Lab 4 – Registry and Browser Forensics

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 10/07/2019

Introduction

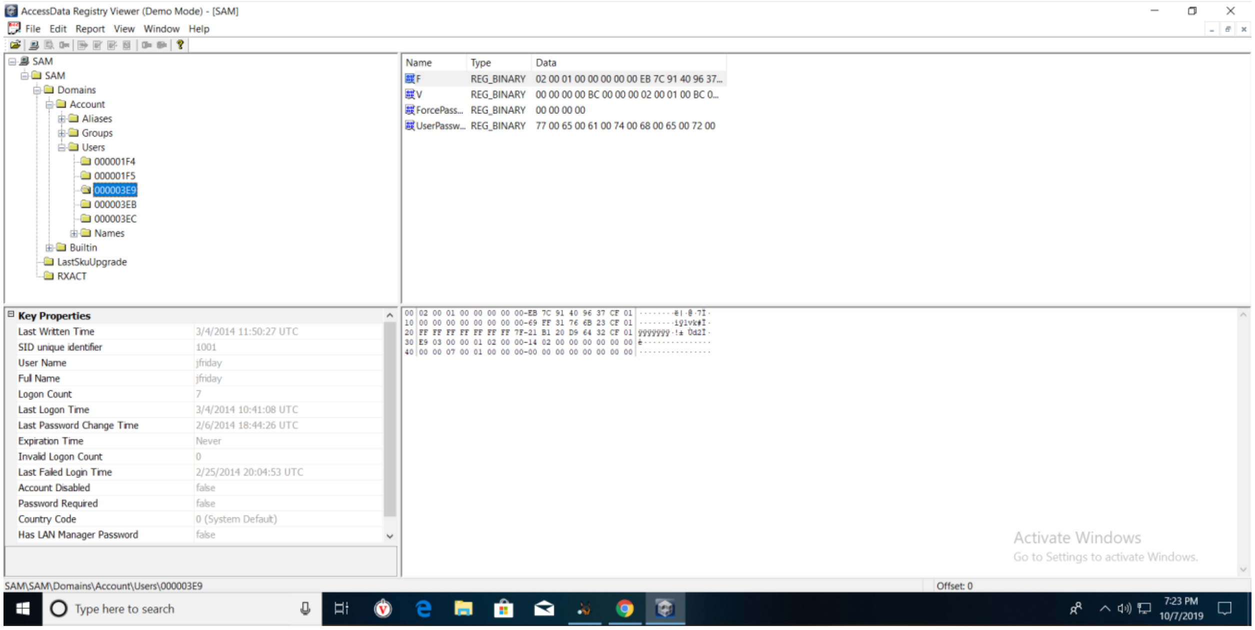
FTH-Imager, also known as Forensics Toolkit Imager, is used to make an image of hard disks, USB sticks, CDs and store in one file future reference. It can also be used to recover deleted file and scan the image for strings to make sense/ search the evidence. Registry Viewer is used for analyzing the contents of Windows registry hive files. Registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems and registry viewer gives a simple user interface to view this information. Autopsy is another forensics tool with a graphical user interface that displays results from a forensic search which makes it easy for investigators traverse and search sections of data

In this lab we will examine registry hives and images that we got from Lab 2 and try to gather more information from the evidence. We will also get more information out of the images gathered from the evidence by examining the meta data of those images.

Part 1. Examining the SAM Hive

1. Which account logged into the system the most?

   Account with most logins is jfriday, 7 logins, this information can be found in the registry file ‘SAM’ ‘USER ACCOUNTS’ in the left lower pane.



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 EB 7C 91 40 96 37...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 0...
ForcePass...	REG_BINARY	00 00 00 00
UserPassw...	REG_BINARY	77 00 65 00 61 00 74 00 68 00 65 00 72 00

Key Properties	
Last Written Time	3/4/2014 11:50:27 UTC
SID unique identifier	1001
User Name	jfriday
Full Name	jfriday
Logon Count	7
Last Logon Time	3/4/2014 10:41:08 UTC
Last Password Change Time	2/6/2014 18:44:26 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2/25/2014 20:04:53 UTC
Account Disabled	false
Password Required	false
Country Code	0 (System Default)
Has LAN Manager Password	false

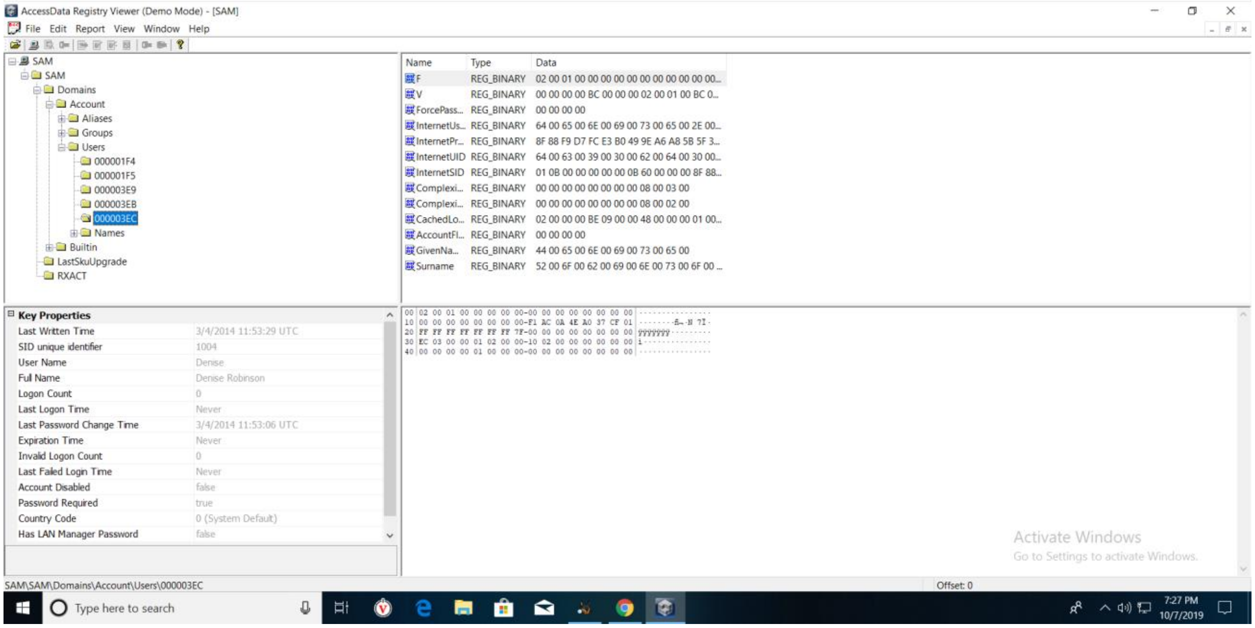
```
00 02 00 01 00 00 00 00 00-EB 7C 91 40 96 37 CF 01 ········ë|·@·7Ï·
10 00 00 00 00 00 00 00 00-69 FF 31 76 6B 23 CF 01 ········iÿ1vk#Ï·
20 FF FF FF FF FF FF FF 7F-21 B1 20 D9 64 32 CF 01 ÿÿÿÿÿÿÿ·!± Ùd2Ï·
30 E9 03 00 00 01 02 00 00-14 02 00 00 00 00 00 00 é···············
40 00 00 07 00 01 00 00 00-00 00 00 00 00 00 00 00 ················
```

