Lab 4 – Registry and Browser Forensics

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Gina Marie

Date – 9th July 2023

Week 4 Discussion -1:

Post the picture and give information regarding the picture this could include, device used to take the picture, GPS location, etc.

- I uploaded the above nature scenic picture on https://fotoforensics.com for analyzing metadata about the image and below is the link and analysis about the image: https://fotoforensics.com/analysis.php?id=2264b9aa5ce9555001923fc24eff7e754c1c879b.1072875
- Digest and Metadata tab contains details about the image filehash and metadata about the image.
- The file name is 20230710_090333.jpg, file type is jpeg and image size is 1,072,875 bytes
- Device use for taking this picture is Samsung Mobile and model name is Galaxy S23 Ultra. The picture is taken on 2023:07:10 09:03:33 and modified date is same.
- The MD5 hash of file is e22a91f72b4a27b96d700f9a57809ba7
- The GPS coordinate of picture is 37 deg 34' 12.00" N, 122 deg 4' 12.00" W
  GPS Latitude Ref – North
  GPS Longitude Ref – West
  GPS Altitude Ref – Above sea level
- The image unique ID is 6452b2d744fc55f00000000000000000
- ICC Profile Copyright - Copyright (c) 2022 Samsung Electronics Co., Ltd.
- Approximate Coordinates 37.57,-122.07
- Approximate Location 3.23 miles (5.20 km) NW of Newark, CA, US

Citations – Hany Farid. (n.d.). FotoForensics. Retrieved July 6, 2023, from https://fotoforensics.com/

Introduction – In this lab, as a forensic investigator, we will simulate the process of acquiring evidence into an image file. During the analysis, we will collect registry information from evidence image file as well as collect files and metadata from an image file for analysis purpose. The registry contain configuration settings and user activity data while image file data holds details regarding the image origin and creation details which will further help in preparing the comprehensive investigation report on the case.

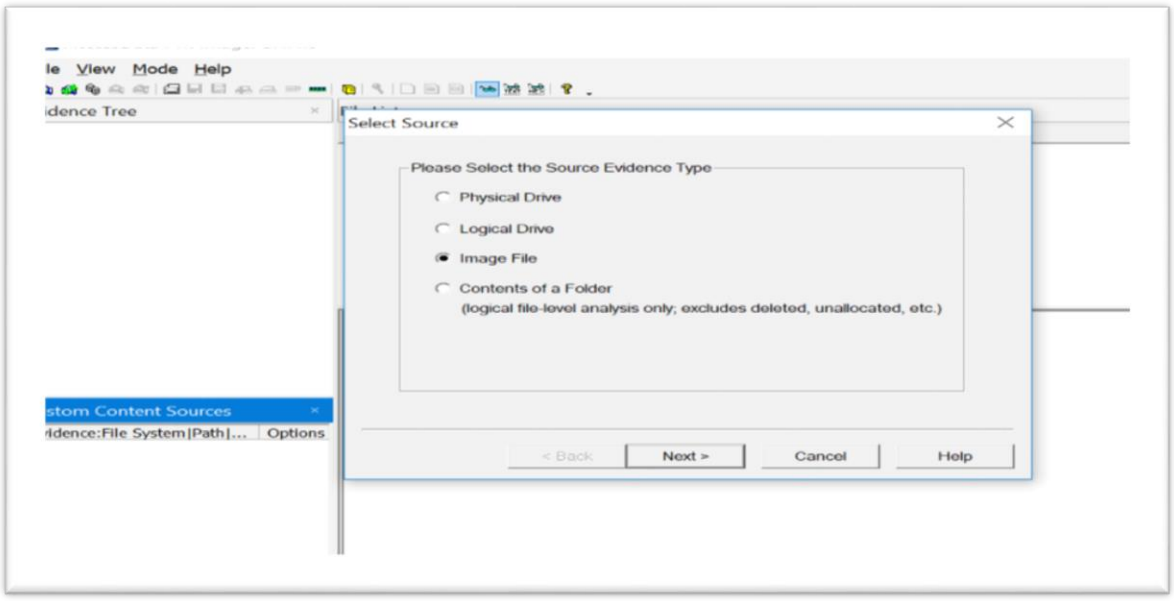
Pre-Analysis – We have created forensic images using 'ProDiscover' and 'FTK Imager'. Now we will be extracting registry information from an image file using 'FTK Imager'. Afterwards, we are going to analyze this extracted registry files using 'Registry Forensic' tool and will collect evidence from registry information and image file metadata.

