CSEC 730 - Advanced Computer Forensics

Homework 3 - Using Registry Viewer to Analyze Windows Registry

Please submit your answers (in pdf format) to the assignment submission folder on *myCourses > Assignments* by the due date.

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

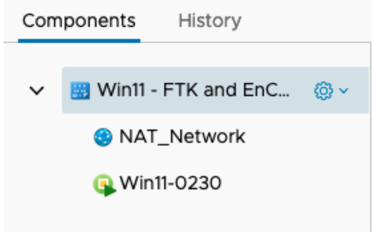
Do you still remember the *Linux_Financial_Case* from Lab 1? *You are given* the registry hive files acquired from Mark's system. In this activity, you will use **Access Data's Registry Viewer** and *RegRipper* (rip.pl) to examine the files and to extract and correlate information to obtain evidence.

Part 1 – Using AccessData's Registry Viewer

Lab Setup

This part uses AccessData's *Registry Viewer*, installed on the virtual machine *Windows 11 w/ FTK 6 & EnCase 8* via the RLES vRealize Automation (vRA) at https://rlescloud.rit.edu. The steps are as follows.

1. Go to https://rlescloud.rit.edu
2. Log in with your RIT username & password
3. Click on the **Catalog** tab and locate "Win11-FTK and EnCase"
4. Click the **Request** button on "Win11-FTK and EnCase".
5. Click the **Submit** button (at the lower-left corner of the window) to deploy the VM.
6. After your request has successfully completed deployment, click on the item (for example, Win11-FTK and EnCase-xxxxxxxx). You will see its Components



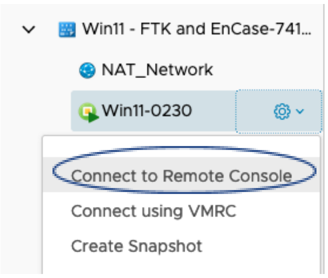
Components History

Win11 - FTK and EnC...

NAT_Network

Win11-0230

7. Use the Actions menu next to Win11-0230 to choose "**Connect to Remote Console**". If Win11-0230 is powered off, choose "**Power on …**" (**refresh the screen to check whether Win11-0230 is powered on**).



The Windows virtual machine is ready to use. In case you need to re-login, the Windows login credential is:
Username: Student
Password: student

Software and registry files

Registry Viewer is installed on the virtual machine *Windows 11 w/ FTK 6 & EnCase 8* on RLES. User Guide download link: https://ad-pdf.s3.amazonaws.com/RegistryViewer_UG.pdf. I also include the registry viewer user guide and an introduction video on myCourses for your reference.

Download and extract the Registry files, *Registry files from HW3.zip*, from myCourses. The Windows registry hive files are:

- SAM
- SYSTEM
- Mark-NTUSER.DAT

Instructions

- Open the hive file you would like to examine.
- 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.