SAM\SAM\Domains\Account\Users\000003E9

Offset: 0

2. Has Denise Robinson logged in?

   No, Denise Robinson does not have any logins, we can find this information in the registry file ‘SAM’ ‘USER ACCOUNTS’ in the left lower pane.



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 00 00 00 00 00 00...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 0...
ForcePass...	REG_BINARY	00 00 00 00
InternetUs...	REG_BINARY	64 00 65 00 6E 00 69 00 73 00 65 00 2E 00...
InternetPr...	REG_BINARY	8F 88 F9 D7 FC E3 B0 49 9E A6 A8 5B 5F 3...
InternetUID	REG_BINARY	64 00 63 00 39 00 30 00 62 00 64 00 30 00...
InternetSID	REG_BINARY	01 0B 00 00 00 00 00 0B 60 00 00 00 8F 88...
Complexi...	REG_BINARY	00 00 00 00 00 00 00 00 08 00 03 00
Complexi...	REG_BINARY	00 00 00 00 00 00 00 00 08 00 02 00
CachedLo...	REG_BINARY	02 00 00 00 BE 09 00 00 48 00 00 00 01 00...
AccountFl...	REG_BINARY	00 00 00 00
GivenNa...	REG_BINARY	44 00 65 00 6E 00 69 00 73 00 65 00
Surname	REG_BINARY	52 00 6F 00 62 00 69 00 6E 00 73 00 6F 00 ...

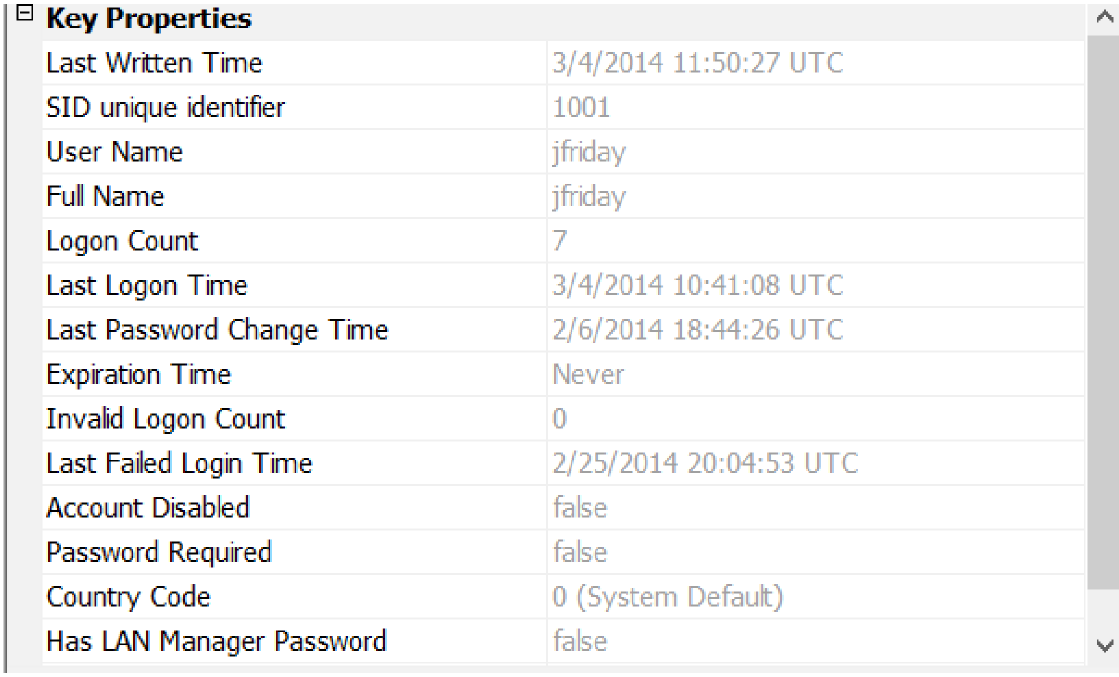
Key Properties	
Last Written Time	3/4/2014 11:53:29 UTC
SID unique identifier	1004
User Name	Denise
Full Name	Denise Robinson
Logon Count	0
Last Logon Time	Never
Last Password Change Time	3/4/2014 11:53:06 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Password	false

```
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-F1 AC 0A 4E A0 37 CF 01 ········ñ¬·N 7Ï·
20 FF FF FF FF FF FF FF 7F-00 00 00 00 00 00 00 00 ÿÿÿÿÿÿÿ·········
30 EC 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00 ì···············
40 00 00 00 00 01 00 00 00-00 00 00 00 00 00 00 00 ················
```