Analysis –

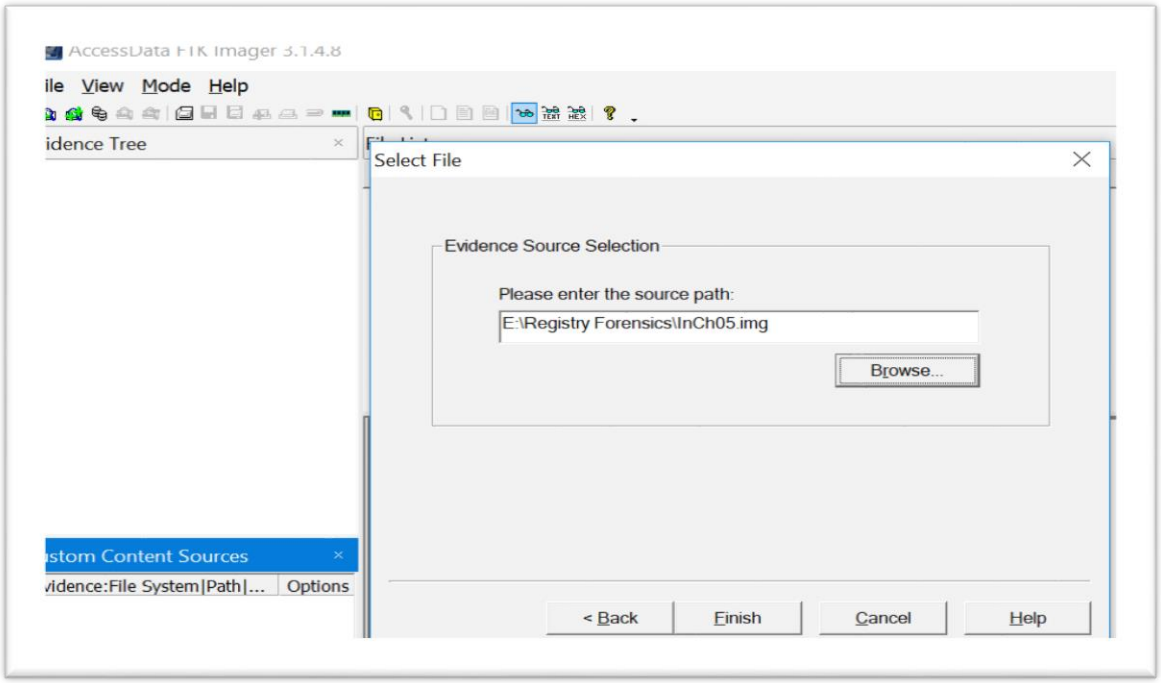
<u>Registry Forensics</u>

1. **Extracting Registry Files from Disk Image:**

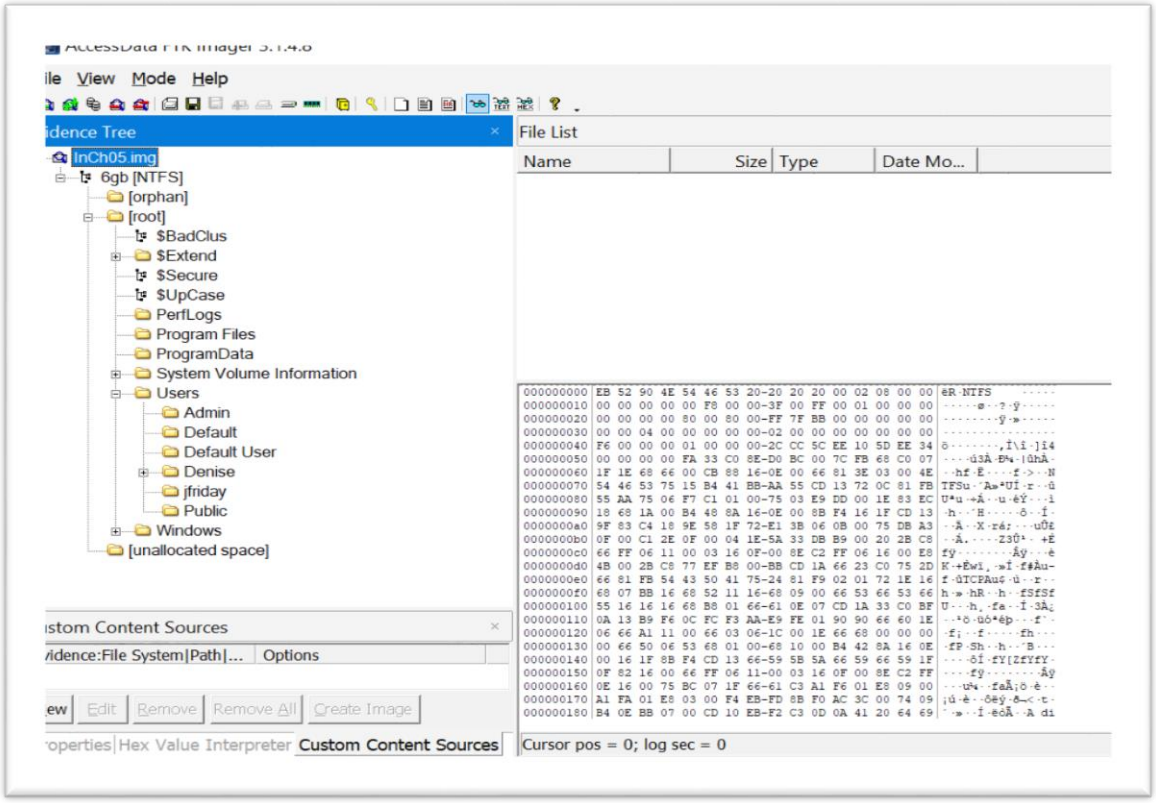
- Open FTK analyzer and click on File from the top left hand corner File → Add evidence Item. Click on image file → Next.



- Now browse to the Evidence drive → Registry Forensics and select InCh05.img and click on Finish.

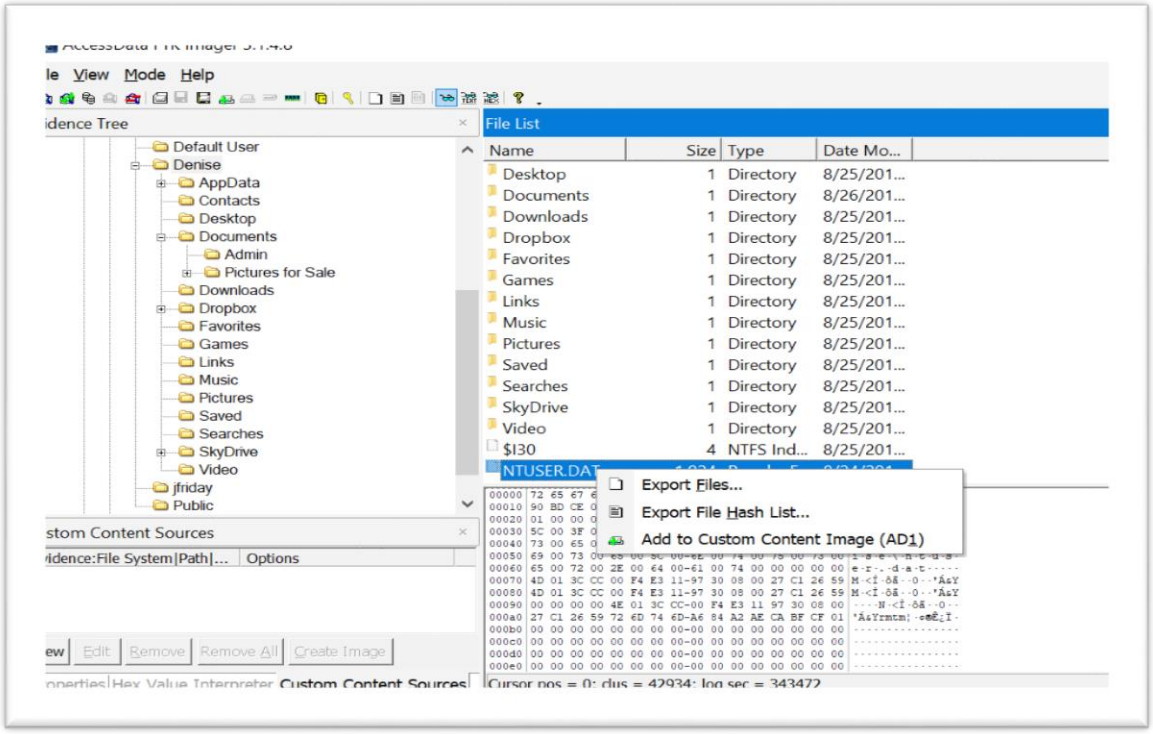


- In the left pane, expand to InCh05.img → 6gb [NTFS]→ [root]→ Users

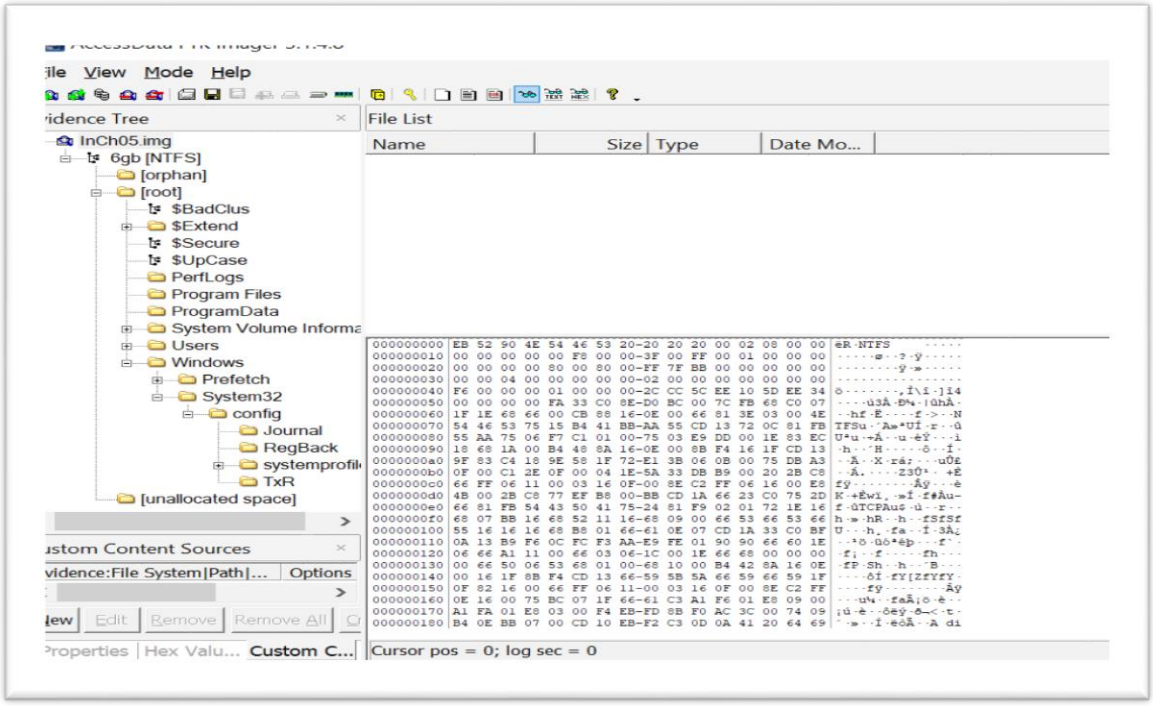


- Open the Denise folder and select NTUSER.dat, then right-click and select Export Files.

