USBs

```
C:\Windows\System32\cmd.exe
C:\Users\Student\Desktop\Registry files for HW3>rip.exe -r SYSTEM -p usb v.20200515
Launching usb v.20200515
usb v.20200515
(System) Get USB key info

USBStor
ControlSet001\Enum\USB

ROOT_HUB [2016-03-08 04:57:55Z]
S/N: 5&17df1c1b&0 [2016-03-08 02:05:04Z]
Properties Key LastWrite: 2016-03-08 02:01:36Z
First InstallDate : 2016-03-08 04:57:55Z
InstallDate : 2016-03-08 04:57:55Z
Last Arrival : 2016-03-08 02:05:04Z

ROOT_HUB20 [2016-03-08 04:57:54Z]
S/N: 5&25f23b66&0 [2016-03-08 02:05:04Z]
Properties Key LastWrite: 2016-03-08 02:01:36Z
ParentIdPrefix: 6&34c6b45e&0
First InstallDate : 2016-03-08 04:57:54Z
InstallDate : 2016-03-08 04:57:54Z
Last Arrival : 2016-03-08 02:05:04Z

ROOT_HUB30 [2016-03-08 04:57:54Z]
S/N: 5&da8887e&0&0 [2016-03-08 02:05:04Z]
Properties Key LastWrite: 2016-03-08 02:05:10Z
ParentIdPrefix: 6&201153c1&0
First InstallDate : 2016-03-08 04:57:54Z
InstallDate : 2016-03-08 04:57:54Z
Last Arrival : 2016-03-08 02:05:04Z
```

```
C:\Windows\System32\cmd.exe
VID_0E0F&PID_0002 [2016-03-08 04:57:55Z]
S/N: 6&201153c1&0&7 [2016-03-08 04:13:12Z]
Properties Key LastWrite: 2016-03-08 02:05:10Z
ParentIdPrefix: 7&208e3713&0
First InstallDate : 2016-03-08 04:57:55Z
InstallDate : 2016-03-08 04:57:55Z
Last Arrival : 2016-03-08 02:05:04Z
S/N: 6&201153c1&0&8 [2016-03-08 02:05:05Z]
Properties Key LastWrite: 2016-03-08 02:05:09Z
First InstallDate : 2016-03-08 04:57:55Z
InstallDate : 2016-03-08 04:57:55Z
Last Arrival : 2016-03-08 02:05:05Z

VID_0E0F&PID_0003 [2016-03-08 04:57:54Z]
S/N: 6&201153c1&0&5 [2016-03-08 02:05:05Z]
Properties Key LastWrite: 2016-03-08 02:05:09Z
ParentIdPrefix: 7&2a0405e8&0
First InstallDate : 2016-03-08 04:57:54Z
InstallDate : 2016-03-08 04:57:54Z
Last Arrival : 2016-03-08 02:05:05Z

VID_0E0F&PID_0003&MI_00 [2016-03-08 04:57:54Z]
S/N: 7&2a0405e8&0&0000 [2016-03-08 02:05:05Z]
Properties Key LastWrite: 2016-03-08 02:05:09Z
ParentIdPrefix: 8&211f5361&0
First InstallDate : 2016-03-08 04:57:54Z
InstallDate : 2016-03-08 04:57:54Z
Last Arrival : 2016-03-08 02:05:05Z

VID_0E0F&PID_0003&MI_01 [2016-03-08 04:57:55Z]
```

2. This plugin works on NTUSER.DAT file and gets information about the user assisting software that has been used, which is sometimes crucial for the analysis.

```
C:\Windows\System32\cmd.exe

C:\Users\Student\Desktop\Registry files for HW3>rip.exe -r Mark-NTUSER.DAT -p userassist v.20170204
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2016-03-08 03:27:39Z

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}
2016-03-08 04:38:52Z
    set_2747713814_en-us (1)

Value names with no time stamps:
    UEME_CTLCUACount:ctor

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2016-03-08 04:40:35Z
    Microsoft.Windows.Desktop (2)
2016-03-08 04:39:14Z
    windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel (1)
2016-03-08 04:11:13Z
    {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (1)

2016-03-08 04:40:35Z
    Microsoft.Windows.Desktop (2)
2016-03-08 04:39:14Z
    windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel (1)
2016-03-08 04:11:13Z
    {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (1)
2016-03-08 04:07:54Z
    Microsoft.InternetExplorer.Default (3)
2016-03-08 04:06:07Z
    {6D809377-6AF0-444B-8957-A3773F02200E}\Windows NT\Accessories\WORDPAD.EXE (2)

Value names with no time stamps:
    UEME_CTLCUACount:ctor
    {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\OpenWith.exe
    Microsoft.Windows.Explorer
    Microsoft.Windows.Shell.RunDialog
    Microsoft.Windows.ControlPanel

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
2016-03-08 04:40:35Z
    {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Desktop.lnk (2)
2016-03-08 04:07:54Z
    {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Internet Explorer.lnk (3)

Value names with no time stamps:
    UEME_CTLCUACount:ctor

{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}
```

3. SYSTEM will be used by this plugin and gets the timezone information that we already saw in Part 1 which is Eastern Standard Time, Sometimes knowing the location would be useful and crucial while analysing the time and dates.