SAM\SAM\Domains\Account\Users\000003EC

3. Expand SAM-Domains-Accounts-Users-Names and identify when jfriday’s account password was last set?

   Jfriday’s account password was last set on 2/6/2014 18:44:26 UTC

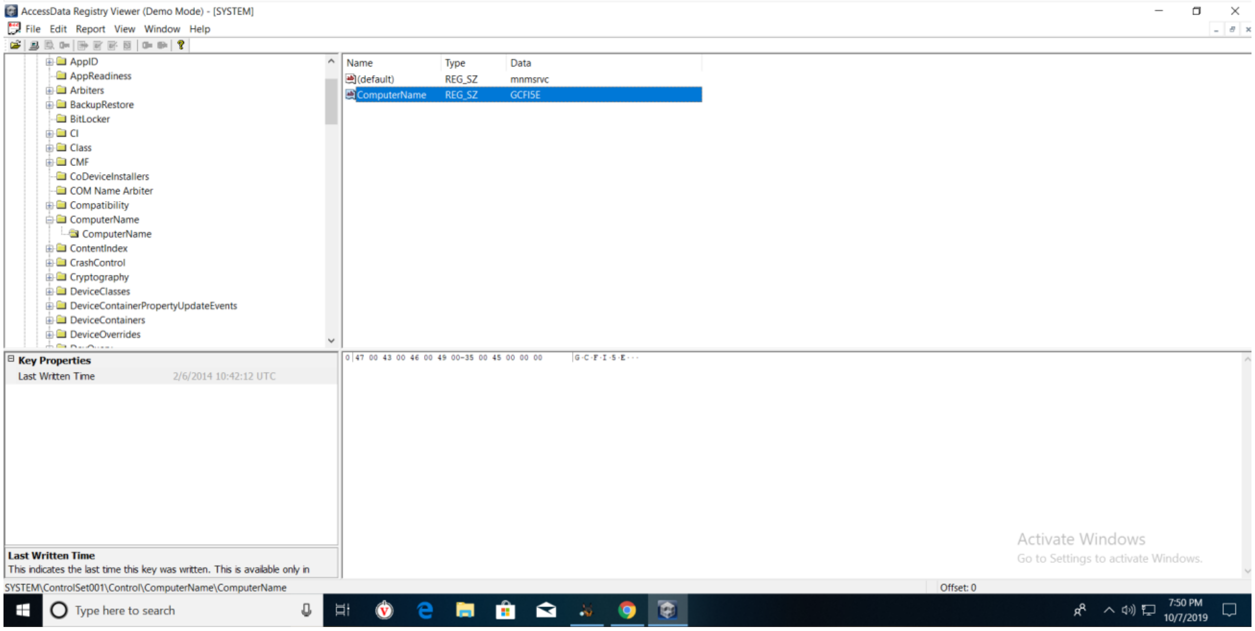


Key Properties	
Last Written Time	3/4/2014 11:50:27 UTC
SID unique identifier	1001
User Name	jfriday
Full Name	jfriday
Logon Count	7
Last Logon Time	3/4/2014 10:41:08 UTC
Last Password Change Time	2/6/2014 18:44:26 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2/25/2014 20:04:53 UTC
Account Disabled	false
Password Required	false
Country Code	0 (System Default)
Has LAN Manager Password	false

Part 2. Examining the SYSTEM Hive

1. What is the computer name this image is from?

   Computer Name: GCFI5E


AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help
Type here to search
Activate Windows
Go to Settings to activate Windows.
7:50 PM
10/7/2019

AppID
AppReadiness
Arbiters
BackupRestore
BitLocker
CI
Class
CMF
CoDeviceInstallers
COM Name Arbiter
Compatibility
ComputerName
ComputerName
ContentIndex
CrashControl
Cryptography
DeviceClasses
DeviceContainerPropertyUpdateEvents
DeviceContainers
DeviceOverrides

Name	Type	Data
(default)	REG_SZ	mnmsrvc
ComputerName	REG_SZ	GCFI5E

Key Properties

Last Written Time	2/6/2014 10:42:12 UTC

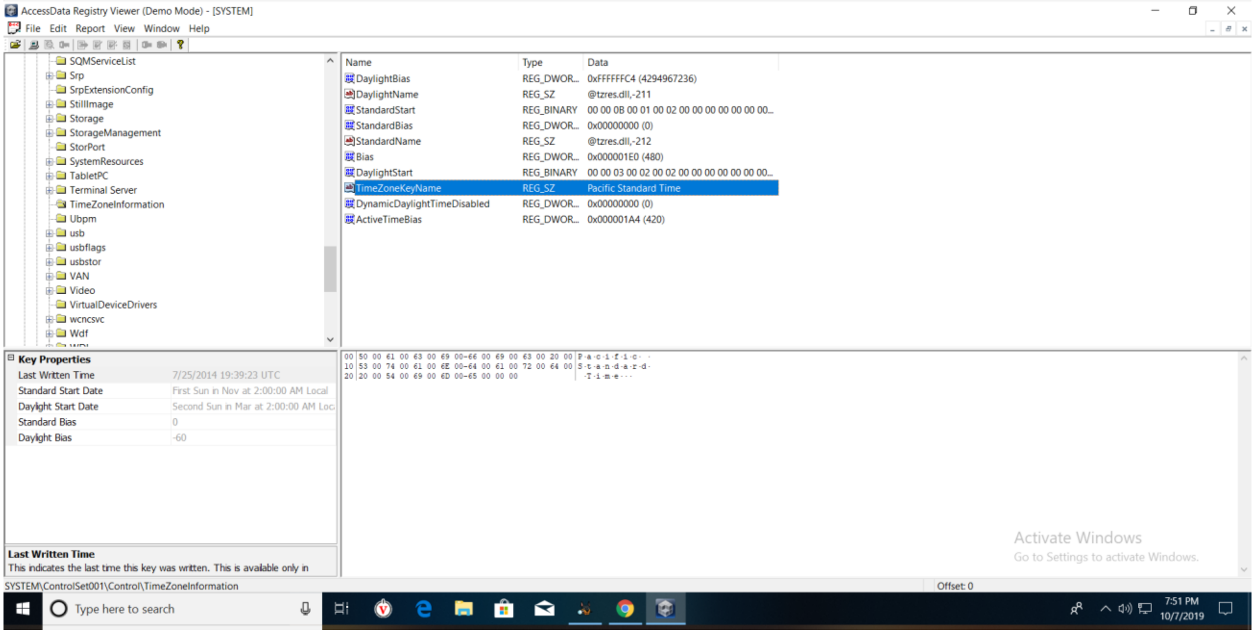
```
0|47 00 43 00 46 00 49 00-35 00 45 00 00 00      |G·C·F·I·5·E···
```

Last Written Time
This indicates the last time this key was written. This is available only in

SYSTEM\ControlSet001\Control\ComputerName\ComputerName   Offset: 0

2. Scroll down to TimeZoneInformation to identify the computer's time zone.

   Computer's Time Zone is: Pacific Standard Time (PST)


AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help
Type here to search
Activate Windows
Go to Settings to activate Windows.
7:51 PM
10/7/2019