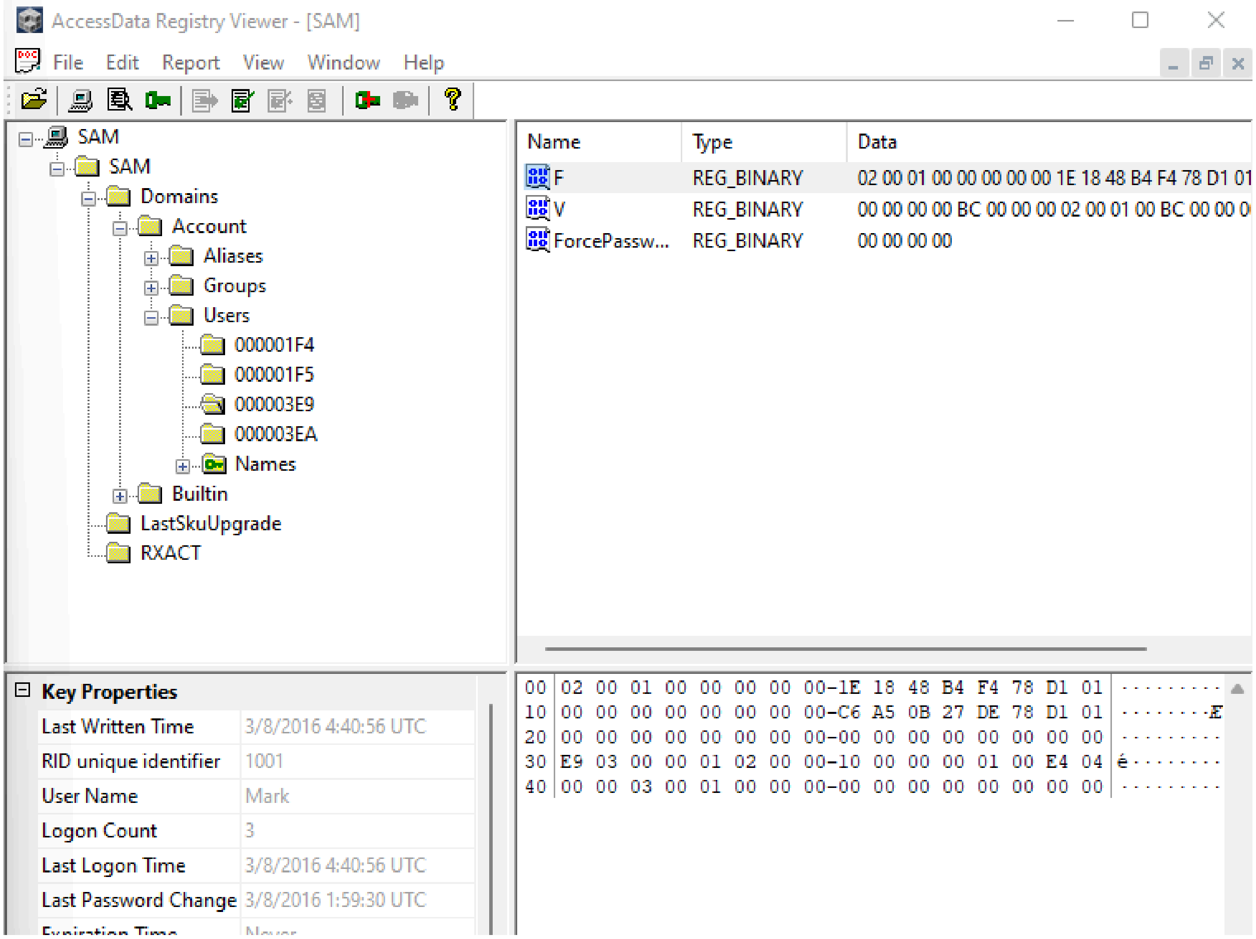
Deliverables for Part 1: (Total: 88 points)

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 RID number logged onto the system on 3/8/2016 at 4:40:56 UTC?

- The user name is Mark with the RID of 1001 that logged onto the system on 3/8/2016 at 4:40:56 UTC.



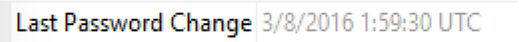
Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 1E 18 48 B4 F4 78 D1 01
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 0
ForcePassw...	REG_BINARY	00 00 00 00

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

```
00 | 02 00 01 00 00 00 00 00-1E 18 48 B4 F4 78 D1 01 | ·········
10 | 00 00 00 00 00 00 00 00-C6 A5 0B 27 DE 78 D1 01 | ········Æ
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········
40 | 00 00 03 00 01 00 00 00-00 00 00 00 00 00 00 00 | ·········
```

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

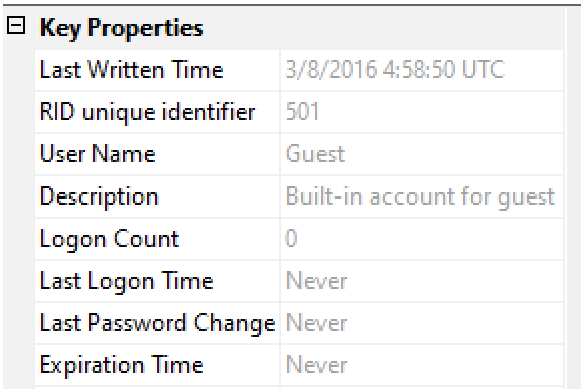
- The last date and time that Mark changed his Windows password is on 3/8/2016 at 1:59:30 UTC.