```
C:\Users\Student\Desktop\Registry files for HW3>Registry files for HW3>rip.exe -r SYSTEM -p timezone v.20200518
Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2016-03-27 03:24:26Z
DaylightName -> @tzres.dll,-111
StandardName -> @tzres.dll,-112
Bias -> 300 (5 hours)
ActiveTimeBias -> 240 (4 hours)
TimeZoneKeyName-> Eastern Standard Time
```

4. This screenshot has lot of information because, it shows all the services registered in the registry, svc v.20200525

```
C:\Users\Student\Desktop\Registry files for HW3>Registry files for HW3>rip.exe -r SYSTEM -p svc v.20200525
Launching svc v.20200525
svc v.20200525
(System) Lists Services key contents by LastWrite time (CSV)

Time,Name,DisplayName,ImagePath\ServiceDll,Type,Start,ObjectName
2016-03-27 03:24:26Z,BITS,@SystemRoot\System32\qmgr.dll,1,1000,SystemRoot\System32\svchost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem,@SystemRoot\System32\qmgr.dll,-1001
2016-03-08 04:58:25Z,(BfAC15CE-A7A6-4B84-BDCE-1F415A5F2C54),,,,,@SystemRoot\System32\wuansvc.dll,-250
2016-03-08 04:58:22Z,drmkaud,@hdaudio.inf;\XdmkAud.SvcDesc\Microsoft Trusted Audio Drivers,SystemRoot\System32\drivers\drmkaud.sys,Kernel driver,Manual,,@SystemRoot\System32\dps.dll,-501
2016-03-08 04:58:21Z,MSKSSrv,@ksfilter.inf;\MSKSSRV.DeviceDesc\Microsoft Streaming Service Proxy,SystemRoot\System32\drivers\MSKSSRV.sys,Kernel driver,Manual,,@SystemRoot\System32\KeyboardFilterSvc.dll,-102
2016-03-08 04:58:21Z,MSPCLOCK,@ksfilter.inf;\MSPCLOCK.DeviceDesc\Microsoft Streaming Clock Proxy,SystemRoot\System32\drivers\MSPCLOCK.sys,Kernel driver,Manual,,@C:\Windows\System32\DRIVERS\msl1dp.sys,-201
2016-03-08 04:58:21Z,MSPQM,@ksfilter.inf;\MSPQM.DeviceDesc\Microsoft Streaming Quality Manager Proxy,SystemRoot\System32\drivers\MSPQM.sys,Kernel driver,Manual,,@C:\Windows\System32\DRIVERS\msl1dp.sys,-201
2016-03-08 04:58:21Z,MSTEE,@ksfilter.inf;\MSTEE.DeviceDesc\Microsoft Streaming Tee/Sink-to-Sink Converter,SystemRoot\System32\drivers\MSTEE.sys,Kernel driver,Manual,,@C:\Windows\System32\DRIVERS\msl1dp.sys,-201
2016-03-08 04:58:19Z,BTHPORT,@bth.inf;\BTHPORT.SvcDesc\Bluetooth Port Driver,SystemRoot\System32\Drivers\BTHport.sys,Kernel driver,Manual,,@bthpan.inf;\BthPan.DisplayName\Bluetooth Device (Personal Area Networ
k)
2016-03-08 04:58:16Z,(211f1c30-8473-4FES-AB7F-BD67472D0FB3),,,,,@SystemRoot\System32\wuansvc.dll,-250
2016-03-08 04:57:54Z,Share,System32\Drivers\Share.sys,Kernel driver,Boot Start,,
2016-03-08 04:57:54Z,ADP80XX,system32\drivers\ADP80XX.SYS,Kernel driver,Boot Start,,
2016-03-08 04:57:54Z,agp440,@machine.inf;\Agp440.SvcDesc\Intel AGP Bus Filter,system32\drivers\agp440.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\afd.sys,-1000
2016-03-08 04:57:54Z,amdatsa,system32\drivers\amdatsa.sys,Kernel driver,Boot Start,,@SystemRoot\System32\alg.exe,-113
2016-03-08 04:57:54Z,amdsb,system32\drivers\amdsb.sys,Kernel driver,Boot Start,,@SystemRoot\System32\alg.exe,-113
2016-03-08 04:57:54Z,amdatsa,system32\drivers\amdatsa.sys,Kernel driver,Boot Start,,@SystemRoot\System32\alg.exe,-113
2016-03-08 04:57:54Z,arcscas,@arcscas.inf;\Arcscas_ServiceName\Adaptec SAS/SATA-II RAID Storport's Miniport Driver,system32\drivers\arcscas.sys,Kernel driver,Boot Start,,@SystemRoot\System32\appxdeploymentserver.d
ll,-2
2016-03-08 04:57:54Z,b06bdrv,@netbvbda.inf;\Vbd_srv_desc\Broadcom NetXtreme II VBD,system32\drivers\bvbda.sys,Kernel driver,Boot Start,,@SystemRoot\System32\AxInstSV.dll,-104
2016-03-08 04:57:54Z,ebrdrv,@netvbda.inf;\Vbd_srv_desc\Broadcom NetXtreme II 10 GbE VBD,system32\drivers\evbda.sys,Kernel driver,Boot Start,,@SystemRoot\System32\leapsvc.dll,-2