SQMServiceList
Srp
SrpExtensionConfig
StillImage
Storage
StorageManagement
StorPort
SystemResources
TabletPC
Terminal Server
TimeZoneInformation
Ubpm
usb
usbflags
usbstor
VAN
Video
VirtualDeviceDrivers
wcncsvc
Wdf

Name	Type	Data
DaylightBias	REG_DWOR...	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-211
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00...
StandardBias	REG_DWOR...	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-212
Bias	REG_DWOR...	0x000001E0 (480)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00...
TimeZoneKeyName	REG_SZ	Pacific Standard Time
DynamicDaylightTimeDisabled	REG_DWOR...	0x00000000 (0)
ActiveTimeBias	REG_DWOR...	0x000001A4 (420)

Key Properties

Last Written Time	7/25/2014 19:39:23 UTC
Standard Start Date	First Sun in Nov at 2:00:00 AM Local
Daylight Start Date	Second Sun in Mar at 2:00:00 AM Loc
Standard Bias	0
Daylight Bias	-60

```
00|50 00 61 00 63 00 69 00-66 00 69 00 63 00 20 00|P·a·c·i·f·i·c· ·
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···
```

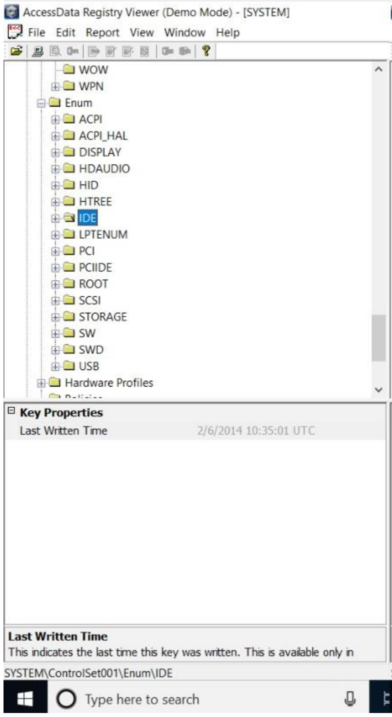
Last Written Time
This indicates the last time this key was written. This is available only in

SYSTEM\ControlSet001\Control\TimeZoneInformation   Offset: 0

3. Expand the Enum folder and then IDE and USB to view the IDE and USB based storage devices plugged into the computer, and when they were last accessed.

   IDE was last written on: 2/6/2014 10:35:01 UTC

   USB was last written on: 7/23/2014 3:50:35 UTC



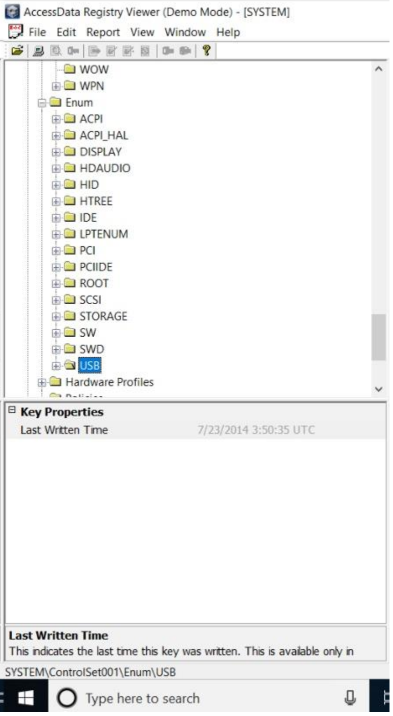
Key Properties

Last Written Time	2/6/2014 10:35:01 UTC

Last Written Time

This indicates the last time this key was written. This is available only in

SYSTEM\ControlSet001\Enum\IDE



Key Properties

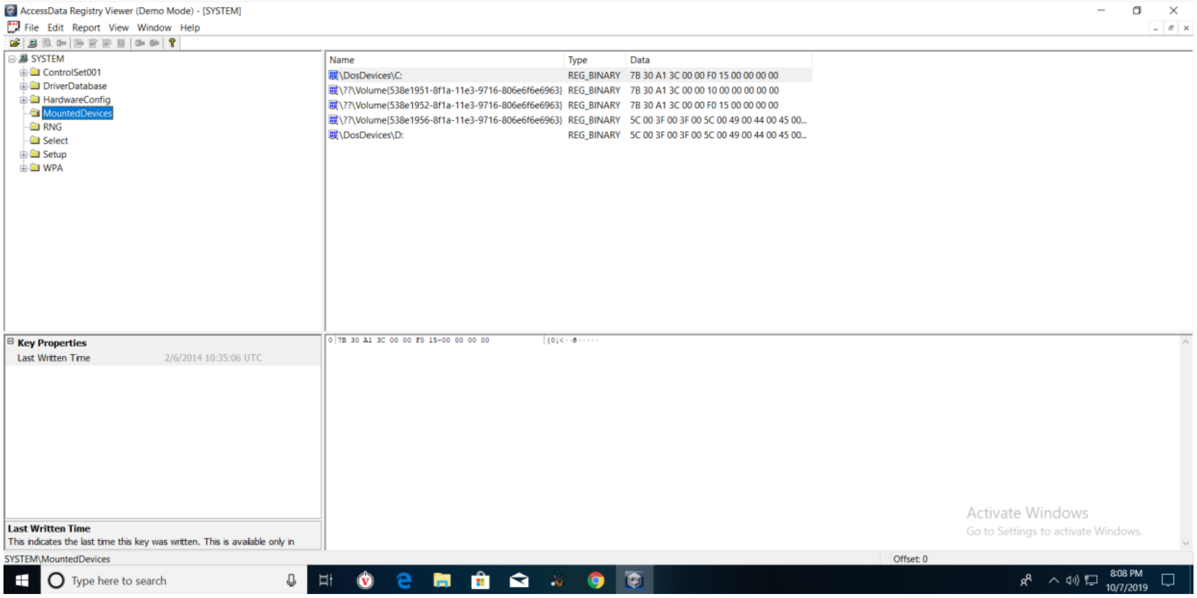
Last Written Time	7/23/2014 3:50:35 UTC

Last Written Time

This indicates the last time this key was written. This is available only in

SYSTEM\ControlSet001\Enum\USB

4. Click on System-MountedDevices to see the list of every storage device that was mounted into the Windows OS and it's associated drive letter/GUID value.