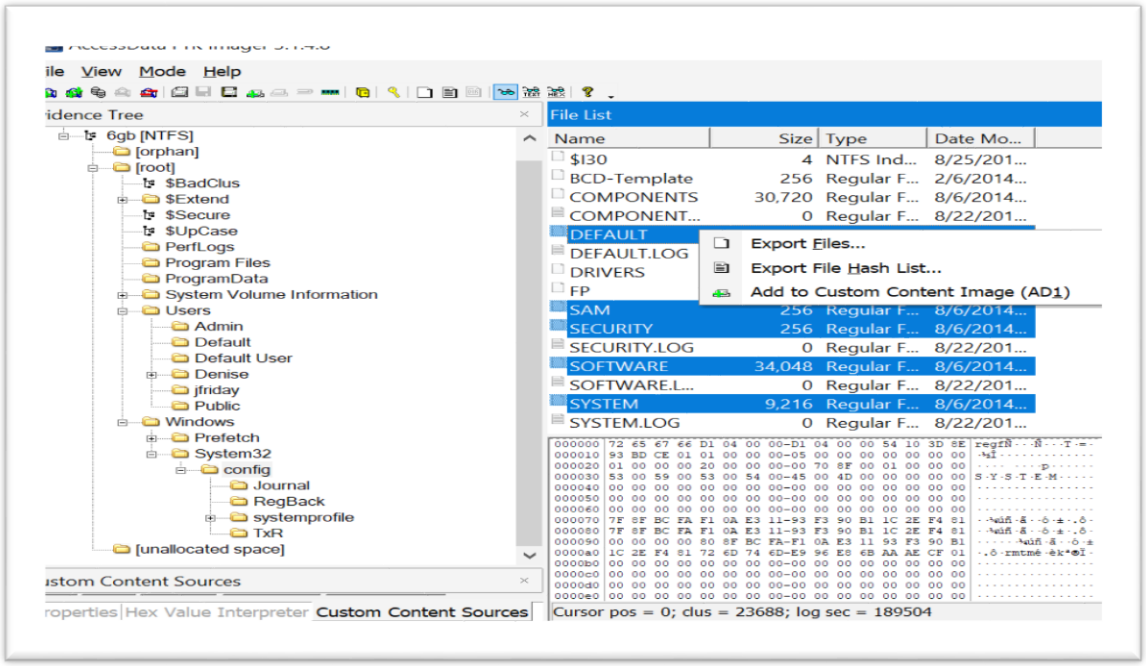
  Now export the NTUSER.dat file to a windows VM for later use.

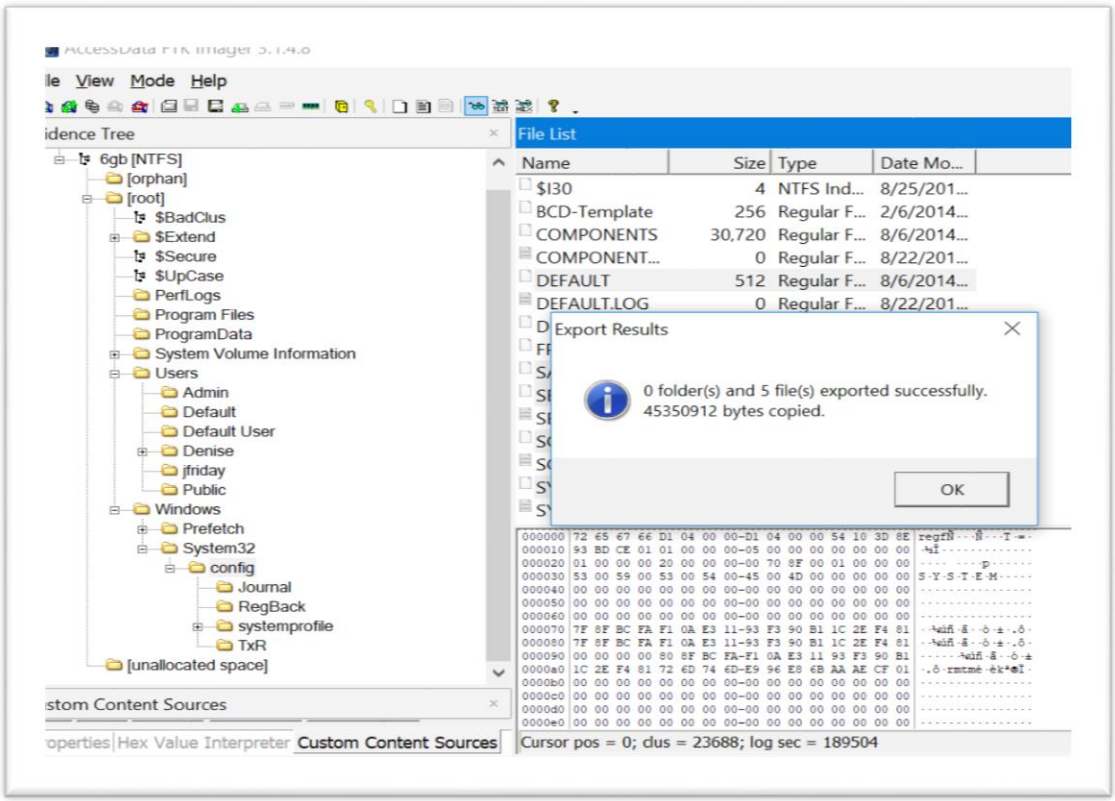


- In the left pane, expand to InCh05.img → 6gb [NTFS] →[root]→ Windows →System32→config.