2016-03-08 04:57:54Z,EhStorTcgDrv,@ehstorctgdrv.inf;\EhStorTcgDrv.Desc\Microsoft driver for storage devices supporting IEEE 1667 and TCG protocols,system32\drivers\EhStorTcgDrv.sys,Kernel driver,Boot Start,,@Sys
temRoot\System32\drivers\EhStorClass.sys,-101
2016-03-08 04:57:54Z,gagp30kx,@machine.inf;\Gagp30kx.SvcDesc\Microsoft Generic AGPv3.0 Filter for KB Processor Platforms,system32\drivers\gagp30kx.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\lve
vol.sys,-100
2016-03-08 04:57:54Z,hpsAMD,system32\drivers\hpsAMD.sys,Kernel driver,Boot Start,,@SystemRoot\System32\provsvc.dll,-101
2016-03-08 04:57:54Z,iaStorAV,@iaStorAV.inf;\iaStorAV.DeviceDesc\Intel(R) SATA RAID Controller Windows,system32\drivers\iaStorAV.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\hwpolicy.sys,-102
2016-03-08 04:57:54Z,iaStorV,@iaStorV.inf;\XMP00000.DeviceDesc\Intel RAID Controller Windows 7,system32\drivers\iaStorV.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\hwpolicy.sys,-102
2016-03-08 04:57:54Z,iasnpp,system32\drivers\iasnpp.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\lrenum.sys,-101
2016-03-08 04:57:54Z,lsl_sas2,system32\drivers\lsl_sas2.sys,Kernel driver,Boot Start,,@SystemRoot\System32\lmhsvc.dll,-102
2016-03-08 04:57:54Z,lsl_sas3,system32\drivers\lsl_sas3.sys,Kernel driver,Boot Start,,@SystemRoot\System32\lmhsvc.dll,-102
2016-03-08 04:57:54Z,lsl_sss,system32\drivers\lsl_sss.sys,Kernel driver,Boot Start,,@SystemRoot\System32\lmhsvc.dll,-102
2016-03-08 04:57:54Z,megasas,system32\drivers\megasas.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\luafv.sys,-101
2016-03-08 04:57:54Z,megasr,system32\drivers\megasr.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\luafv.sys,-101
2016-03-08 04:57:54Z,mvumi,system32\drivers\mvumi.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\mup.sys,-102
2016-03-08 04:57:54Z,nvraid,system32\drivers\nvraid.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\ntiproxy.sys,-1
2016-03-08 04:57:54Z,nvstor,system32\drivers\nvstor.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\ntiproxy.sys,-1
2016-03-08 04:57:54Z,nv_agn,@machine.inf;\Aggnwidia.SvcDesc\NVIDIA nforce AGP Bus Filter,system32\drivers\nv_agn.sys,Kernel driver,Boot Start,,@SystemRoot\System32\drivers\ntiproxy.sys,-1
2016-03-08 04:57:54Z,pclide,system32\drivers\pclide.sys,Kernel driver,Boot Start,,@SystemRoot\System32\pcasvc.dll,-2
2016-03-08 04:57:54Z,pcmcia,system32\drivers\pcmcia.sys,Kernel driver,Boot Start,,@SystemRoot\System32\pcasvc.dll,-2
2016-03-08 04:57:54Z,sbp2port,@sbp2.inf;\Sbp2_ServiceDesc\SBP-2 Transport/Protocol Bus Driver,system32\drivers\sbp2port.sys,Kernel driver,Boot Start,,@SystemRoot\System32\samsrv.dll,-2
2016-03-08 04:57:54Z,s1sRaid2,system32\drivers\s1sRaid2.sys,Kernel driver,Boot Start,,@SystemRoot\System32\shsvcs.dll,-12289
2016-03-08 04:57:54Z,s1sRaid4,system32\drivers\s1sRaid4.sys,Kernel driver,Boot Start,,@SystemRoot\System32\shsvcs.dll,-12289
2016-03-08 04:57:54Z,stexstor,system32\drivers\stexstor.sys,Kernel driver,Boot Start,,@SystemRoot\System32\stspvc.dll,-201
2016-03-08 04:57:54Z,storflt,@SystemRoot\System32\vmstorfltn.dll,-1000,system32\DRIVERS\vmstorflt.sys,Kernel driver,Boot Start,,@SystemRoot\System32\wlaservc.dll,-10
2016-03-08 04:57:54Z,stornmme,@stornmme.inf;\StorNMME.ServiceDesc\Microsoft Standard NM Express Driver,system32\drivers\stornmme.sys,Kernel driver,Boot Start,,@SystemRoot\System32\wlaservc.dll,-10
```



5. All the dynamically linked libraries can be analysed and displayed through this plugin, which also shows about the services that uses the .dll files in a location ( system ).

