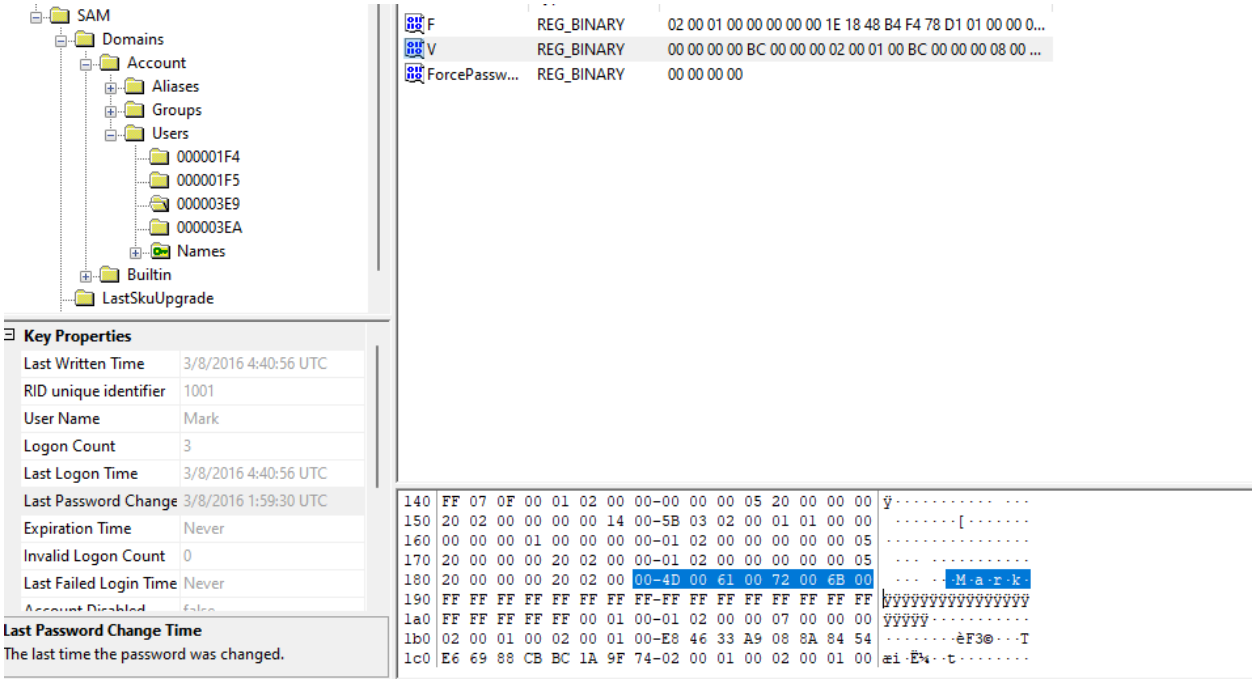
CSEC 730 ADVANCED FORENSICS

Name : Shriram Karpoora Sundara Pandian (KP)

Title : Homework 3

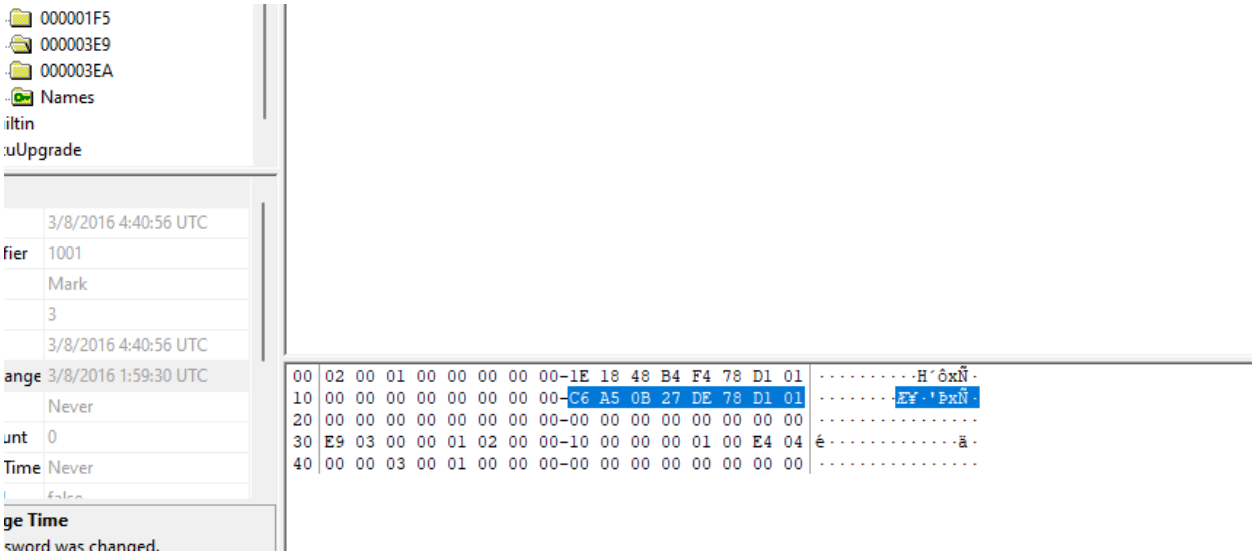
Part 1 – Using AccessData's Registry Viewer

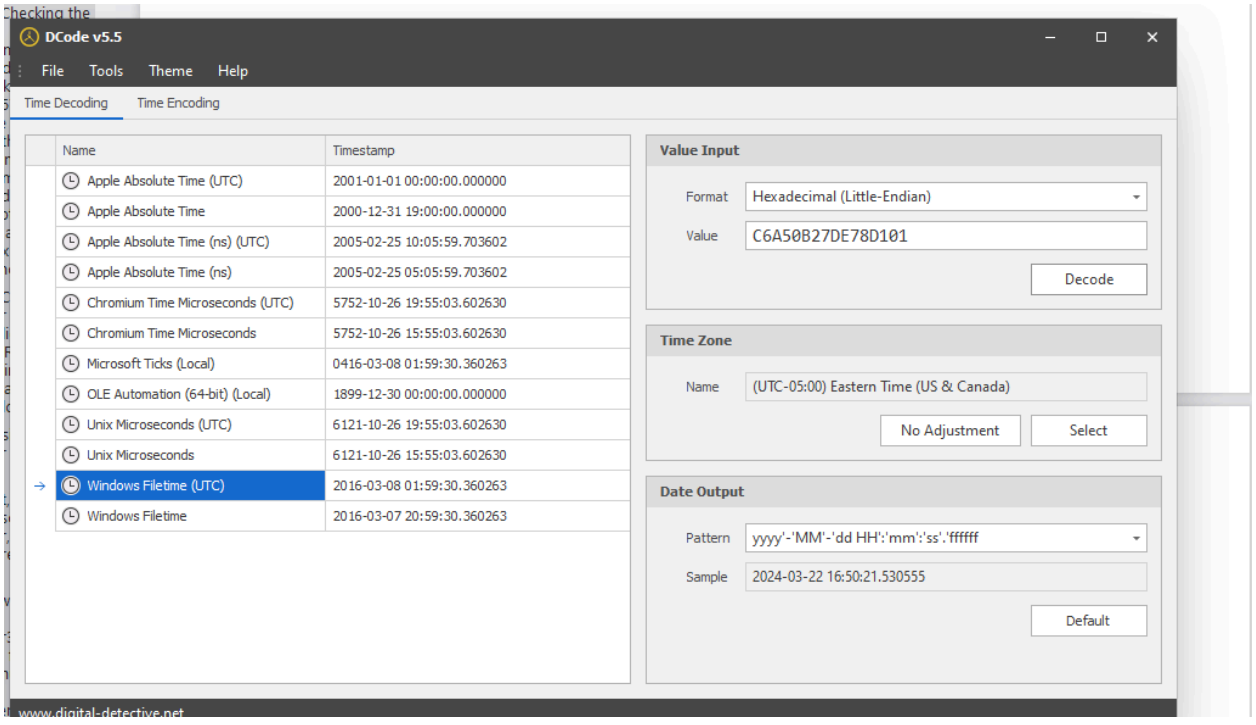
1. Examine the SAM registry hive by expanding SAM>Domains>Account>Users.
Question 1. Which user name and RID number logged onto the system on 3/8/2016 at
4:40:56 UTC?
Username is "MARK" and the RID number for mark is 1001