Last Password Change	3/8/2016 1:59:30 UTC

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

- The account name with Guest and the RID of 501.

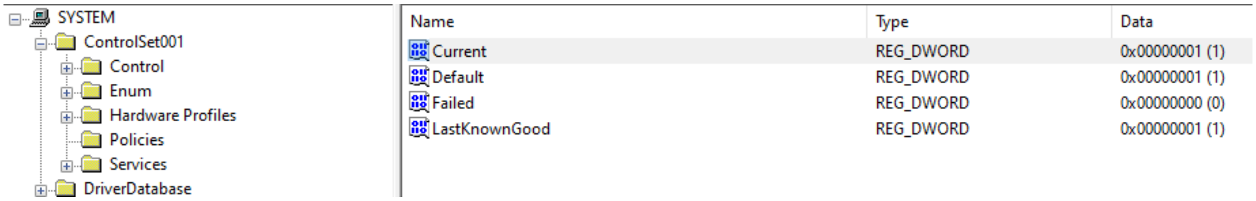


Key Properties	
Last Written Time	3/8/2016 4:58:50 UTC
RID unique identifier	501
User Name	Guest
Description	Built-in account for guest
Logon Count	0
Last Logon Time	Never
Last Password Change	Never
Expiration Time	Never

2. Examine the SYSTEM registry hive.

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

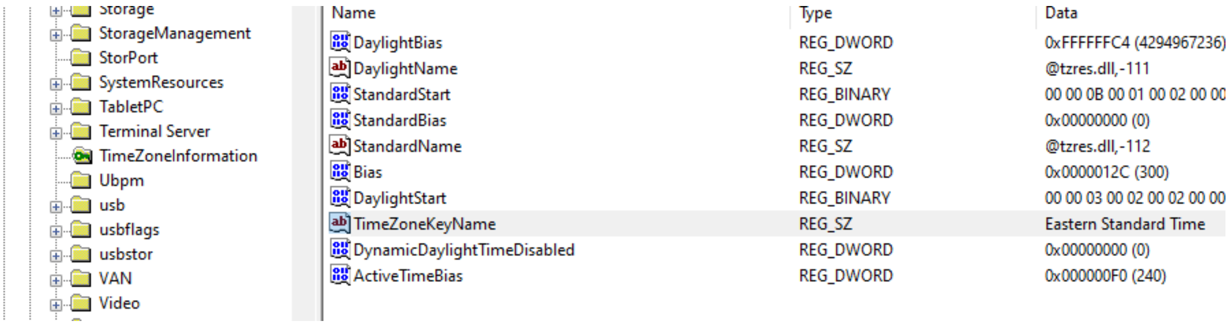
- The current ControlSet of “Current” is set to 1. Meaning it’s used by the Windows OS.



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

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

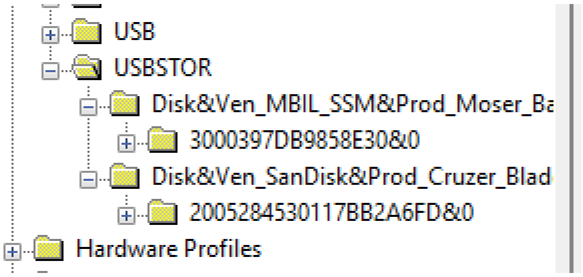
- The TimeZoneKeyName is Eastern Standard Time.