Name	Type	Data
\DosDevices\C:	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\??\Volume{538e1951-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	7B 30 A1 3C 00 00 10 00 00 00 00 00
\??\Volume{538e1952-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\??\Volume{538e1956-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00...
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00...

Key Properties

Last Written Time	2/6/2014 10:35:06 UTC

```
0 |7B 30 A1 3C 00 00 F0 15-00 00 00 00   |{0;<··ð·····
```

Last Written Time

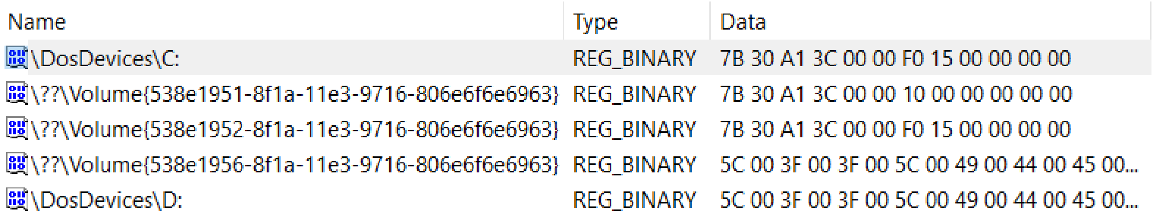
This indicates the last time this key was written. This is available only in

SYSTEM\MountedDevices

Offset: 0

5. How many mounted devices on the system have an assigned drive letter?

   A total of 5 device were mounted out of which 2 devices had a drive letter assigned, C & D.



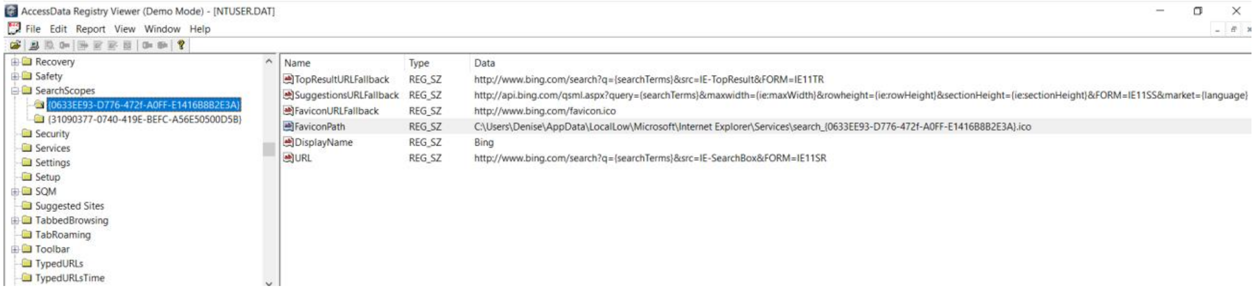
Name	Type	Data
\DosDevices\C:	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\??\Volume{538e1951-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	7B 30 A1 3C 00 00 10 00 00 00 00 00
\??\Volume{538e1952-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\??\Volume{538e1956-8f1a-11e3-9716-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00...
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00...

Part 3. Examining the NTUSER.DAT File

1. GUID associated with the username

   A GUID is an acronym that stands for *Globally Unique Identifier*, they are 128-bit unique reference numbers. It follows a specific structure xxxxxxxx-xxxx-Mxxx-Nxxx-xxxxxxxxxxxx. GUID is typically created by Microsoft, so traversing through the registry hive we find two such values

   0633EE93-D776-472f-A0FF-F1416B8B3E3A and 31090377-0740-419E-A56E50500D5B.

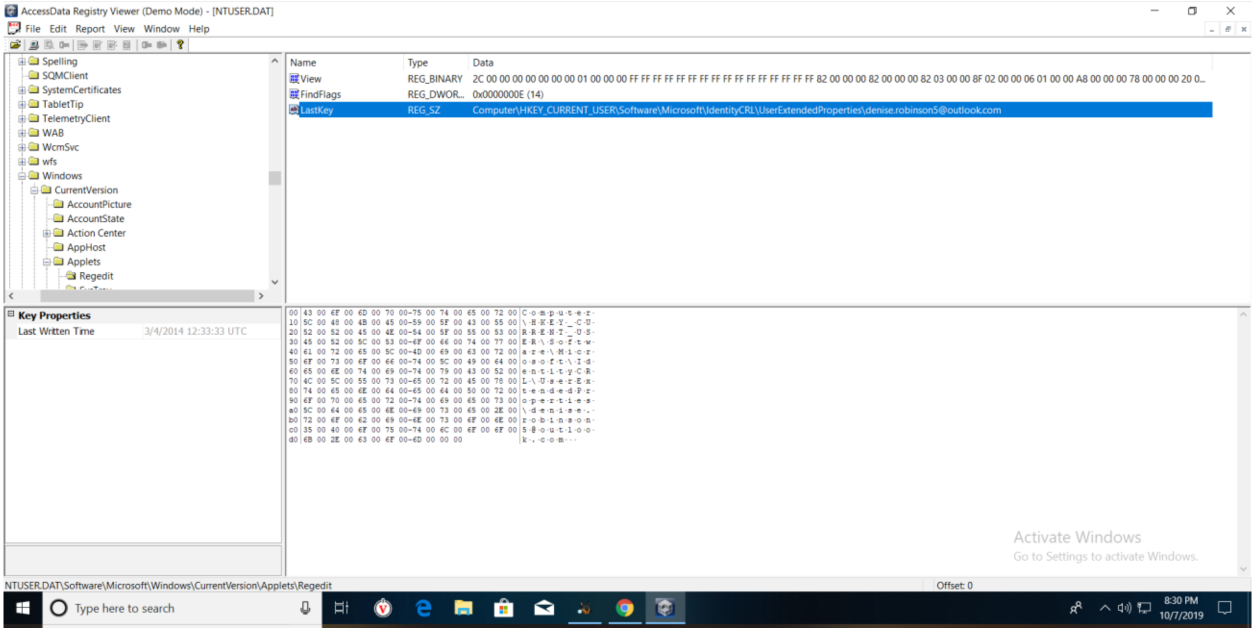


```
Recovery
Safety
SearchScopes
    {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
    {31090377-0740-419E-BEFC-A56E50500D5B}
Security
Services
Settings
Setup
SQM
Suggested Sites
TabbedBrowsing
TabRoaming
Toolbar
TypedURLs
TypedURLsTime
```