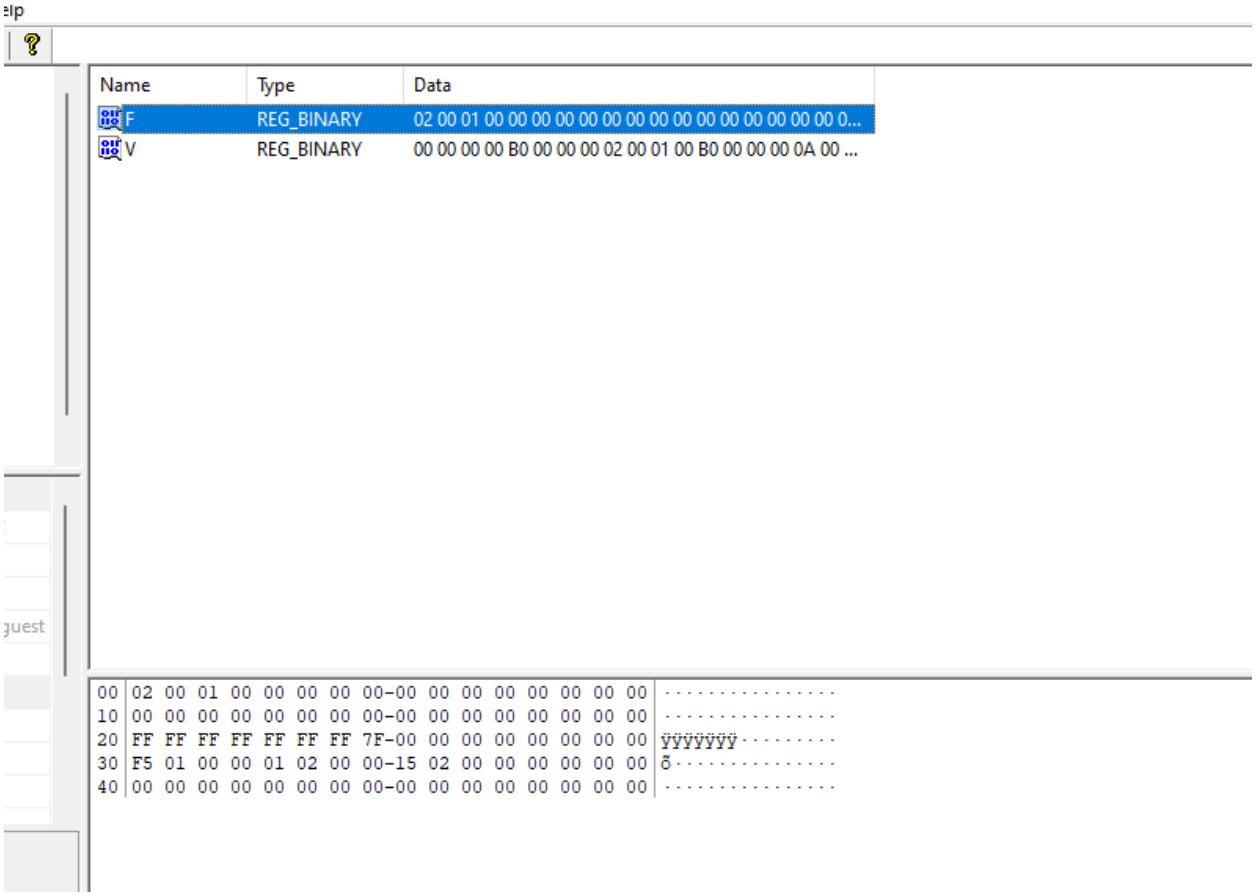
Question 2. When was the last date and time that Mark changed his Windows password?

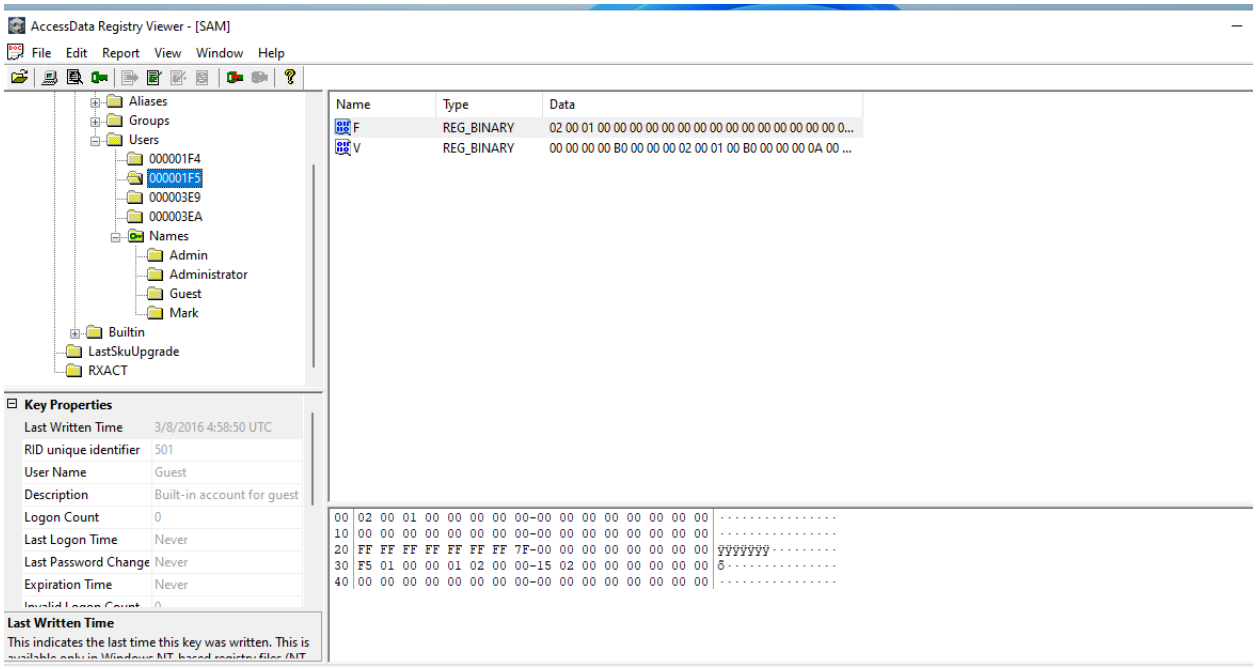
From Below we can see that the Last date and time the Mark changed the password is “ 2016-03-08 and 01:59:30 “

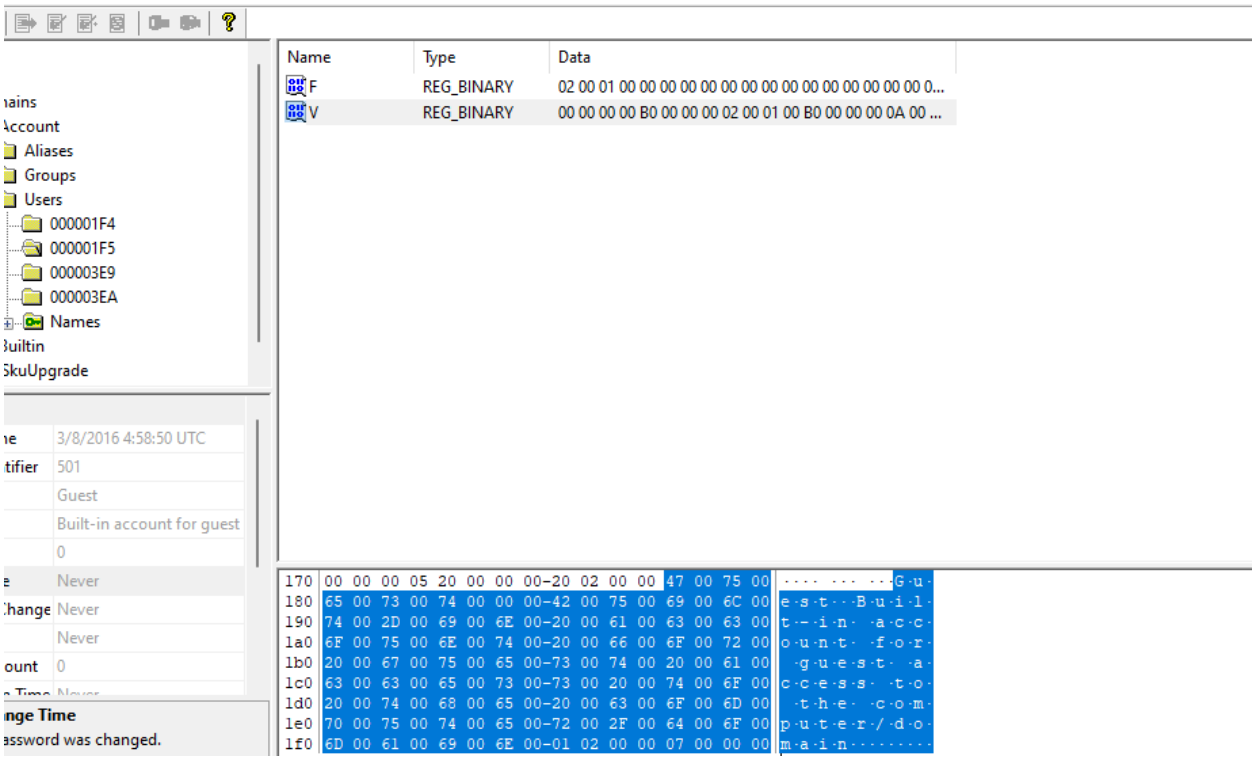




Question 3. Who has never logged onto this Windows system?