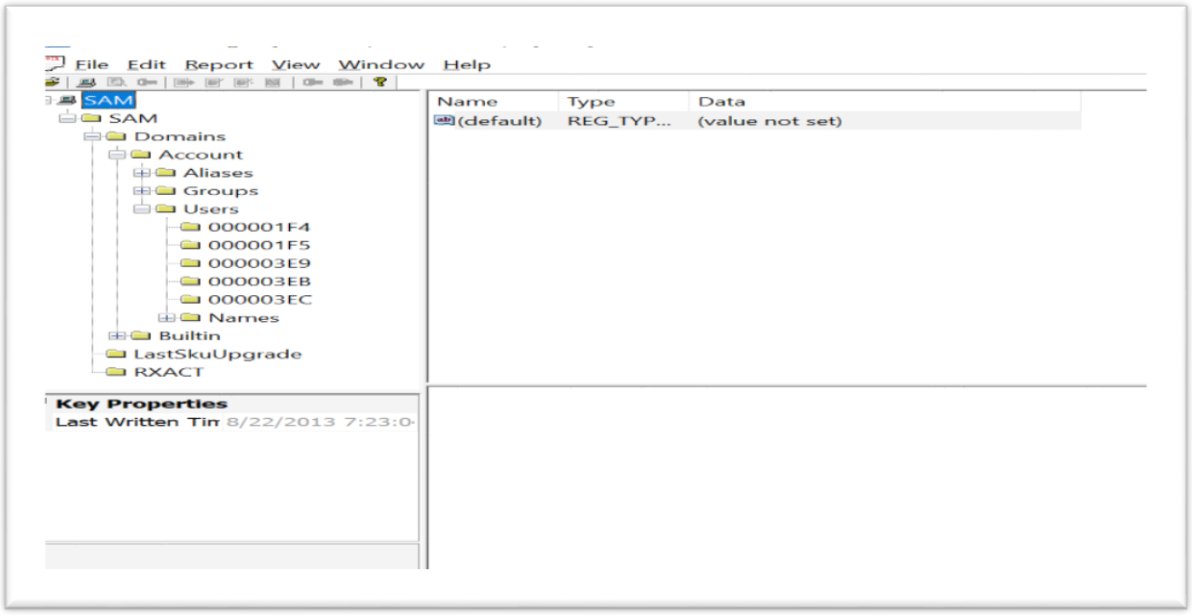
- Select SAM, DEFAULT, SYSTEM, SOFTWARE, SECURITY folders and export it to the same location as NTUSER.dat. [1]





2. Examining the SAM Hive:

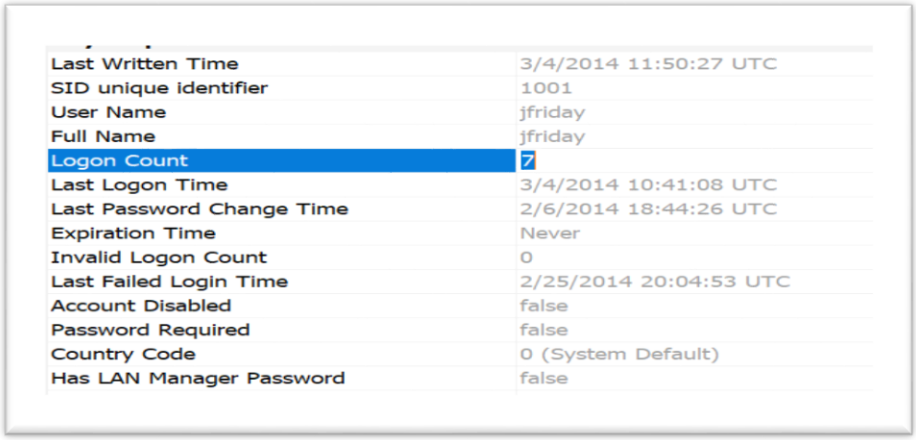
- SAM hive is a database file in the Microsoft Operating System that contains username and passwords. The main purpose of SAM is to make system more secure and protect from data breach. [3]
- It is located on HKEY_LOCAL_MACHINE\SAM : \system32\config\sam [1]
- Open the registry viewer in the Demo Mode for that click “No” and “Okay” to the resulting pop-ups referencing a Security licensing dongle.
- Now click File → Open and navigate to the folder where registry files are extracted and select SAM registry file. Now expand SAM → Domains → Account → Users folders.



- After exploring the user details under the user’s folder below is the analysis:

1. Which account logged into the system the most?

➢ Jfriday was logon to the account the most. His logon count is Count 7 times.

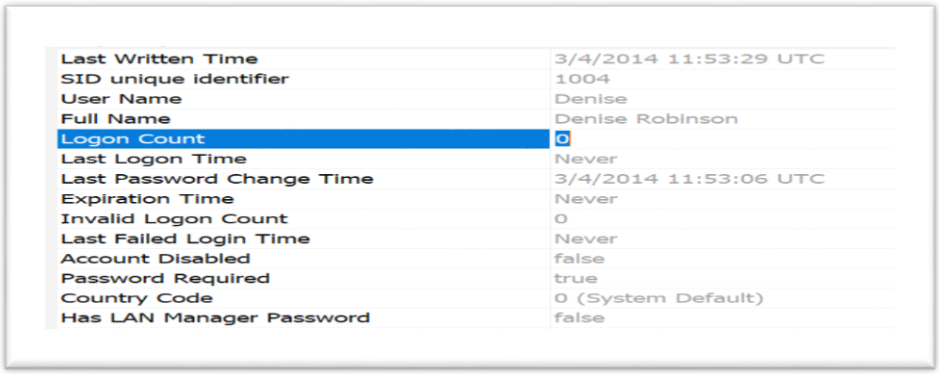


Last Written Time	3/4/2014 11:50:27 UTC
SID unique identifier	1001
User Name	jfriday
Full Name	jfriday
Logon Count	7
Last Logon Time	3/4/2014 10:41:08 UTC
Last Password Change Time	2/6/2014 18:44:26 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2/25/2014 20:04:53 UTC
Account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

2. Has Denise Robinson logged in?

➢ Denise Robinson was never login to the account as his logon count is ‘Zero’ and

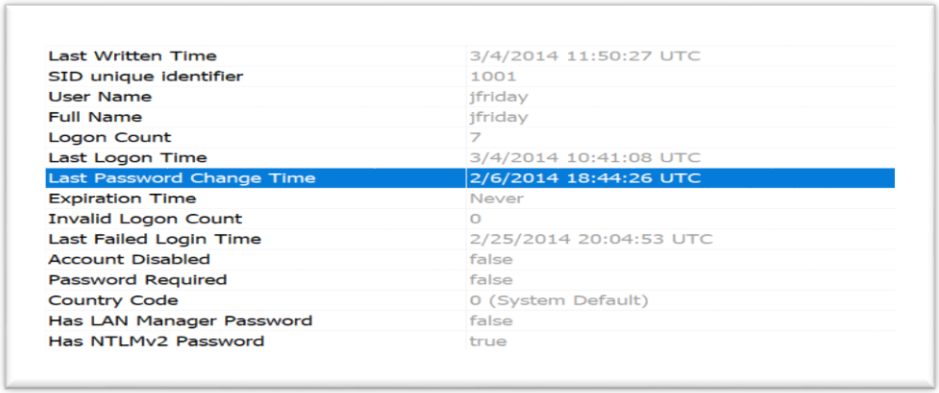
Last logon time is ‘Never’