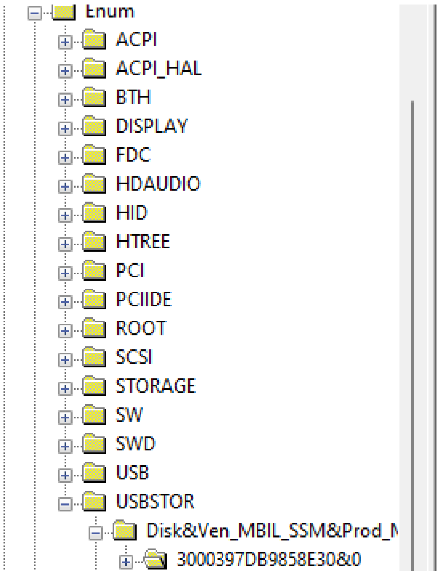


Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
Bias	REG_DWORD	0x0000012C (300)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00
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”)

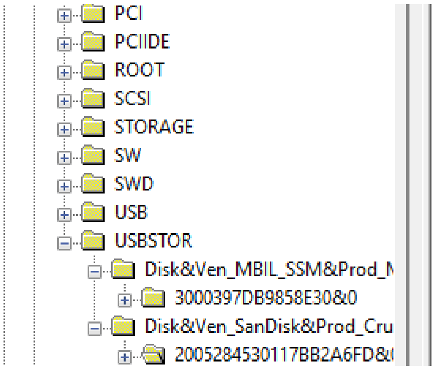
- There were two USBs that were plugged into the system and the friendlyname for each USBs are “MBIL SSM Moser Baer Disk USB Device” and “SanDisk Cruzer Blade USB Device”





```
Enum
  ACPI
  ACPI_HAL
  BTH
  DISPLAY
  FDC
  HDAUDIO
  HID
  HTREE
  PCI
  PCIIDE
  ROOT
  SCSI
  STORAGE
  SW
  SWD
  USB
  USBSTOR
    Disk&Ven_MBIL_SSM&Prod_N
      3000397DB9858E30&0
```

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_...	USBSTOR\DiskMBIL_SSMMoser_Baer_Disk_PMAP US...
CompatibleIDs	REG_MULTI_...	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)

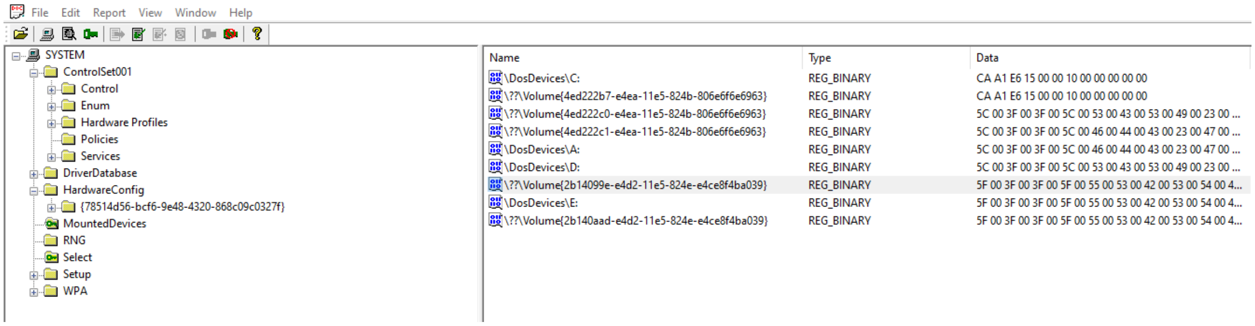


```
  PCI
  PCIIDE
  ROOT
  SCSI
  STORAGE
  SW
  SWD
  USB
  USBSTOR
    Disk&Ven_MBIL_SSM&Prod_N
      3000397DB9858E30&0
    Disk&Ven_SanDisk&Prod_Cru
      2005284530117BB2A6FD&0
```

Name	Type	Data
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)

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

- The volume that the USB device mounted to was "\??\Volume{2b14099e-ee4d2-11e5-824e-e4c38f4ba039}"