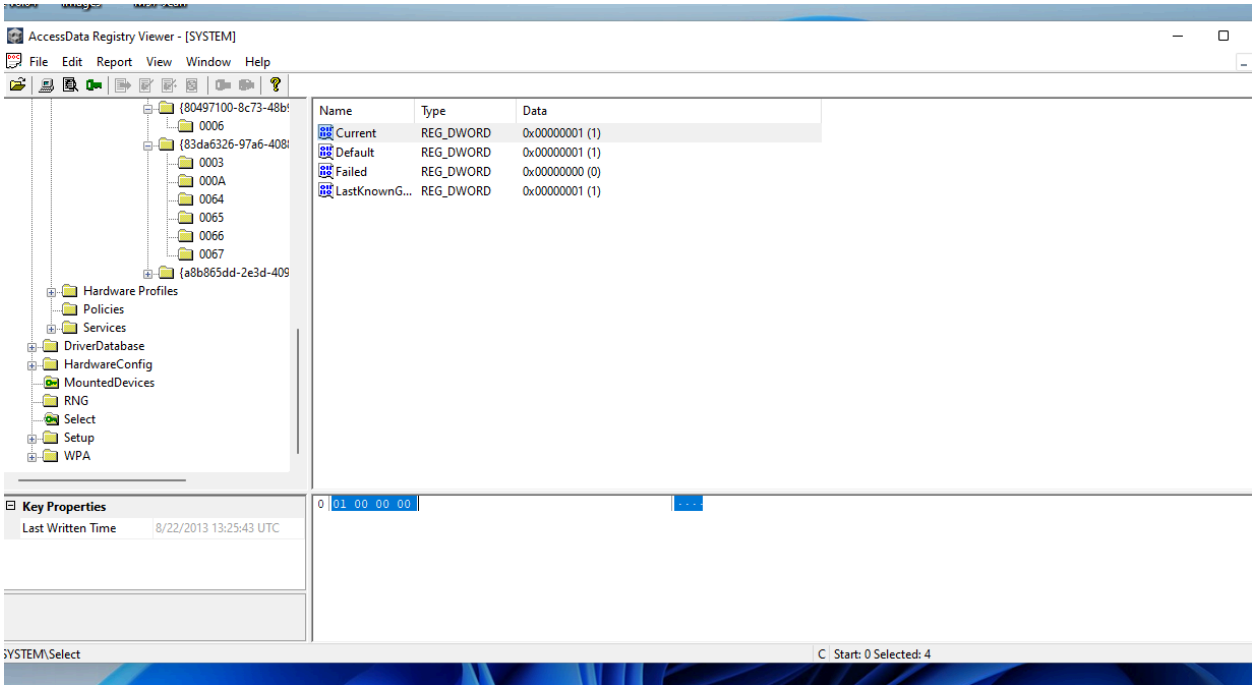


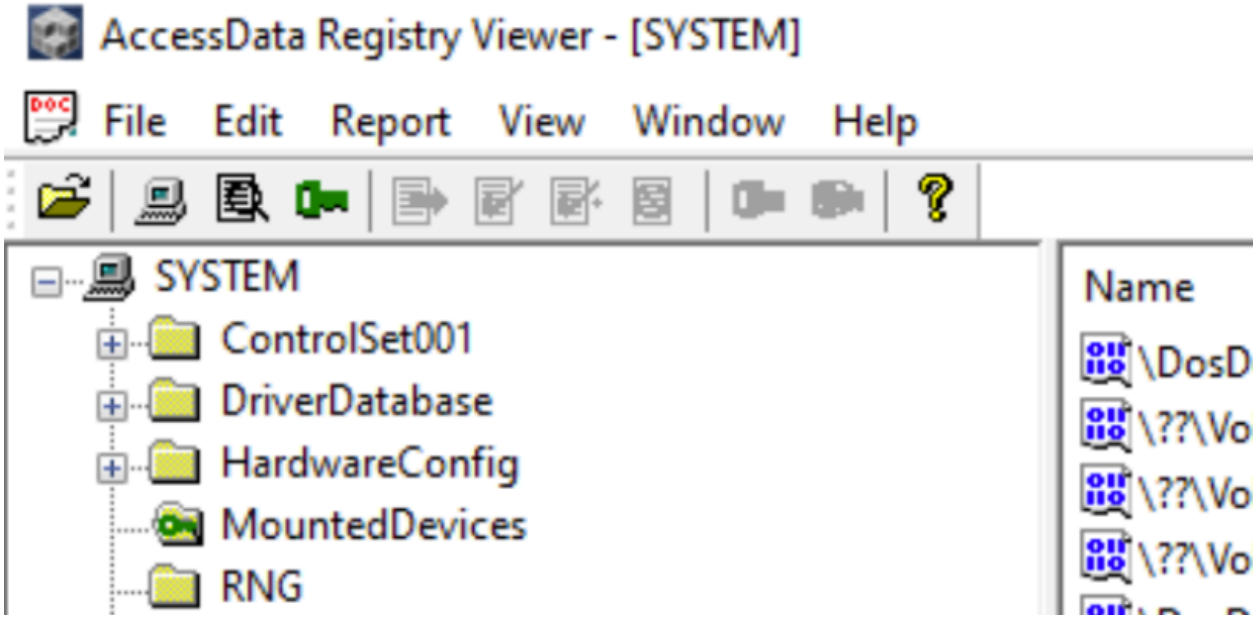


From the above screenshot, we can see the username is “Guest Built-in account for guest access to the computer / domain “. Never logged on, we can confirm that from the screenshot above.

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

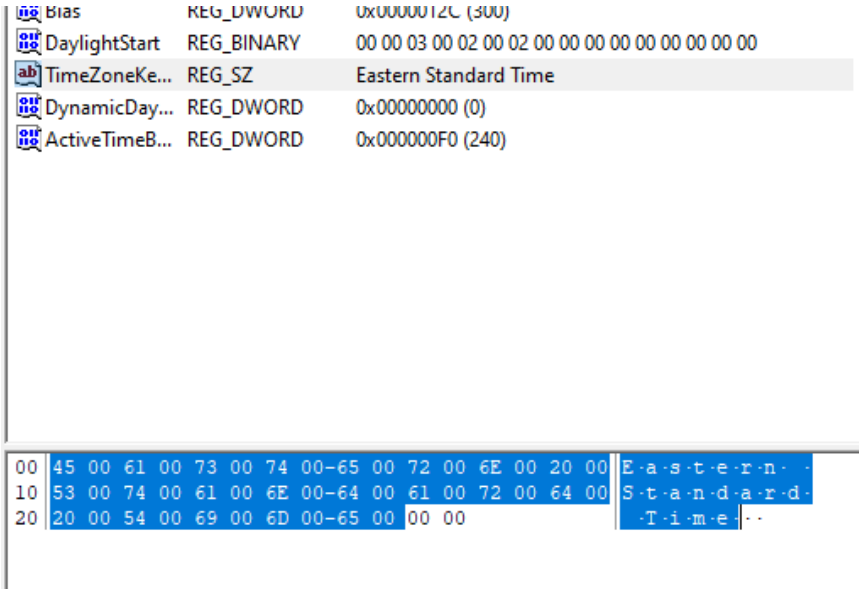
The hex values say 01 00 00 00, which means decimal 1, which is ControlSet001 in current use. Also, the second screenshot supports my statement.





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

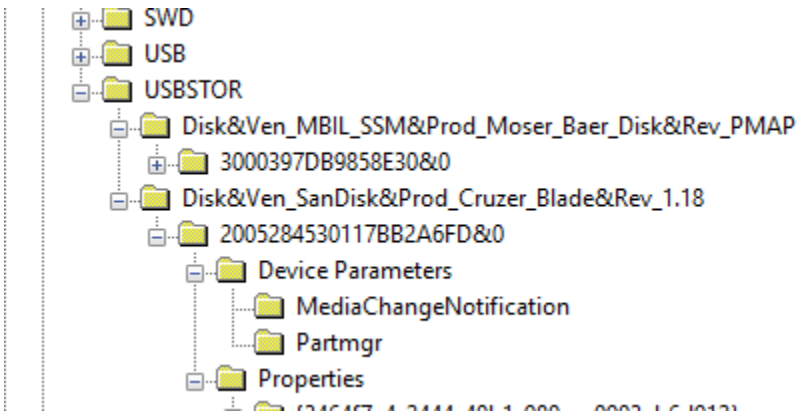
Eastern Standard Time



:

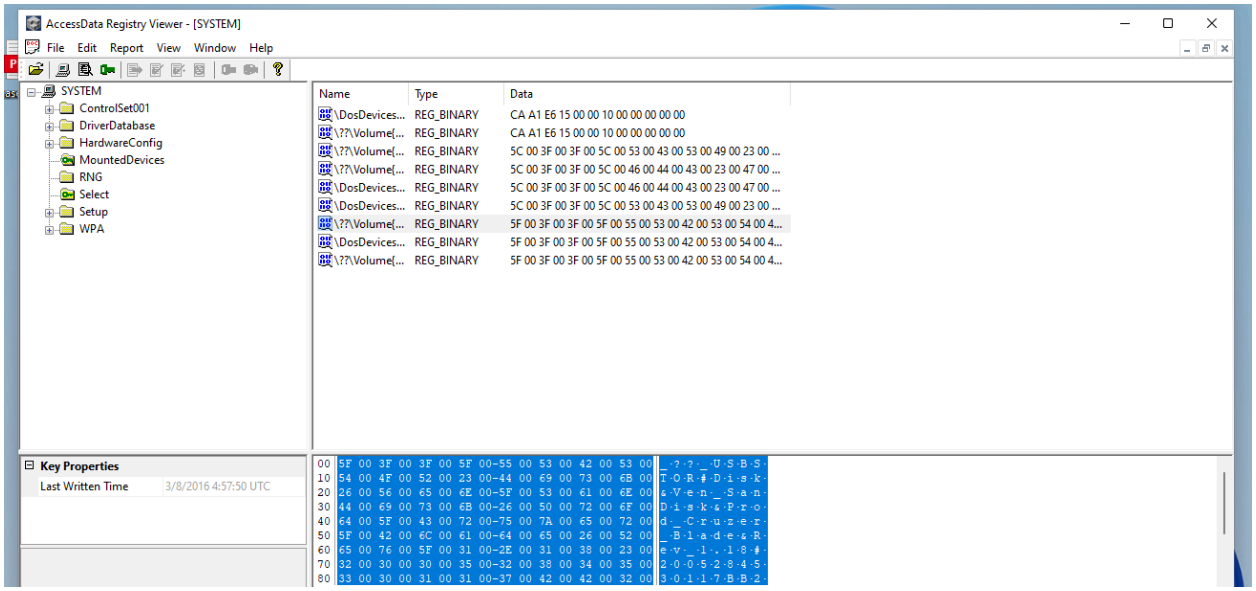
Question 6. Expand ControlSet001>Enum>USBSTOR. How many USBs were plugged into the system and what are the USB’s friendly names? (Hint: expand each device entry and click on the unique instance ID, for example “2005284530117BB2A6FD&0”)

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?

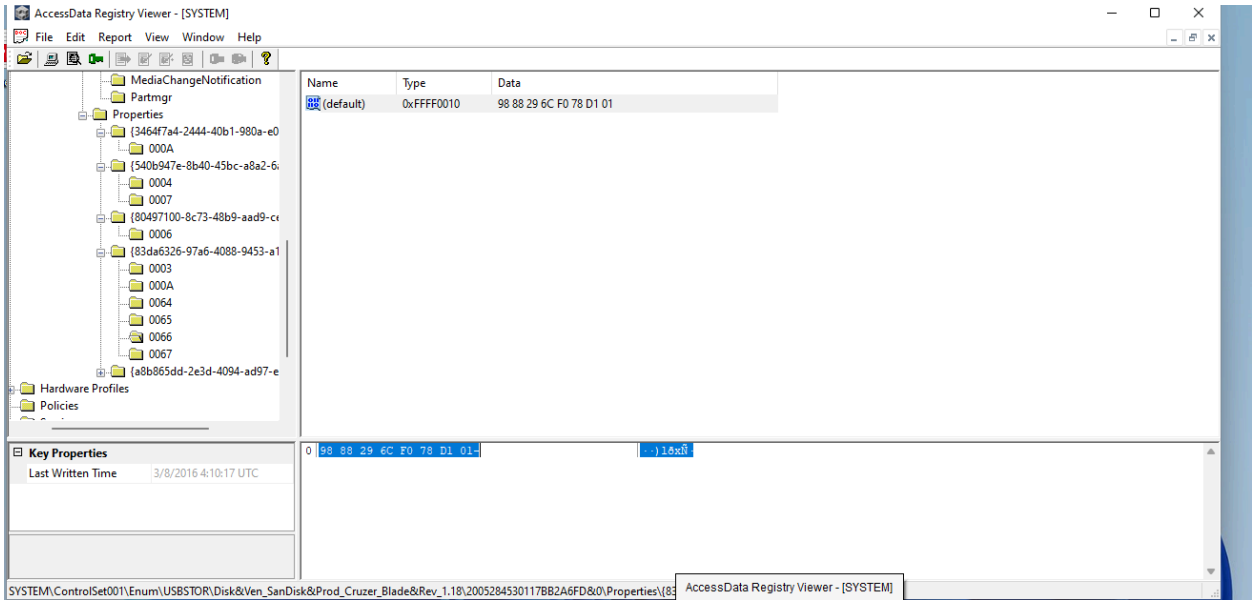
We can see from the screenshot below that is USBSTOR and the Disk name is Cruzer Blade.

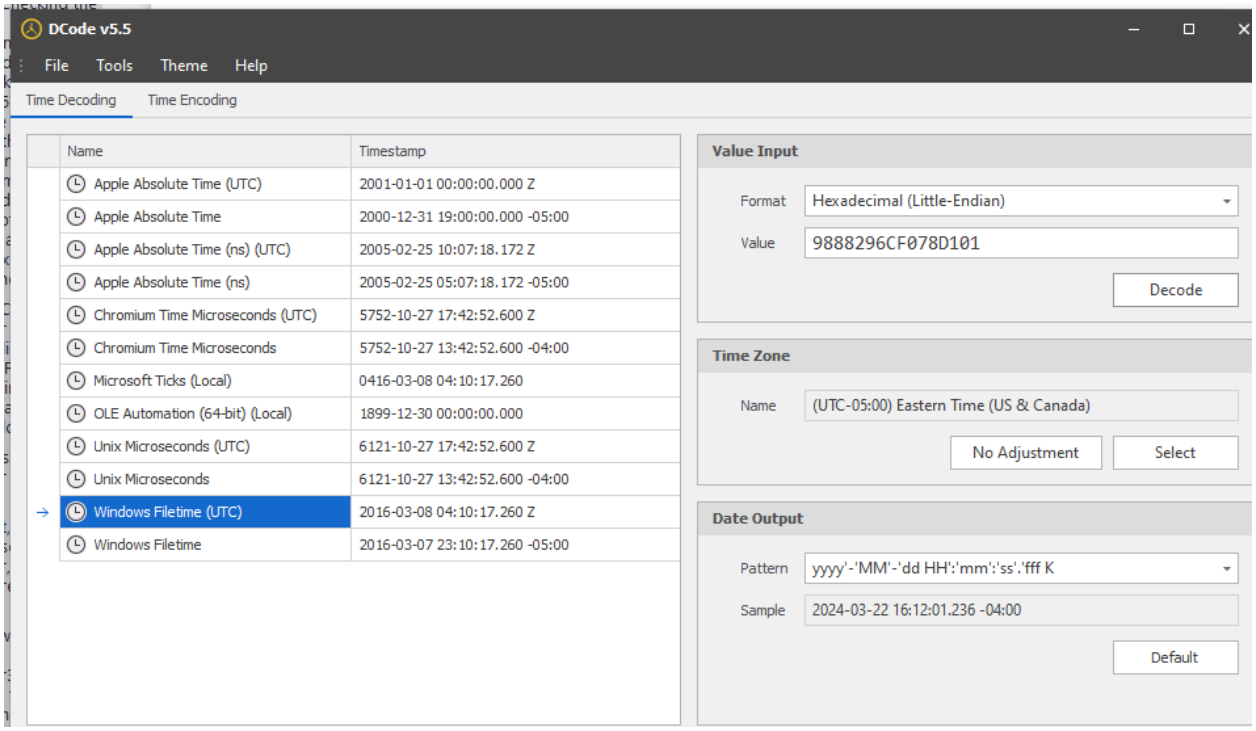


Question 8. When was the USB with the instance ID of "2005284530117BB2A6FD&0" last inserted into the system, and when was it last removed? (Hint: See Registry Lecture PowerPoint slides)

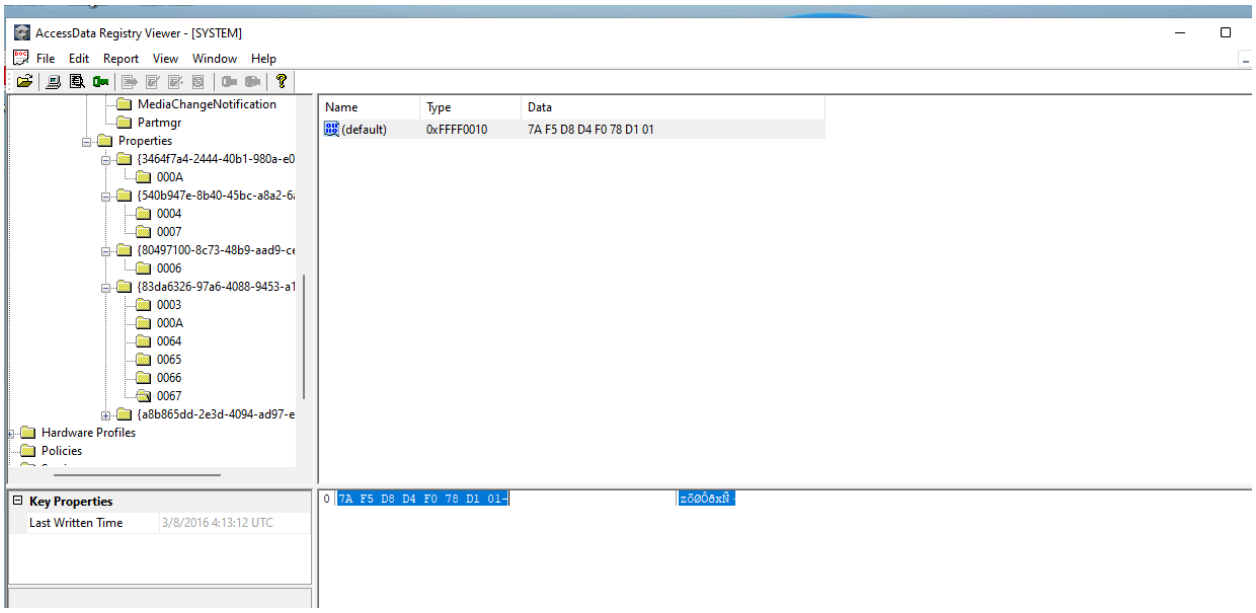
From the slides, I understood that 0067 says about the last inserted time and 0068 says about last removed