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

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

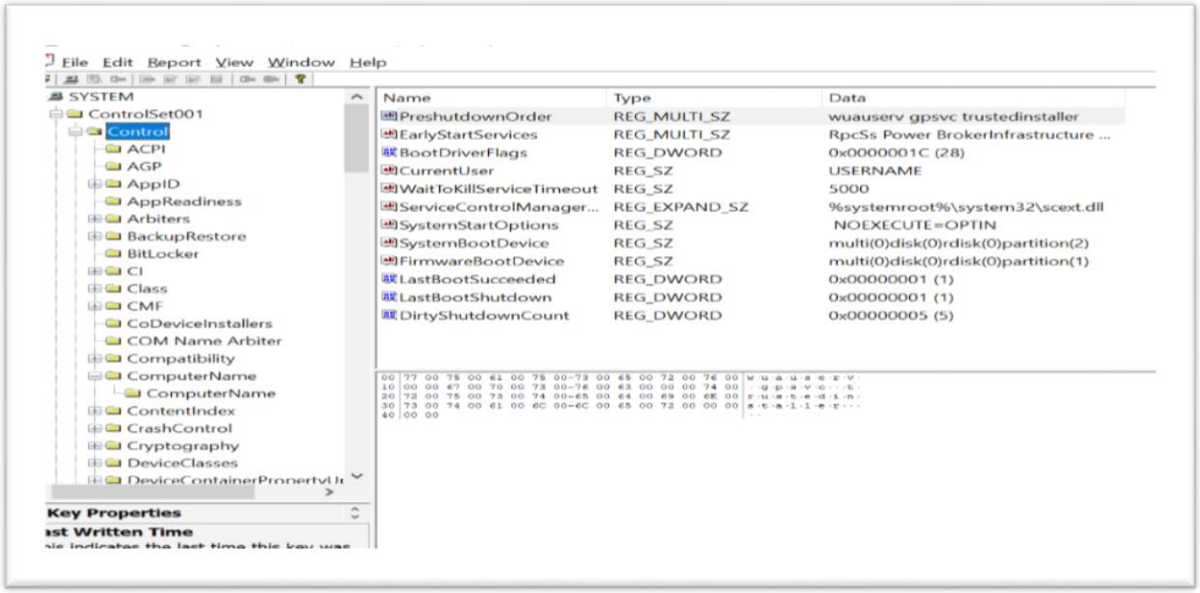
➢ Jfriday’s account password was last set at ‘02-06-2014 18:44:26 UTC’



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
Has NTLMv2 Password	true

3. Examining the SYSTEM Hive:

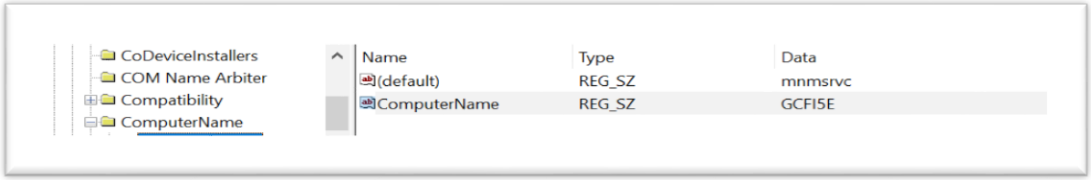
- It is located on path HKEY_LOCAL_MACHINE\SYSTEM : \system32\config\system [1]
- Now open the System registry file from the extracted registry files to examine the System Hive. Expand SYSTYEM → ControlSet001 → Control



- Below are the analysis after exploring details from the above folder.

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

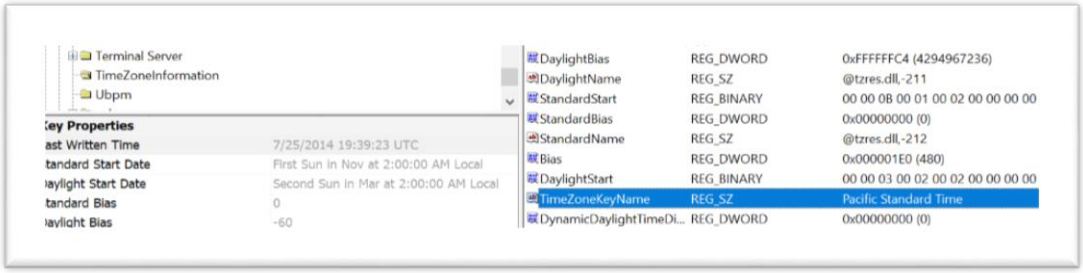
➢ Now navigate to the ComputerName → ComputerName folder to find computer name details. ComputerName : GCFI5E



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

➢ To get the Time Zone details navigate to the TimeZoneInformation folder

Computer's time zone is in 'Pacific Standard Time'

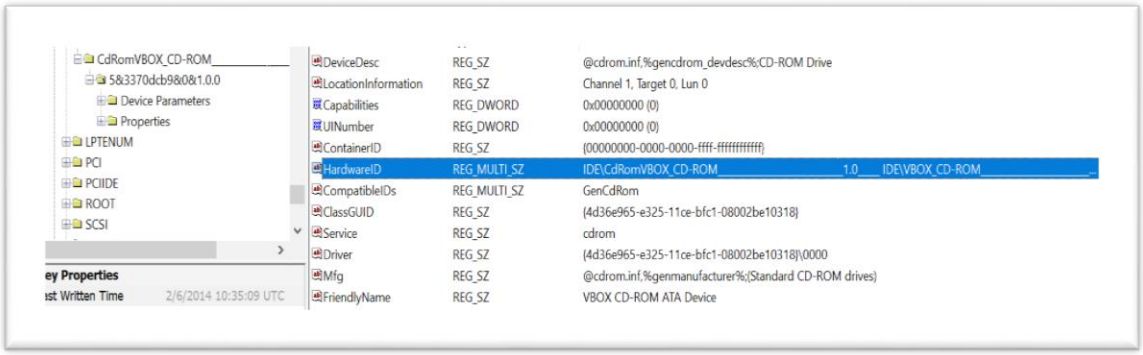


3. Expand the Enum folder and then IDE and USB to view the IDE and USB based storage devices plugged into the computer, and when they were last accessed.

➢ Navigate to the Enum → IDE folder to check the storage devices which were

connected to the computer and when they were last accessed

Last access Time – 02/06/2014 10:35:09 UTC



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

➢ Similarly, can check storage device details from USB folder.

Navigate to Enum → USB folder to check the storage devices which were

connected to the computer and when they were last accessed

Below are the list of storage devices and last connected date:

ROOT_HUB: 8/6/2014 2:54:48 UTC

VID_08C2&PID_50A5: 3/4/2014 14:17:28 UTC

VID_08DA&PID_0158: 7/24/2014 2:37:57 UTC

VID_1058&PID_10A2: 7/24/2014 2:37:36 UTC

VID_1241&PID_1203: 7/23/2014 10:20:27 UTC

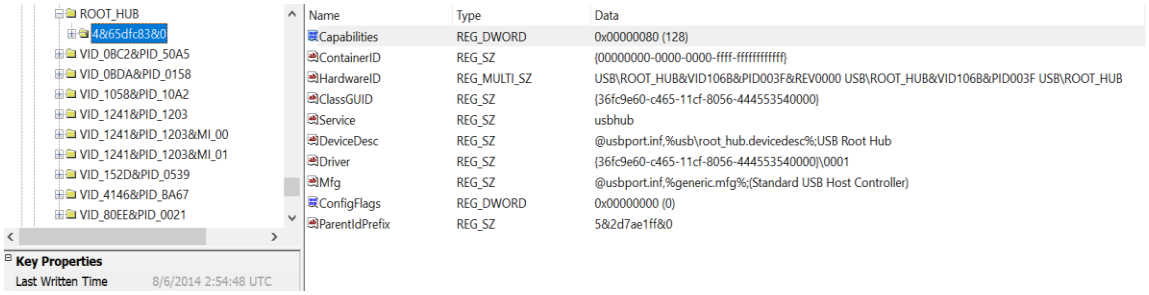
VID_1241&PID_1203&MI_00: 8/6/2014 2:54:49 UTC