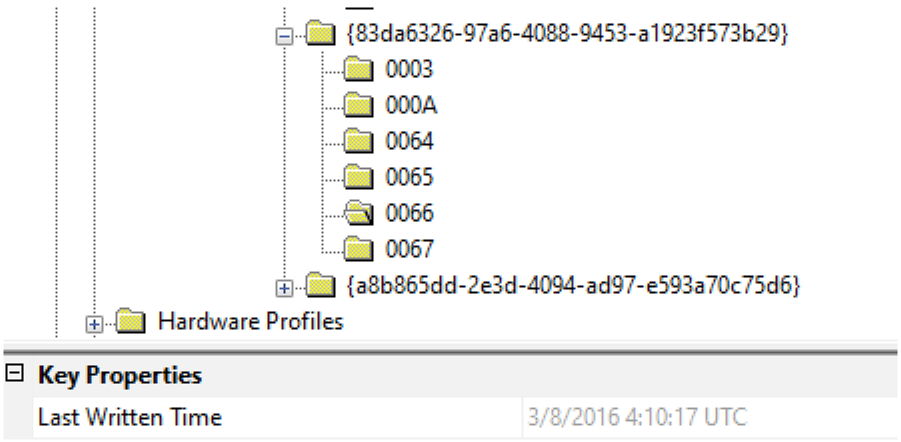
```
SYSTEM
  ControlSet001
    Control
    Enum
    Hardware Profiles
    Policies
    Services
  DriverDatabase
  HardwareConfig
    {78514d56-bcf6-9e48-4320-868c09c0327f}
  MountedDevices
  RNG
  Select
  Setup
  WPA
```

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 49 00 23 00 ...
\??\Volume{4ed222c1-e4ea-11e5-824b-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 49 00 23 00 ...
\??\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 4...
\DosDevices\E:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\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 4...

-

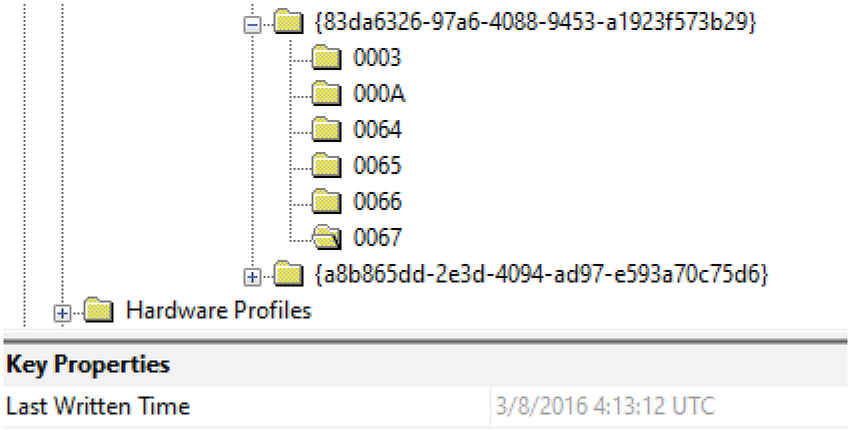
Question 8. When was the USB with the instance ID of "2005284530117BB2A6FD&0" last inserted into the system, and when was it last removed? (Hint: See Registry Lecture PowerPoint slides)

- The USB was last inserted on 3/8/2016 4:10:17 UTC, and the last removal was on 3/8/2016 4:13:12 UTC.


{83da6326-97a6-4088-9453-a1923f573b29}
0003
000A
0064
0065
0066
0067
{a8b865dd-2e3d-4094-ad97-e593a70c75d6}
Hardware Profiles

⊟ **Key Properties**

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


{83da6326-97a6-4088-9453-a1923f573b29}
0003
000A
0064
0065
0066
0067
{a8b865dd-2e3d-4094-ad97-e593a70c75d6}
Hardware Profiles

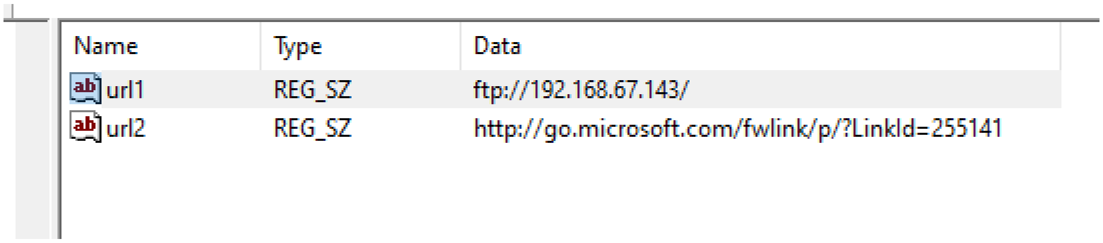
Key Properties

Last Written Time	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?