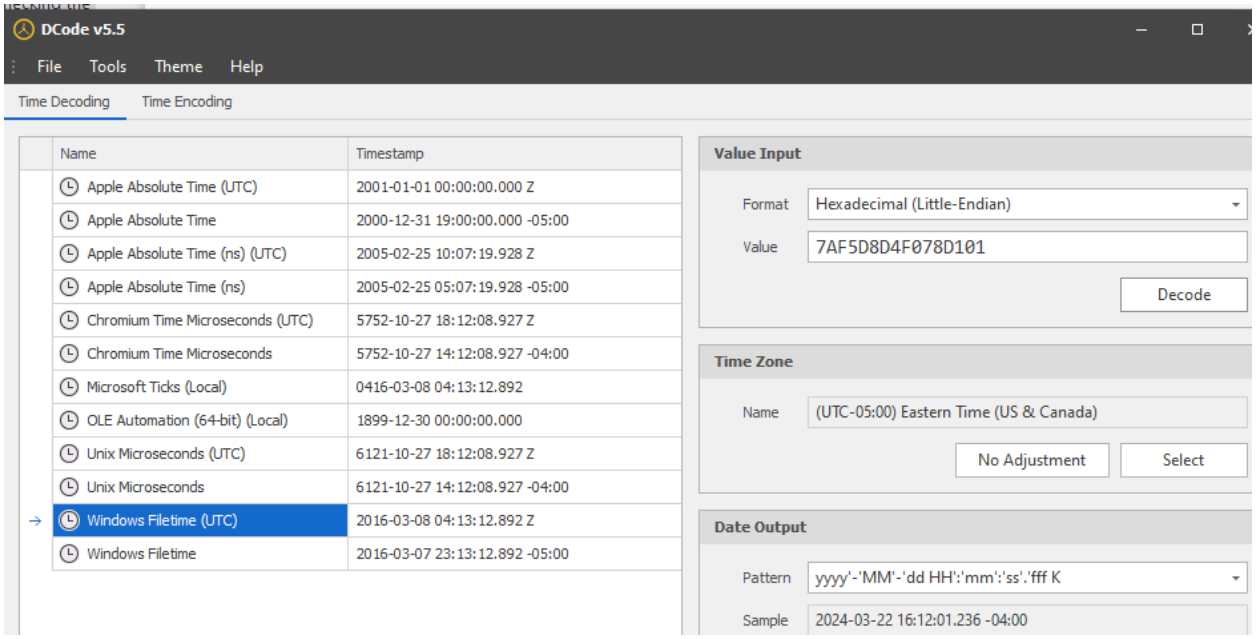
Below is hex values of 0066 and its time values and we can see the time is 04:10:17





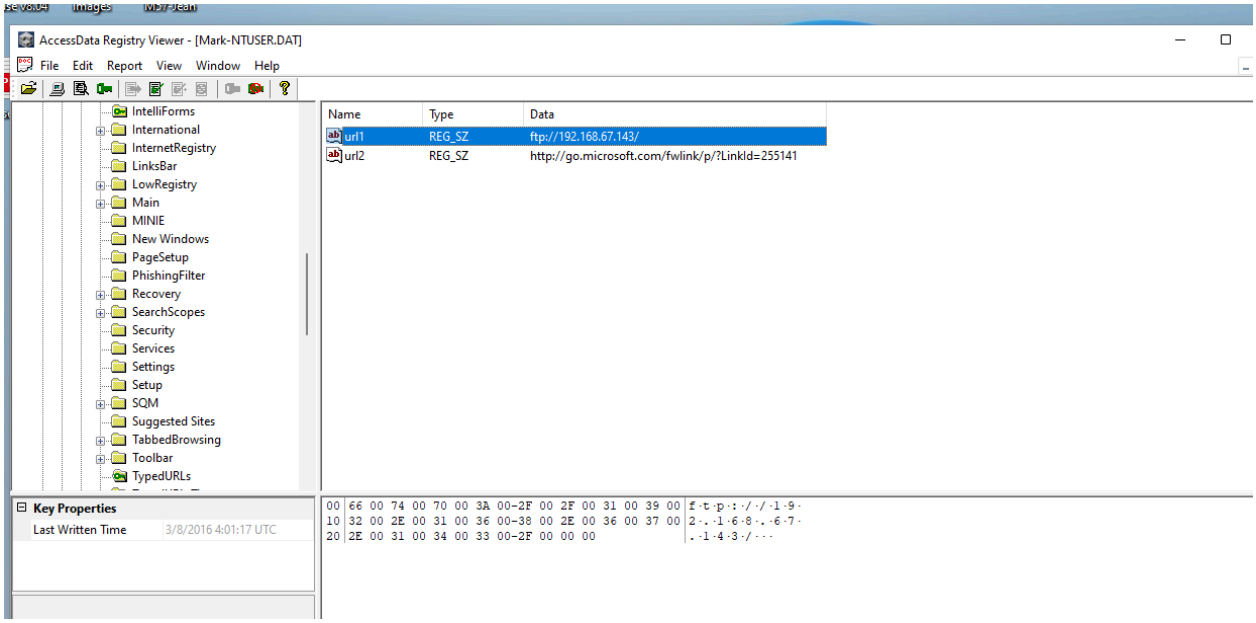
Below is hex of 0067 and its time values, it says removed it 04:13:12.





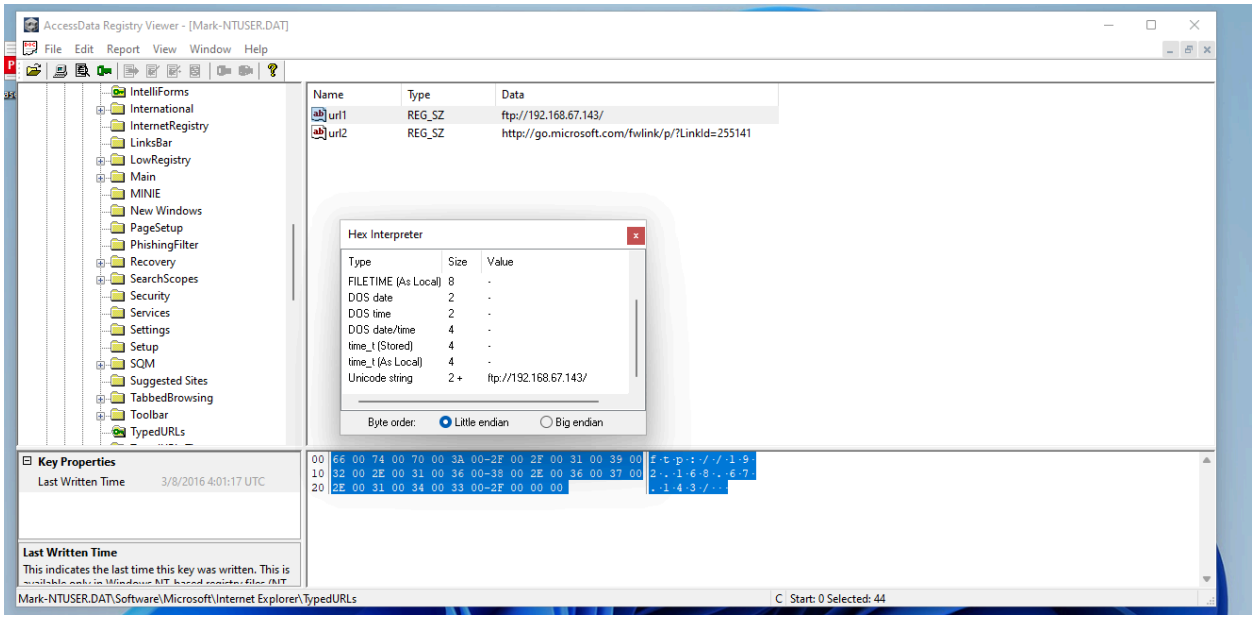
Question 9. Click on “Mark-NTUSER.DAT”. To find the URLs Mark visited, you select Edit >
Find, enter the registry key “TypedURL” in the Find what: text area, and click Find Next. Check the
data of “TypedURL”, What URLs did Mark visit?