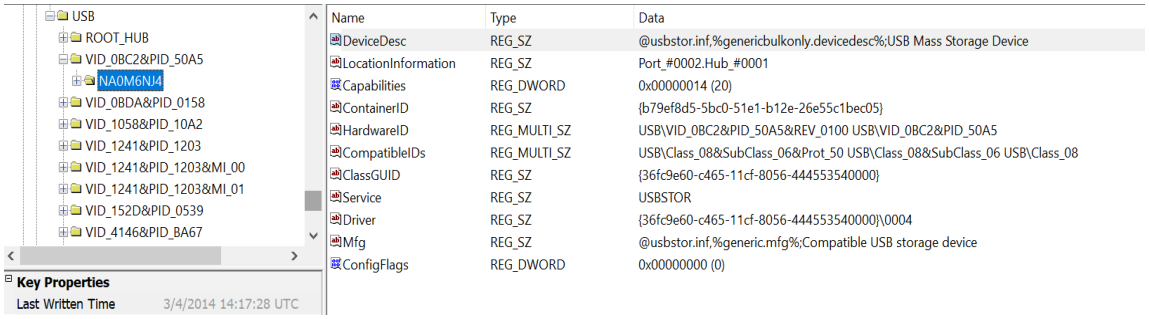
VID_1241&PID_1203&MI_01: 8/6/2014 2:54:49 UTC

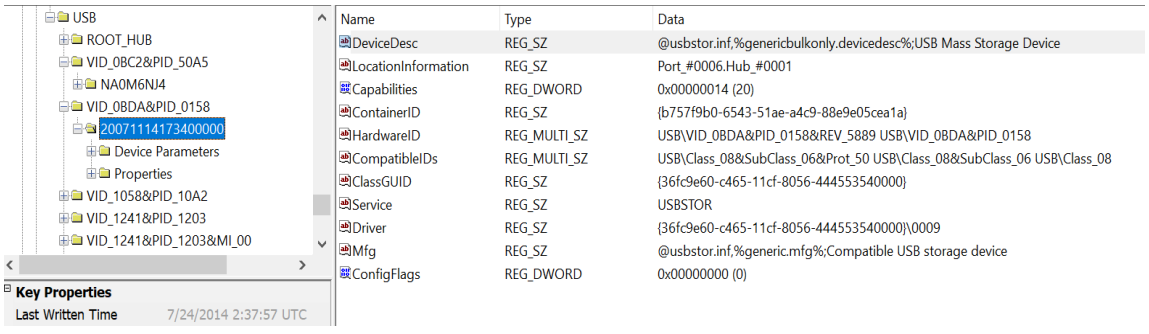
VID_152D&PID_0539: 7/23/2014 10:27:12 UTC

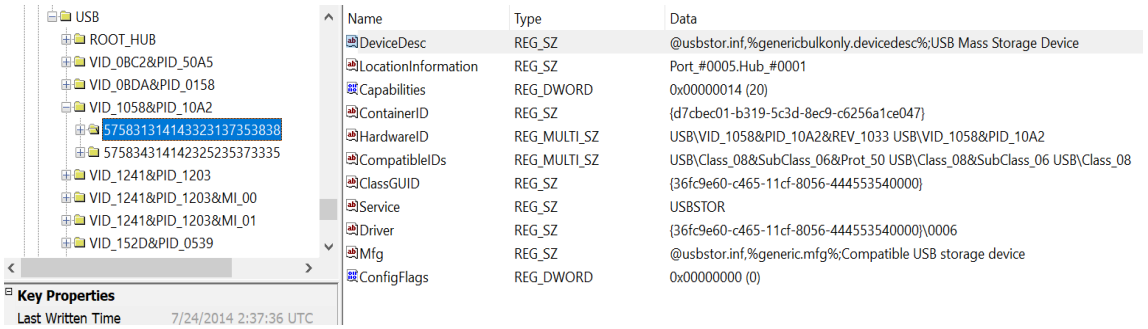
VID_4146&PID_BA67: 3/4/2014 14:25:03 UTC