```
C:\Users\Student\Desktop\Registry files for HW3\Registry files for HW3>rip.exe -r SYSTEM -p svcdll v.20200525
Launching svcdll v.20200525
svcdll v.20200525
(System) Lists Services keys with ServiceDll values

2016-03-27 03:24:49Z
BITS -> %SystemRoot%\System32\qmgr.dll

2016-03-08 02:04:17Z
wuauerv -> %systemroot%\system32\wuaueng.dll

2016-03-08 02:01:39Z
PrintNotify -> C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll

2013-08-22 19:11:29Z
AppMgmt -> %SystemRoot%\System32\appmgmts.dll
CscService -> %SystemRoot%\System32\cscsvc.dll
MsKeyboardFilter -> %SystemRoot%\System32\KeyboardFilterSvc.dll
PeerDistSvc -> %SystemRoot%\system32\peerdistsvc.dll
SensrSvc -> %SystemRoot%\system32\sensrsvc.dll
UmRdpService -> %SystemRoot%\System32\umrdp.dll

2013-08-22 15:39:37Z
AudioEndpointBuilder -> %SystemRoot%\System32\AudioEndpointBuilder.dll
Audiosrv -> %SystemRoot%\System32\Audiosrv.dll
MMCSS -> %SystemRoot%\system32\mmcscs.dll
SSDPSSRV -> %SystemRoot%\System32\ssdpsrv.dll
upnphost -> %SystemRoot%\System32\upnphost.dll

2013-08-22 15:37:10Z
AeLookupSvc -> %SystemRoot%\System32\aelupsvc.dll
AppIDSvc -> %SystemRoot%\System32\appidsvc.dll
AppInfo -> %SystemRoot%\System32\appinfo.dll
AppReadiness -> %SystemRoot%\system32\AppReadiness.dll
AppXSvc -> %SystemRoot%\system32\appxdeploymentservice.dll
AxInstSV -> %SystemRoot%\System32\AxInstSV.dll
BDESVC -> %SystemRoot%\System32\bdesvc.dll
BFE -> %SystemRoot%\System32\bfe.dll
BrokerInfrastructure -> %SystemRoot%\System32\bisrv.dll
Browser -> %SystemRoot%\System32\browser.dll
bthserv -> %SystemRoot%\system32\bthserv.dll
CertPropSvc -> %SystemRoot%\System32\certprop.dll
CryptSvc -> %SystemRoot%\system32\cryptsvc.dll
DcomLaunch -> %SystemRoot%\system32\rpcss.dll
defragsvc -> %SystemRoot%\System32\defragsvc.dll
DeviceAssociationService -> %SystemRoot%\system32\das.dll
DeviceInstall -> %SystemRoot%\system32\umprpmgr.dll
Dnscache -> %SystemRoot%\System32\dnscache.dll
dot3svc -> %SystemRoot%\System32\dot3svc.dll
DPS -> %SystemRoot%\system32\dps.dll
DsmSvc -> %SystemRoot%\System32\DeviceSetupManager.dll
Eaphost -> %SystemRoot%\System32\l2cap.dll
```

6. This is a simple yet important plugin that shows the shutdown time and last write time of the machine, which is very crucial evidence.

```
C:\Users\Student\Desktop\Registry files for HW3\Registry files for HW3>rip.exe -r SYSTEM -p shutdown v.20200518
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2016-03-08 02:04:39Z
ShutdownTime : 2016-03-08 02:04:39Z
```

Overall RegRipper is a great tool with more than 200 plugins to get the information about the registry. Also, its plugins work on different registry hives accordingly like some plugin work on SYSTEM and some on NTUSER.DAT.