These are two URL Mark visited “ Url1 and Url2 “



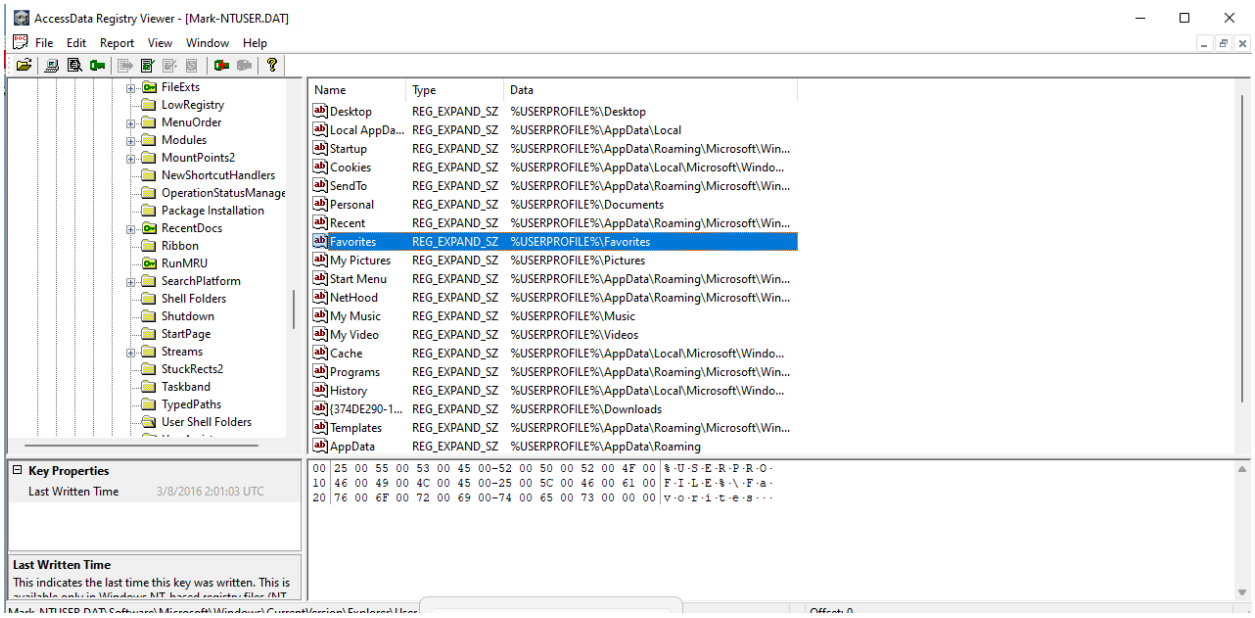
Question 10. Checking the value of “TypedRULsTime”, when were the last date and time
that Mark visited ftp://192.168.67.143? (Hint: the date and time are shown in the key
properties pane. It can also be determined by selecting the data in hex at the right bottom
pane, right-clicking, and using the “Show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

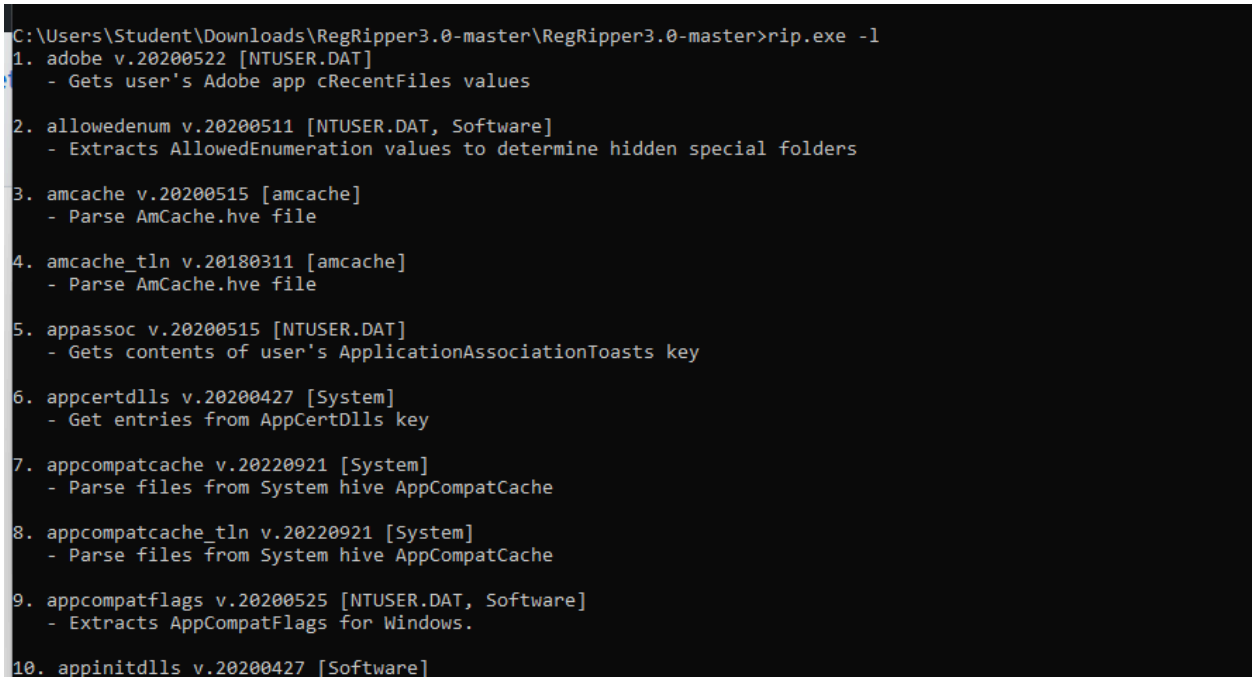
From the screenshot below %USERPROFILE%\Favorites