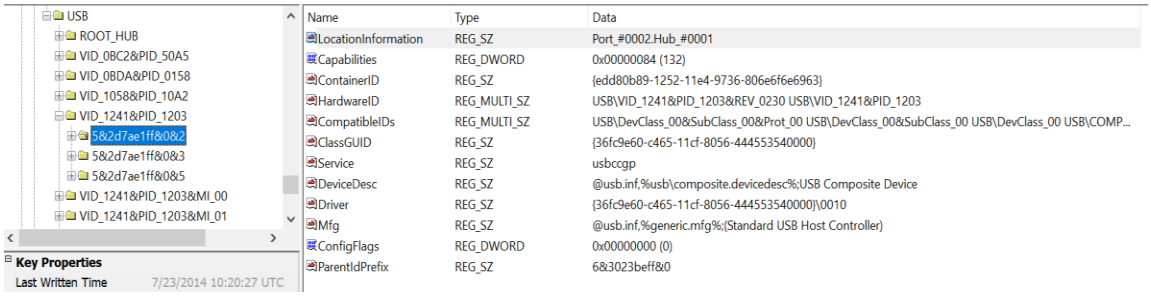
VID_80EE&PID_0021: 8/6/2014 2:54:48 UTC

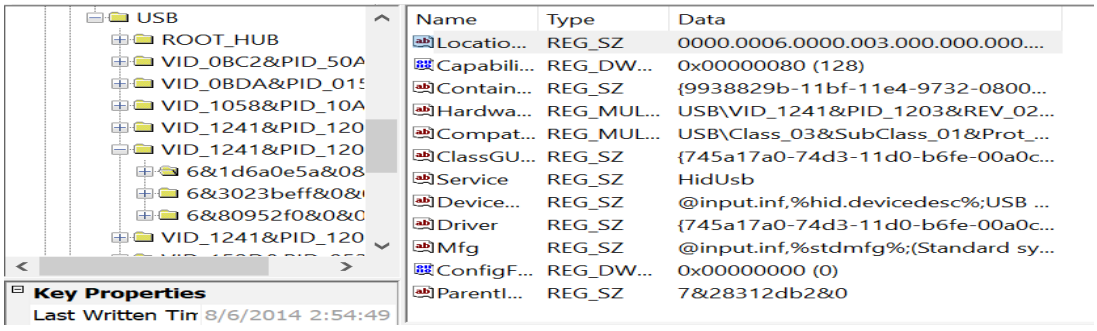


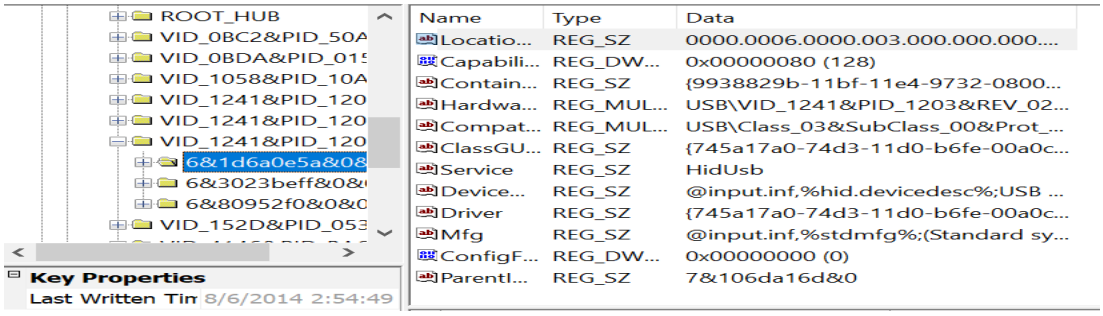


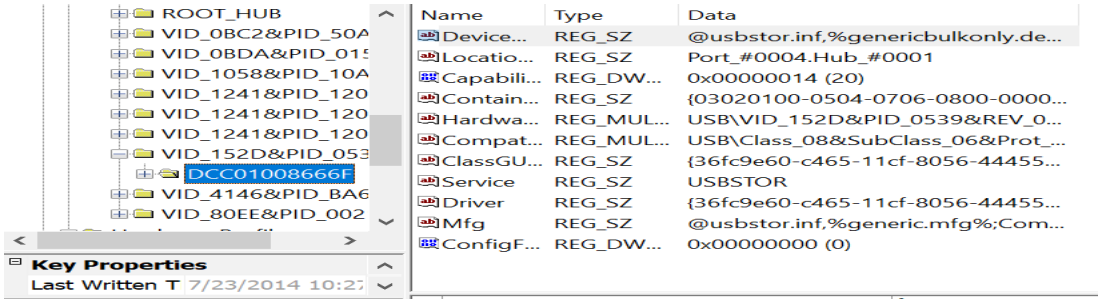


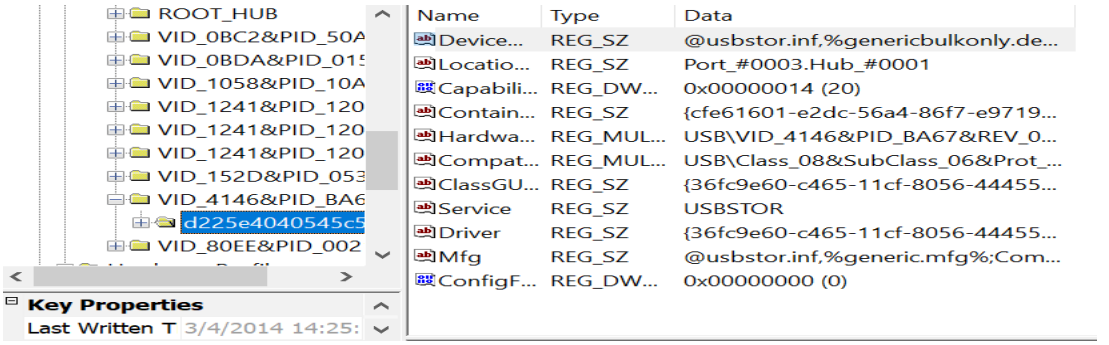

USB
ROOT_HUB
VID_0BC2&PID_50A5
VID_0BDA&PID_0158
VID_1058&PID_10A2
575831314143323137353838
575834314142325235373335
VID_1241&PID_1203
VID_1241&PID_1203&MI_00
VID_1241&PID_1203&MI_01
VID_152D&PID_0539
Key Properties
Last Written Time 7/24/2014 2:37:36 UTC
Name Type Data
DeviceDesc REG_SZ @usbstor.inf,%genericbulkonly.devicedesc%;USB Mass Storage Device
LocationInformation REG_SZ Port_#0005.Hub_#0001
Capabilities REG_DWORD 0x00000014 (20)
ContainerID REG_SZ {d7cbec01-b319-5c3d-8ec9-c6256a1ce047}
HardwareID REG_MULTI_SZ USB\VID_1058&PID_10A2&REV_1033 USB\VID_1058&PID_10A2
CompatibleIDs REG_MULTI_SZ USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ClassGUID REG_SZ {36fc9e60-c465-11cf-8056-444553540000}
Service REG_SZ USBSTOR
Driver REG_SZ {36fc9e60-c465-11cf-8056-444553540000}\0006
Mfg REG_SZ @usbstor.inf,%generic.mfg%;Compatible USB storage device
ConfigFlags REG_DWORD 0x00000000 (0)

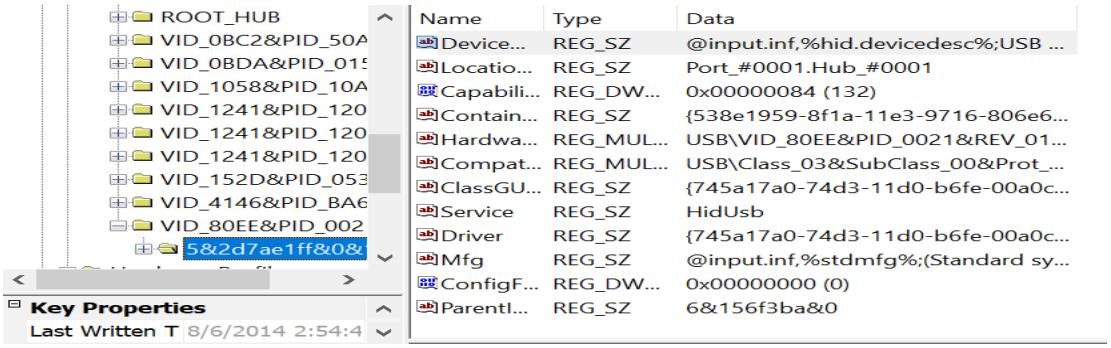

USB
ROOT_HUB
VID_0BC2&PID_50A5
VID_0BDA&PID_0158
VID_1058&PID_10A2
VID_1241&PID_1203
58&2d7ae1ff&0&2
58&2d7ae1ff&0&3
58&2d7ae1ff&0&5
VID_1241&PID_1203&MI_00
VID_1241&PID_1203&MI_01
Key Properties
Last Written Time 7/23/2014 10:20:27 UTC
Name Type Data
LocationInformation REG_SZ Port_#0002.Hub_#0001
Capabilities REG_DWORD 0x00000084 (132)
ContainerID REG_SZ {edd80b89-1252-11e4-9736-806e6f6e6963}
HardwareID REG_MULTI_SZ USB\VID_1241&PID_1203&REV_0230 USB\VID_1241&PID_1203
CompatibleIDs REG_MULTI_SZ USB\DevClass_00&SubClass_00&Prot_00 USB\DevClass_00&SubClass_00 USB\DevClass_00 USB\COMP...
ClassGUID REG_SZ {36fc9e60-c465-11cf-8056-444553540000}
Service REG_SZ usbccgp
DeviceDesc REG_SZ @usb.inf,%usb\composite.devicedesc%;USB Composite Device
Driver REG_SZ {36fc9e60-c465-11cf-8056-444553540000}\0010
Mfg REG_SZ @usb.inf,%generic.mfg%;(Standard USB Host Controller)
ConfigFlags REG_DWORD 0x00000000 (0)
ParentIdPrefix REG_SZ 6&3023beff&0


USB
ROOT_HUB
VID_0BC2&PID_50A
VID_0BDA&PID_015
VID_1058&PID_10A
VID_1241&PID_120
VID_1241&PID_120
6&1d6a0e5a&08
6&3023beff&0&
6&80952f0&0&0
VID_1241&PID_120
Key Properties
Last Written Tin 8/6/2014 2:54:49
Name Type Data
Locatio... REG_SZ 0000.0006.0000.003.000.000.000....
Capabili... REG_DW... 0x00000080 (128)
Contain... REG_SZ {9938829b-11bf-11e4-9732-0800...
Hardwa... REG_MUL... USB\VID_1241&PID_1203&REV_02...
Compat... REG_MUL... USB\Class_03&SubClass_01&Prot_...
ClassGU... REG_SZ {745a17a0-74d3-11d0-b6fe-00a0c...
Service REG_SZ HidUsb
Device... REG_SZ @input.inf,%hid.devicedesc%;USB ...
Driver REG_SZ {745a17a0-74d3-11d0-b6fe-00a0c...
Mfg REG_SZ @input.inf,%stdmfg%;(Standard sy...
ConfigF... REG_DW... 0x00000000 (0)
ParentI... REG_SZ 7&28312db2&0