Name	Type	Data
TopResultURLFallback	REG_SZ	http://www.bing.com/search?q={searchTerms}&src=IE-TopResult&FORM=IE11TR
SuggestionsURLFallback	REG_SZ	http://api.bing.com/qsml.aspx?query={searchTerms}&maxwidth={ie:maxWidth}&rowheight={ie:rowHeight}&sectionHeight={ie:sectionHeight}&FORM=IE11SS&market={language}
FaviconURLFallback	REG_SZ	http://www.bing.com/favicon.ico
FaviconPath	REG_SZ	C:\Users\Denise\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico
DisplayName	REG_SZ	Bing
URL	REG_SZ	http://www.bing.com/search?q={searchTerms}&src=IE-SearchBox&FORM=IE11SR

2. Email account information

   Email: denise.robinson5@outlook.com



Name	Type	Data
View	REG_BINARY	2C 00 00 00 00 00 00 00 01 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 82 00 00 00 82 00 00 00 82 03 00 00 8F 02 00 00 06 01 00 00 A8 00 00 00 78 00 00 00 20 0...
FindFlags	REG_DWOR...	0x0000000E (14)
LastKey	REG_SZ	Computer\HKEY_CURRENT_USER\Software\Microsoft\IdentityCRL\UserExtendedProperties\denise.robinson5@outlook.com

```
00 43 00 6F 00 6D 00 70 00-75 00 74 00 65 00 72 00 C·o·m·p·u·t·e·r·
10 5C 00 48 00 4B 00 45 00-59 00 5F 00 43 00 55 00 \·H·K·E·Y·_·C·U·
20 52 00 52 00 45 00 4E 00-54 00 5F 00 55 00 53 00 R·R·E·N·T·_·U·S·
30 45 00 52 00 5C 00 53 00-6F 00 66 00 74 00 77 00 E·R·\·S·o·f·t·w·
40 61 00 72 00 65 00 5C 00-4D 00 69 00 63 00 72 00 a·r·e·\·M·i·c·r·
50 6F 00 73 00 6F 00 66 00-74 00 5C 00 49 00 64 00 o·s·o·f·t·\·I·d·
60 65 00 6E 00 74 00 69 00-74 00 79 00 43 00 52 00 e·n·t·i·t·y·C·R·
70 4C 00 5C 00 55 00 73 00-65 00 72 00 45 00 78 00 L·\·U·s·e·r·E·x·
80 74 00 65 00 6E 00 64 00-65 00 64 00 50 00 72 00 t·e·n·d·e·d·P·r·
90 6F 00 70 00 65 00 72 00-74 00 69 00 65 00 73 00 o·p·e·r·t·i·e·s·
a0 5C 00 64 00 65 00 6E 00-69 00 73 00 65 00 2E 00 \·d·e·n·i·s·e·.·
b0 72 00 6F 00 62 00 69 00-6E 00 73 00 6F 00 6E 00 r·o·b·i·n·s·o·n·
c0 35 00 40 00 6F 00 75 00-74 00 6C 00 6F 00 6F 00 5·@·o·u·t·l·o·o·
d0 6B 00 2E 00 63 00 6F 00-6D 00 00 00             k·.·c·o·m···
```

Key Properties

Last Written Time 3/4/2014 12:33:33 UTC

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Offset: 0

Click Edit-Find, and type “jfriday” in the resulting search box.

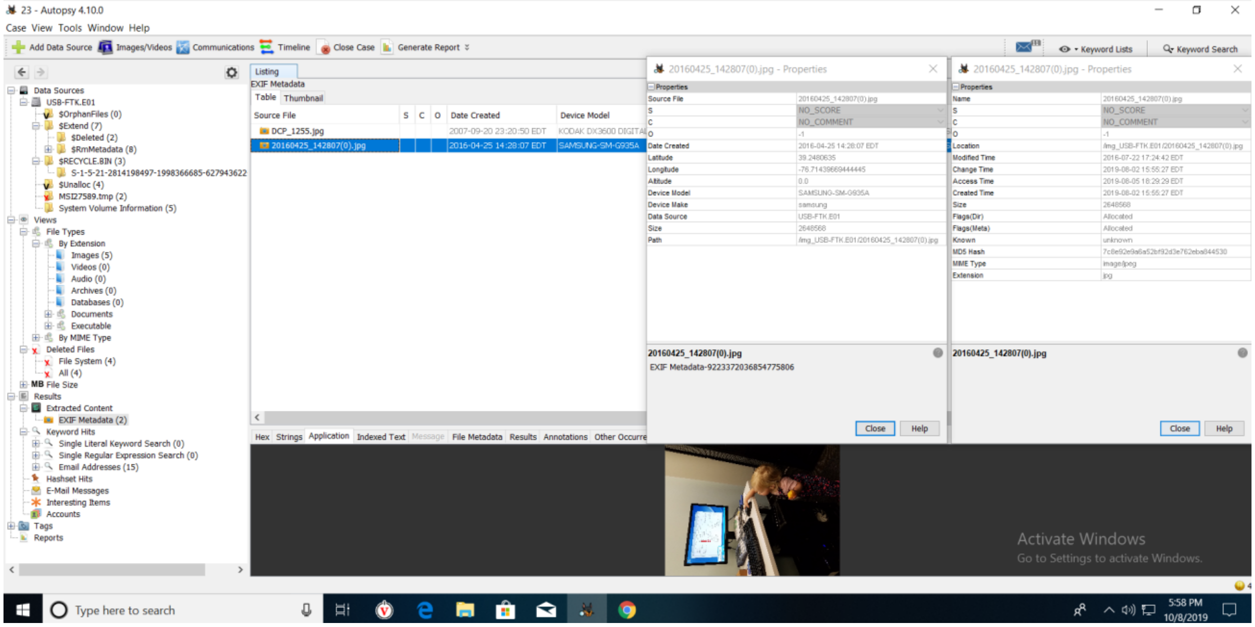
1. What information can you find for jfriday? Why?

   We are traversing through the registry file that is particular to Denise and that is reason why we can’t find any information related to jfriday.