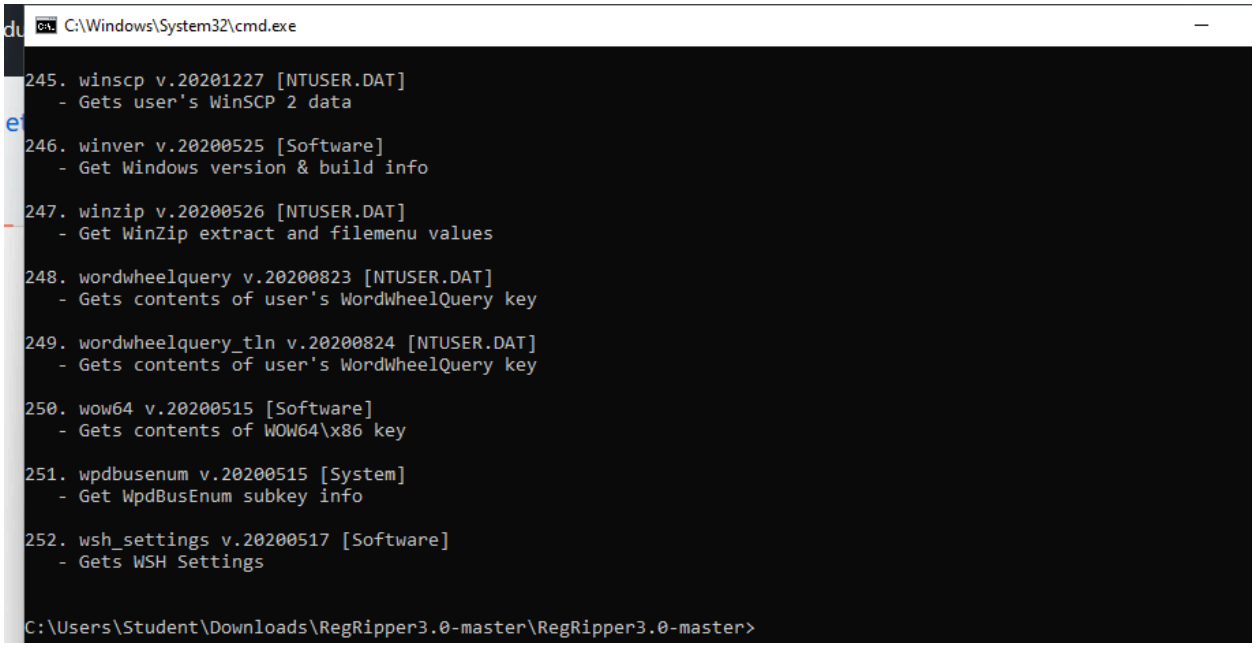


Part 2 – Using RegRipper 3.0

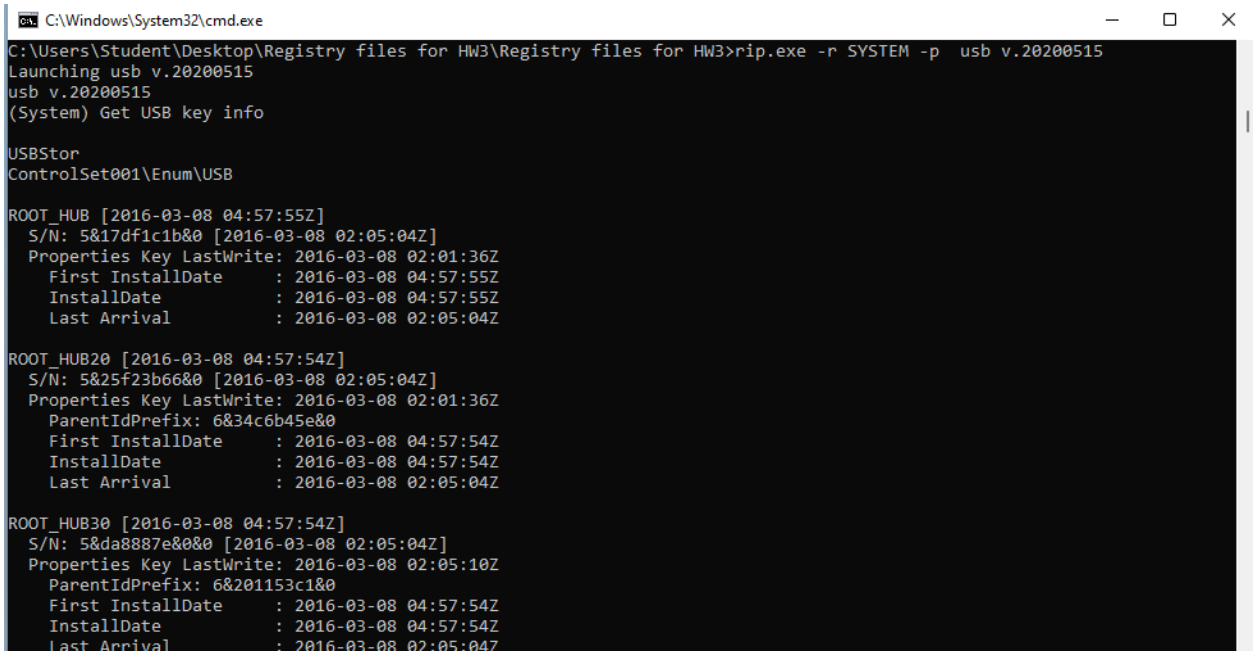
I unzipped the RegRipper3.0 and added this file to my Registry folder to do the analysis.

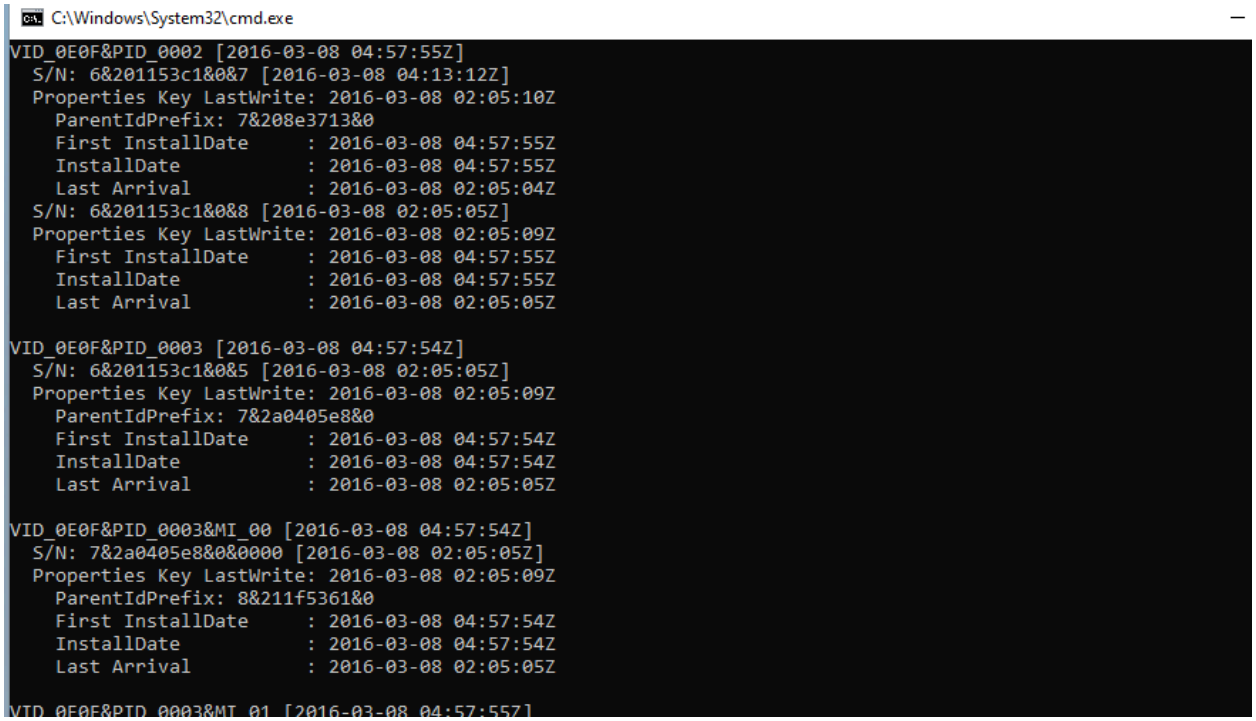
Below to show the available plugins in RegRipper.



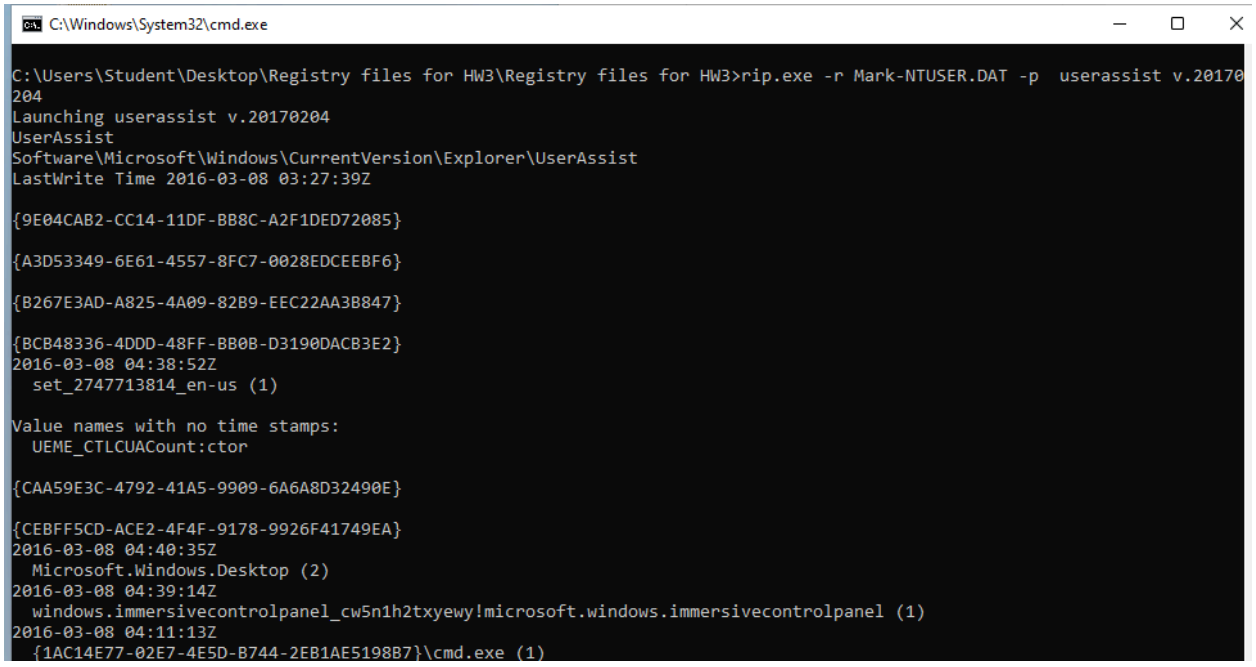


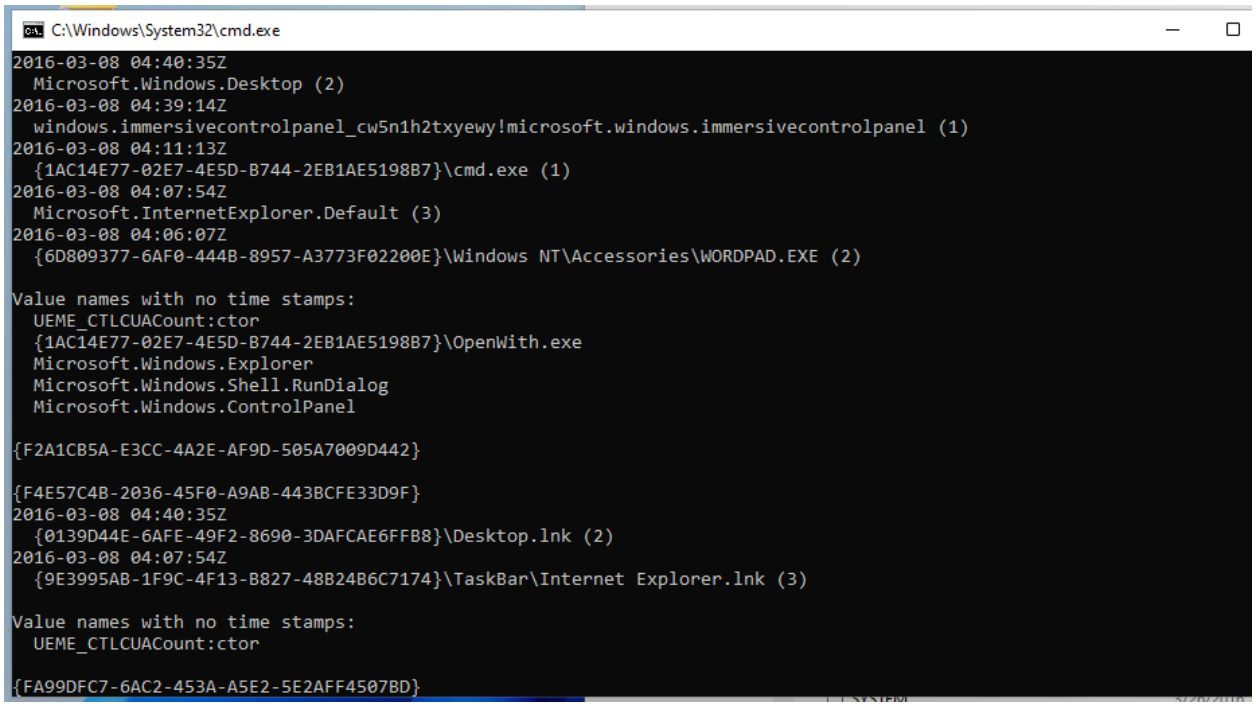
1. This Plugin is used to get the info about the USB that may be recorded on the registry and we got some information about the USBs