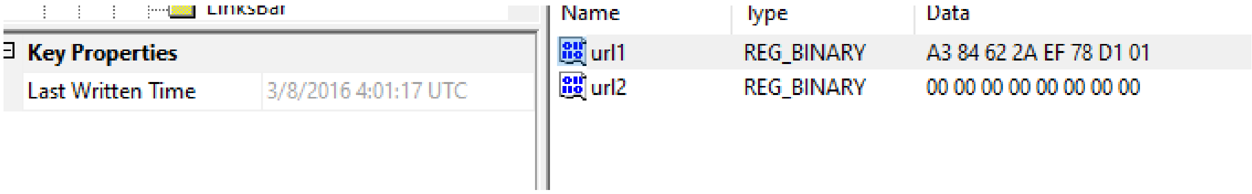
- Mark visited “ftp://192.168.67.143/” and “http://go.microsoft.com/fwlink/p/?Linkid=255141”



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 "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.)

- The last date and time that Mark visited the URL is on 3/8/2016 4:01:17 UTC.



LinksBar

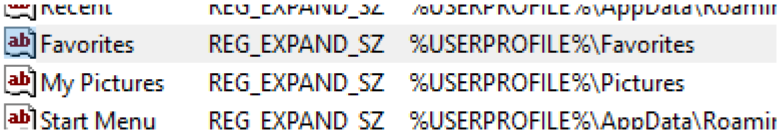
Key Properties

Last Written Time	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

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?

- The path to Mark's Favorites fold is "%USERPROFILE%\Favorites"



Recent	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roamir
Favorites	REG_EXPAND_SZ	%USERPROFILE%\Favorites
My Pictures	REG_EXPAND_SZ	%USERPROFILE%\Pictures
Start Menu	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roamir

Part 2 – Using RegRipper 3.0 (Total: 12 Points)

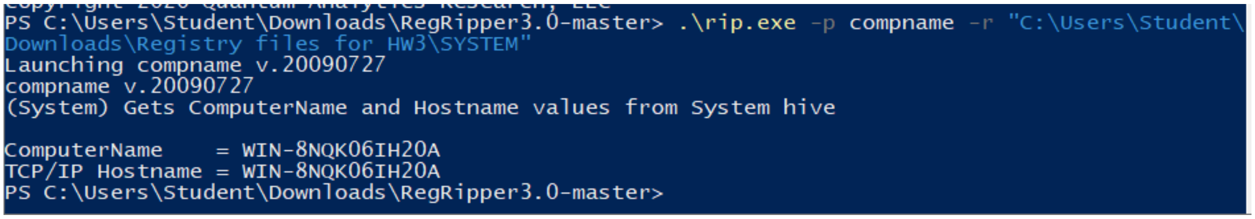
In this part, you will the open-source tool, RegRipper, for Windows registry analysis. First, you will download ***RegRipper3.0-master.zip*** from https://github.com/keydet89/RegRipper3.0 to your virtual machine Windows 11 w/ FTK 6 & EnCase 8. Then, you will use the Windows command line tool ***rip.exe*** to practice registry analysis with RegRipper as an alternative tool.

Deliverables for Part 2:

Run ***rip.exe*** on the given registry hives (from Part 1) with three (3) plugins you choose. **For each plugin you run**, provide a brief description of the result and the screenshot of the command & results you received. (Note: *rip.exe -l* shows all the plugins supported by *rip* at the current version.)