Part 4: Analysis of image files

1. What information can you see related to the images you identified previously?

   For image 20160425_142807(0).jpg this is the information we get from autopsy



Source File	S	C	O	Date Created	Device Model
DCP_1255.jpg				2007-09-20 23:20:50 EDT	KODAK DX3600 DIGITAL
20160425_142807(0).jpg				2016-04-25 14:28:07 EDT	SAMSUNG-SM-G935A

20160425_142807(0).jpg - Properties

Properties	
Source File	20160425_142807(0).jpg
S	NO_SCORE
C	NO_COMMENT
O	-1
Date Created	2016-04-25 14:28:07 EDT
Latitude	39.2480635
Longitude	-76.71439669444445
Altitude	0.0
Device Model	SAMSUNG-SM-G935A
Device Make	samsung
Data Source	USB-FTK.E01
Size	2648568
Path	/img_USB-FTK.E01/20160425_142807(0).jpg

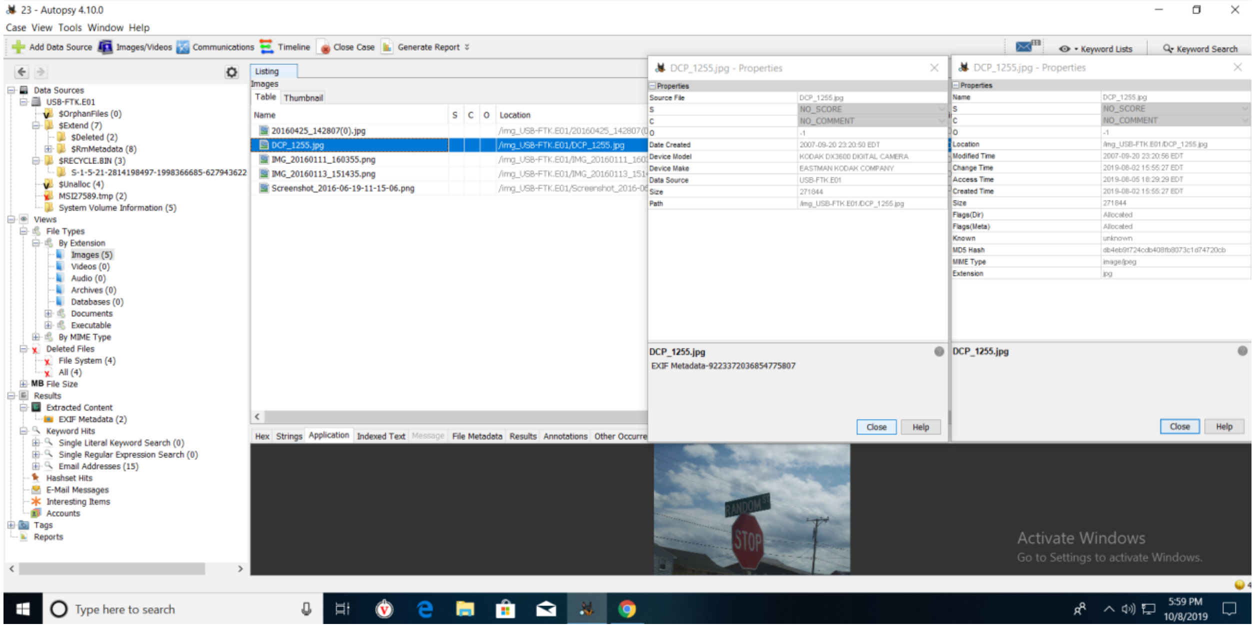
20160425_142807(0).jpg
EXIF Metadata-9223372036854775806

20160425_142807(0).jpg - Properties

Properties	
Name	20160425_142807(0).jpg
S	NO_SCORE
C	NO_COMMENT
O	-1
Location	/img_USB-FTK.E01/20160425_142807(0).jpg
Modified Time	2016-07-22 17:24:42 EDT
Change Time	2019-08-02 15:55:27 EDT
Access Time	2019-08-05 18:29:29 EDT
Created Time	2019-08-02 15:55:27 EDT
Size	2648568
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
MD5 Hash	7c8e92e9a6a52bf92d3e762eba844530
MIME Type	image/jpeg
Extension	jpg

20160425_142807(0).jpg

For image DCP_1255.jpg this is the information we get from autopsy.



Name	S	C	O	Location
20160425_142807(0).jpg				/img_USB-FTK.E01/20160425_142807(0
DCP_1255.jpg				/img_USB-FTK.E01/DCP_1255.jpg
IMG_20160111_160355.png				/img_USB-FTK.E01/IMG_20160111_160
IMG_20160113_151435.png				/img_USB-FTK.E01/IMG_20160113_151
Screenshot_2016-06-19-11-15-06.png				/img_USB-FTK.E01/Screenshot_2016-06

DCP_1255.jpg - Properties

Properties	
Source File	DCP_1255.jpg
S	NO_SCORE
C	NO_COMMENT
O	-1
Date Created	2007-09-20 23:20:50 EDT
Device Model	KODAK DX3600 DIGITAL CAMERA
Device Make	EASTMAN KODAK COMPANY
Data Source	USB-FTK.E01
Size	271844
Path	/img_USB-FTK.E01/DCP_1255.jpg

DCP_1255.jpg
EXIF Metadata-9223372036854775807

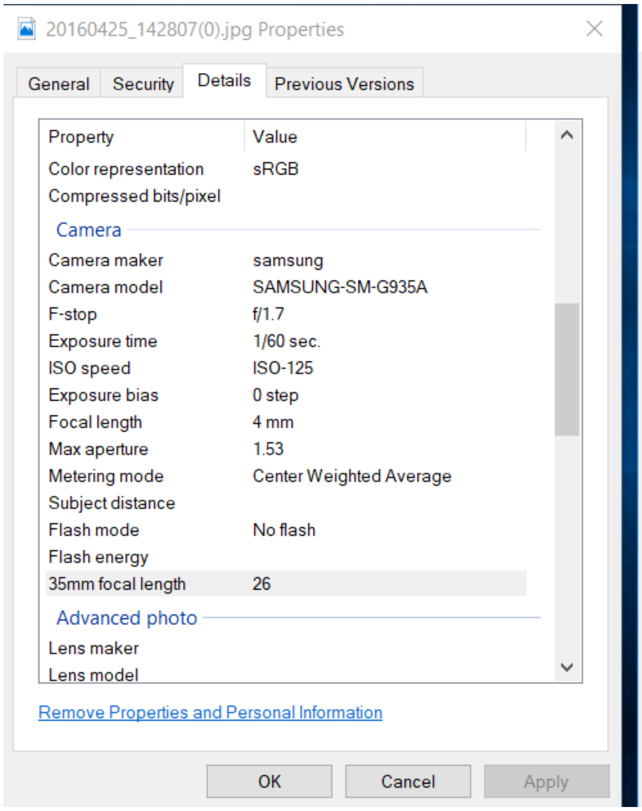
DCP_1255.jpg - Properties

Properties	
Name	DCP_1255.jpg
S	NO_SCORE
C	NO_COMMENT
O	-1
Location	/img_USB-FTK.E01/DCP_1255.jpg
Modified Time	2007-09-20 23:20:56 EDT
Change Time	2019-08-02 15:55:27 EDT
Access Time	2019-08-05 18:29:29 EDT
Created Time	2019-08-02 15:55:27 EDT
Size	271844
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
MD5 Hash	db4eb9f724cdb408fb8073c1d74720cb
MIME Type	image/jpeg
Extension	jpg