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.

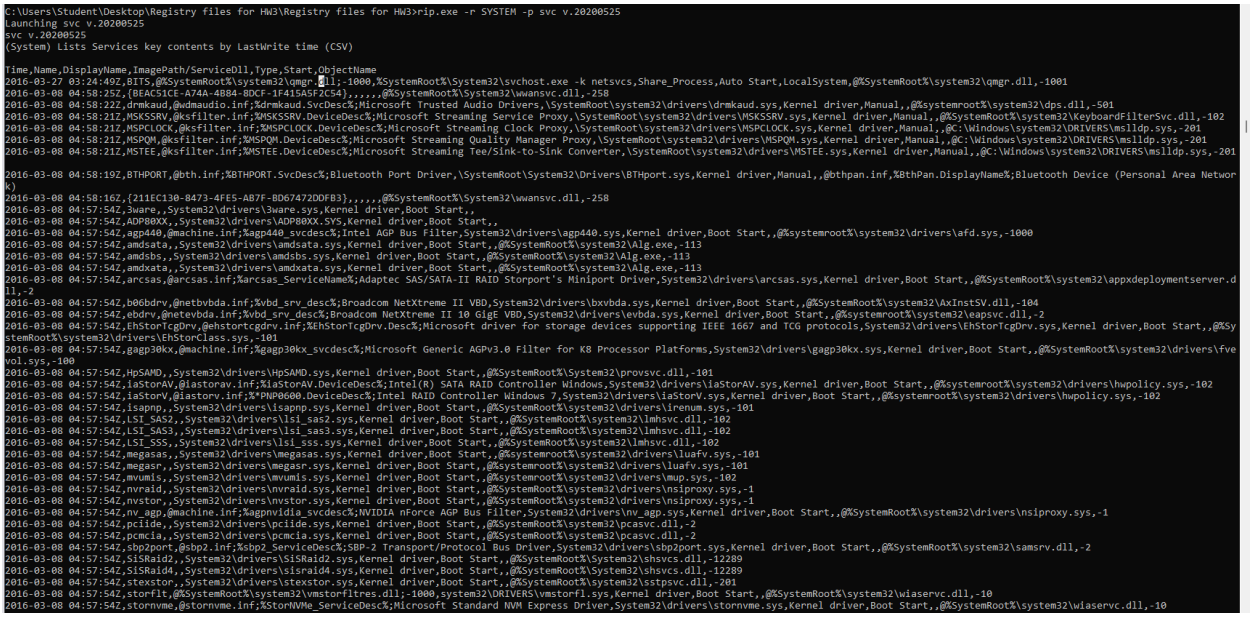




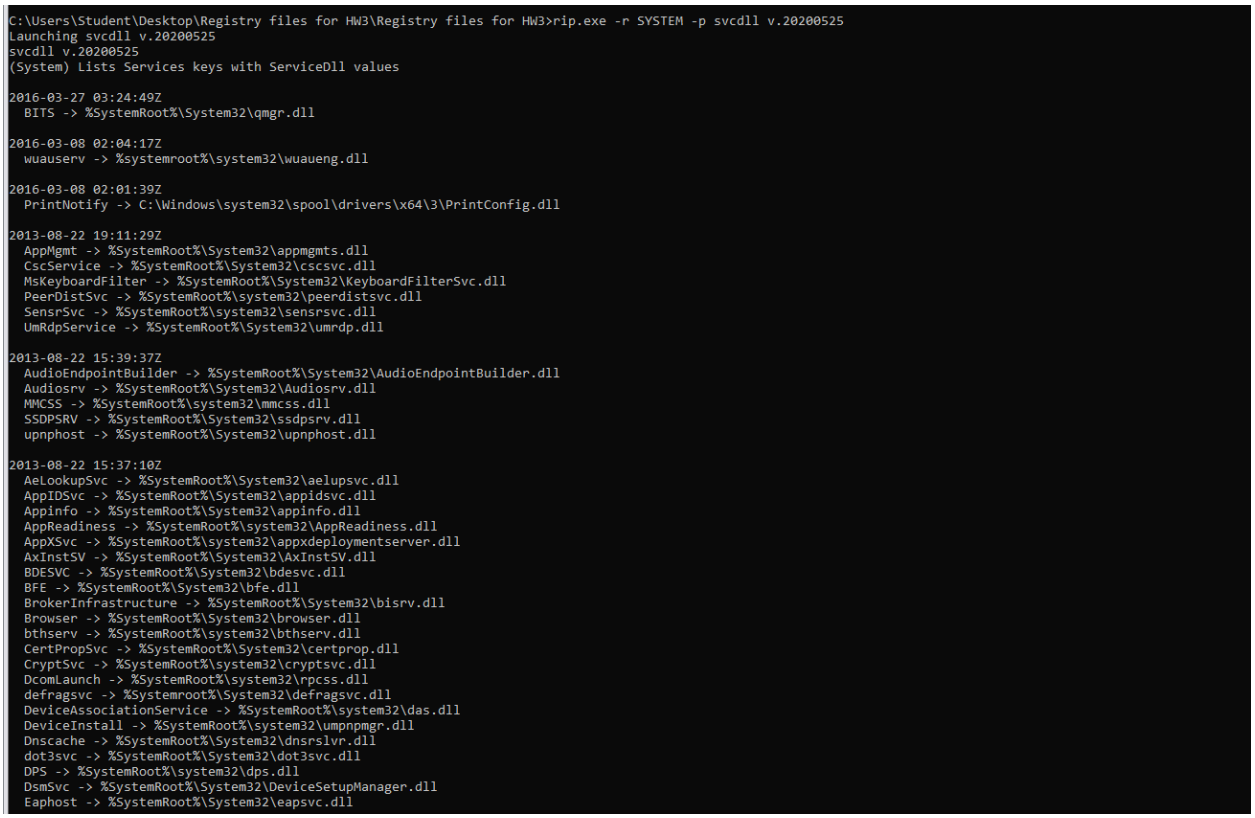
3. SYSTEM will be used by this plugin and gets the timezone information that we already saw in Part 1 which is Eastern Standard Time, Sometimes knowing the location would be useful and crucial while analysing the time and dates.

```
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

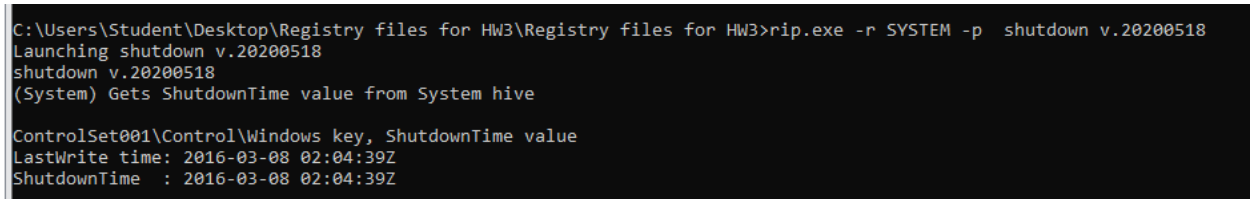


5. All the dynamically linked libraries can be analysed and displayed through this plugin, which also shows about the services that uses the .dll files in a location (system).



```
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
  wuauserv -> %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\mmcss.dll
  SSDPSRV -> %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\appxdeploymentserver.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\umpnpmgr.dll
  Dnscache -> %SystemRoot%\System32\dnsrslvr.dll
  dot3svc -> %SystemRoot%\System32\dot3svc.dll
  DPS -> %SystemRoot%\system32\dps.dll
  DsmSvc -> %SystemRoot%\System32\DeviceSetupManager.dll
  Eaphost -> %SystemRoot%\System32\eapsvc.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.