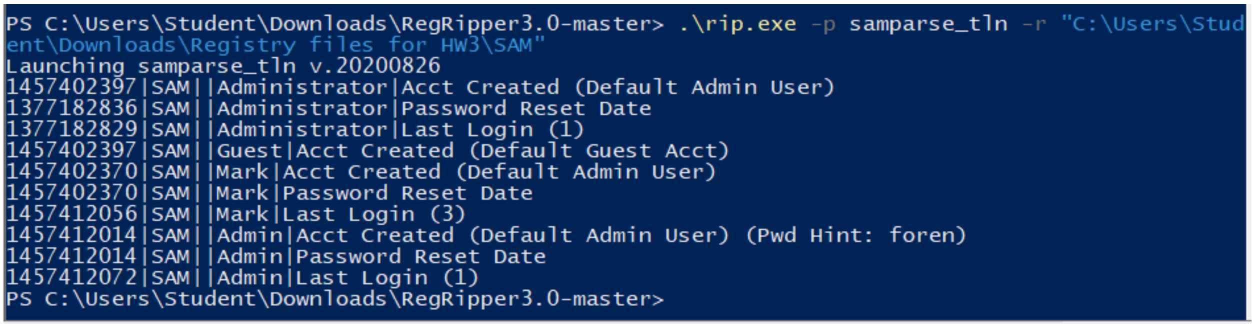
ENJOY!

- Using the "compname" plugin on the SYSTEM hive:
  - Description: This plugin gets ComputerName and Hostname values from System hive. By running the command in the screenshot below I was able to get the Computername and Hostname of WIN-8NQK06IH20A.



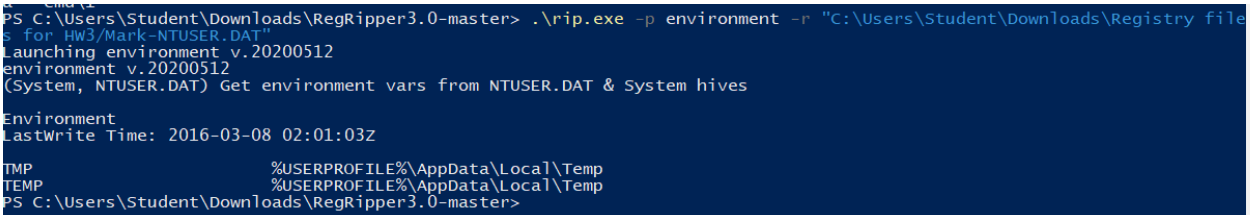
```
Copyright 2020 Quantum Analytics Research, LLC
PS C:\Users\Student\Downloads\RegRipper3.0-master> .\rip.exe -p compname -r "C:\Users\Student\
Downloads\Registry files for HW3\SYSTEM"
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName     = WIN-8NQK06IH20A
TCP/IP Hostname = WIN-8NQK06IH20A
PS C:\Users\Student\Downloads\RegRipper3.0-master>
```

- Using the "samparse_tln" plugin on the SAM hive:
  - Description: parses the SAM file for user account into.



```
PS C:\Users\Student\Downloads\RegRipper3.0-master> .\rip.exe -p samparse_tln -r "C:\Users\Stud
ent\Downloads\Registry files for HW3\SAM"
Launching samparse_tln v.20200826
1457402397|SAM||Administrator|Acct Created (Default Admin User)
1377182836|SAM||Administrator|Password Reset Date
1377182829|SAM||Administrator|Last Login (1)
1457402397|SAM||Guest|Acct Created (Default Guest Acct)
1457402370|SAM||Mark|Acct Created (Default Admin User)
1457402370|SAM||Mark|Password Reset Date
1457412056|SAM||Mark|Last Login (3)
1457412014|SAM||Admin|Acct Created (Default Admin User) (Pwd Hint: foren)
1457412014|SAM||Admin|Password Reset Date
1457412072|SAM||Admin|Last Login (1)
PS C:\Users\Student\Downloads\RegRipper3.0-master>
```

- Used the “environment” plugin on Mark_NTUSER.DAT:
    - Description: The plugin is used to get the environment variable of user Mark



```
PS C:\Users\Student\Downloads\RegRipper3.0-master> .\rip.exe -p environment -r "C:\Users\Student\Downloads\Registry file
s for HW3/Mark-NTUSER.DAT"
Launching environment v.20200512
environment v.20200512
(System, NTUSER.DAT) Get environment vars from NTUSER.DAT & System hives

Environment
LastWrite Time: 2016-03-08 02:01:03Z

TMP                        %USERPROFILE%\AppData\Local\Temp
TEMP                       %USERPROFILE%\AppData\Local\Temp
PS C:\Users\Student\Downloads\RegRipper3.0-master>
```