DCP_1255.jpg

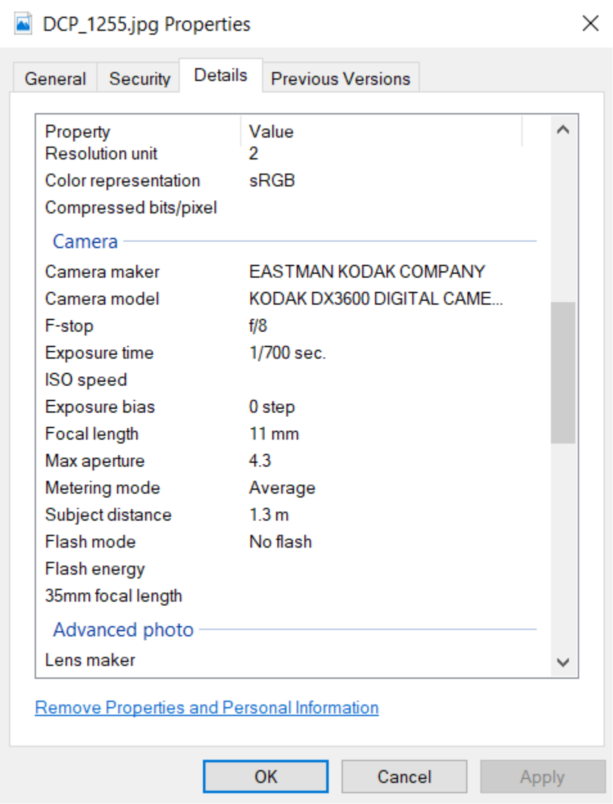
When viewing through the EXIF meta data we get additional information about ithe image such as the make and model of the device that was used to take the picture and/ or the exact the location the picture was taken.

2. Do you see any additional EXIF Metadata that wasn't present in Autopsy?



20160425_142807(0).jpg Properties

Property	Value
Color representation	sRGB
Compressed bits/pixel	
Camera	
Camera maker	samsung
Camera model	SAMSUNG-SM-G935A
F-stop	f/1.7
Exposure time	1/60 sec.
ISO speed	ISO-125
Exposure bias	0 step
Focal length	4 mm
Max aperture	1.53
Metering mode	Center Weighted Average
Subject distance	
Flash mode	No flash
Flash energy	
35mm focal length	26
Advanced photo	
Lens maker	
Lens model	

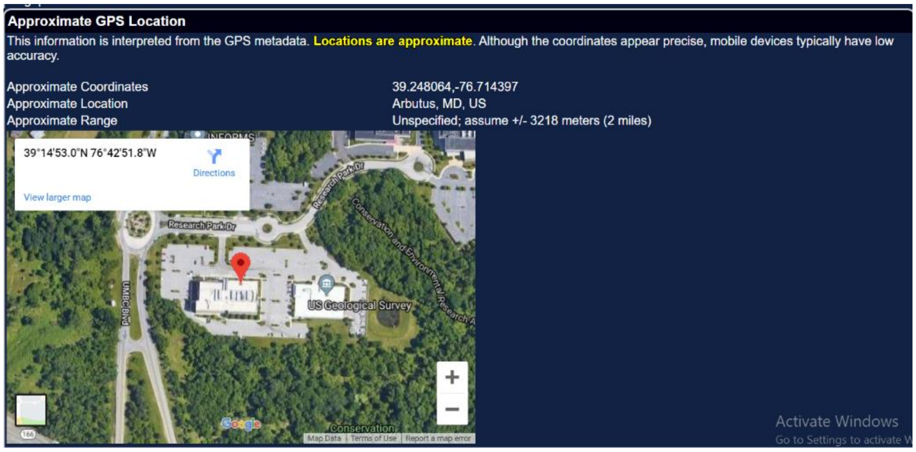


DCP_1255.jpg Properties

Property	Value
Resolution unit	2
Color representation	sRGB
Compressed bits/pixel	
Camera	
Camera maker	EASTMAN KODAK COMPANY
Camera model	KODAK DX3600 DIGITAL CAME...
F-stop	f/8
Exposure time	1/700 sec.
ISO speed	
Exposure bias	0 step
Focal length	11 mm
Max aperture	4.3
Metering mode	Average
Subject distance	1.3 m
Flash mode	No flash
Flash energy	
35mm focal length	
Advanced photo	
Lens maker	

We do find some additional information related to the device and the settings which were used to take the picture, such as the ISO, focal length, metering mode, etc.

1. Any additional EXIF Metadata, such as a location where the image was captured?



Approximate GPS Location

This information is interpreted from the GPS metadata. Locations are approximate. Although the coordinates appear precise, mobile devices typically have low accuracy.

Approximate Coordinates	39.248064,-76.714397
Approximate Location	Arbutus, MD, US
Approximate Range	Unspecified; assume +/- 3218 meters (2 miles)

39°14'53.0"N 76°42'51.8"W
Directions
View larger map
Research Park Dr
US Geological Survey
UMBC Blvd
Google
Map Data | Terms of Use | Report a map error
Activate Windows
Go to Settings to activate W

Yes, we find few additional files in EXIF data, such as lacation (not just coordinates). Other than that the information displayed in fotoforensics and autopsy are pretty much the same.

Conclusion

From this lab we learn how to use forensic tools such as autopsy, registry viewer, and websites like fotoforensics to go through evidence and find information to leverage on. We also learn how to go through the metadata of an image.