ROOT_HUB
VID_0BC2&PID_50A
VID_0BDA&PID_015
VID_1058&PID_10A
VID_1241&PID_120
VID_1241&PID_120
VID_1241&PID_120
6&1d6a0e5a&08
6&3023beff&0&
6&80952f0&0&0
VID_152D&PID_053
Key Properties
Last Written Tin 8/6/2014 2:54:49
Name Type Data
Locatio... REG_SZ 0000.0006.0000.003.000.000.000....
Capabili... REG_DW... 0x00000080 (128)
Contain... REG_SZ {9938829b-11bf-11e4-9732-0800...
Hardwa... REG_MUL... USB\VID_1241&PID_1203&REV_02...
Compat... REG_MUL... USB\Class_03&SubClass_00&Prot_...
ClassGU... REG_SZ {745a17a0-74d3-11d0-b6fe-00a0c...
Service REG_SZ HidUsb
Device... REG_SZ @input.inf,%hid.devicedesc%;USB ...
Driver REG_SZ {745a17a0-74d3-11d0-b6fe-00a0c...
Mfg REG_SZ @input.inf,%stdmfg%;(Standard sy...
ConfigF... REG_DW... 0x00000000 (0)
ParentI... REG_SZ 7&106da16d&0


ROOT_HUB
VID_0BC2&PID_50A
VID_0BDA&PID_015
VID_1058&PID_10A
VID_1241&PID_120
VID_1241&PID_120
VID_1241&PID_120
VID_152D&PID_053
DCC01008666F
VID_4146&PID_BA6
VID_80EE&PID_002
Key Properties
Last Written T 7/23/2014 10:27
Name Type Data
Device... REG_SZ @usbstor.inf,%genericbulkonly.de...
Locatio... REG_SZ Port_#0004.Hub_#0001
Capabili... REG_DW... 0x00000014 (20)
Contain... REG_SZ {03020100-0504-0706-0800-0000...
Hardwa... REG_MUL... USB\VID_152D&PID_0539&REV_0...
Compat... REG_MUL... USB\Class_08&SubClass_06&Prot_...
ClassGU... REG_SZ {36fc9e60-c465-11cf-8056-44455...
Service REG_SZ USBSTOR
Driver REG_SZ {36fc9e60-c465-11cf-8056-44455...
Mfg REG_SZ @usbstor.inf,%generic.mfg%;Com...
ConfigF... REG_DW... 0x00000000 (0)

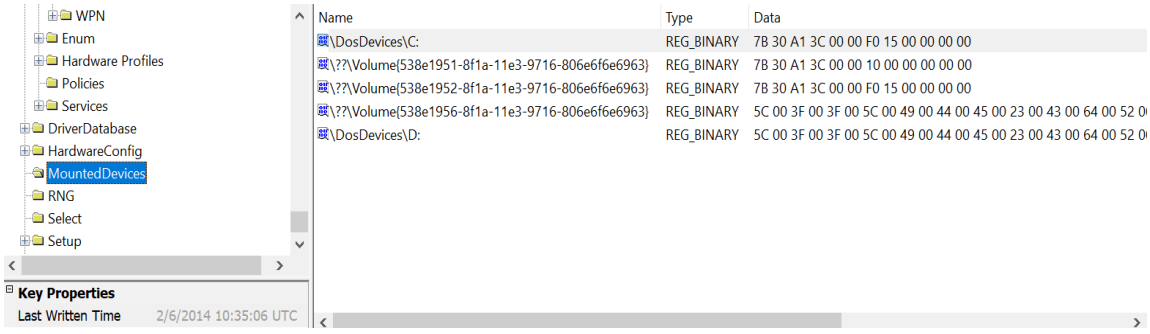




5. How many mounted devices on the system have an assigned drive letter?

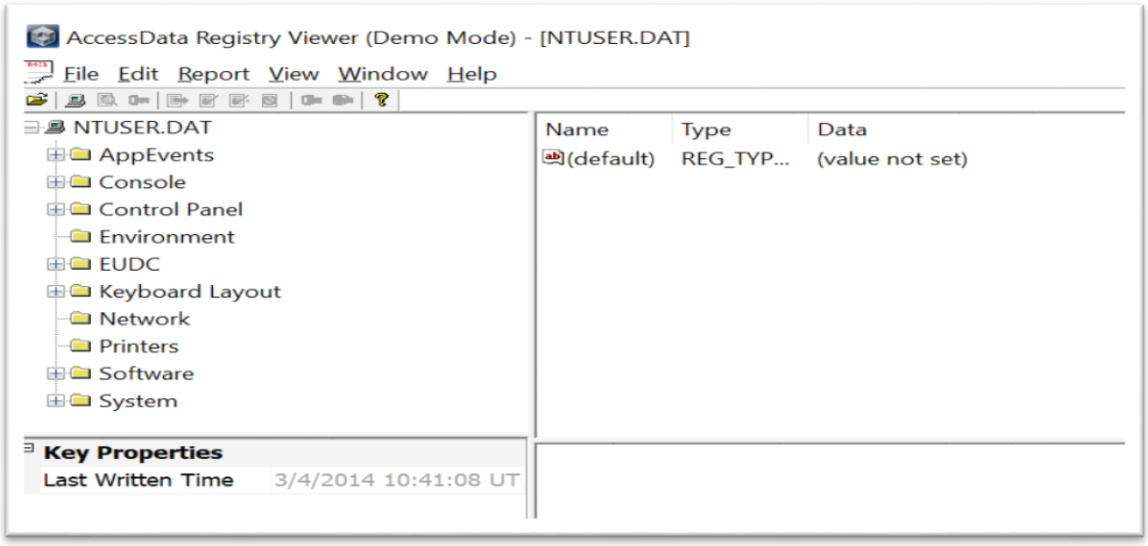
➢ There are 5 mounted devices was attached to the computer and out of which 2 devices on the system have an attached a drive letter

\DosDevices\C: , \DosDevices\D:

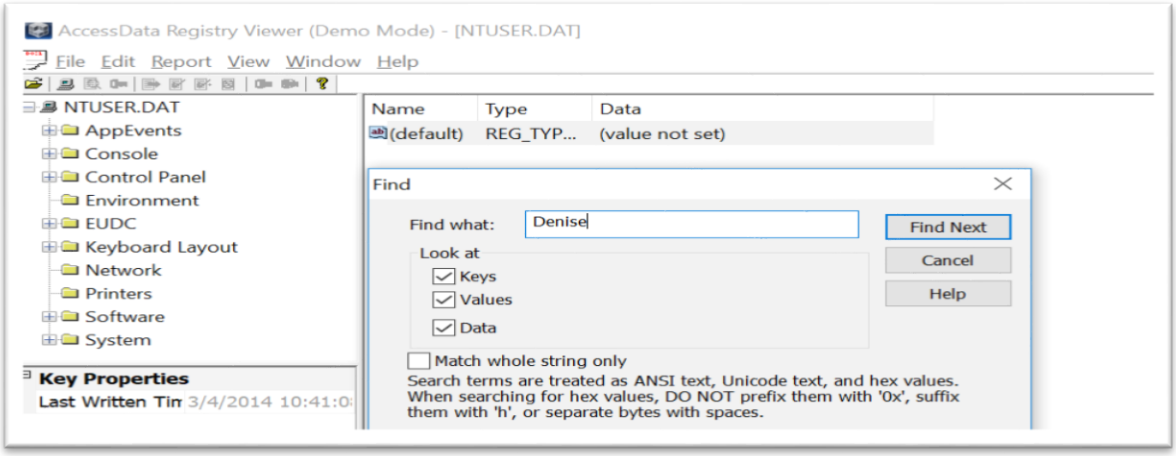


4. Examining the NTUSER.DAT File

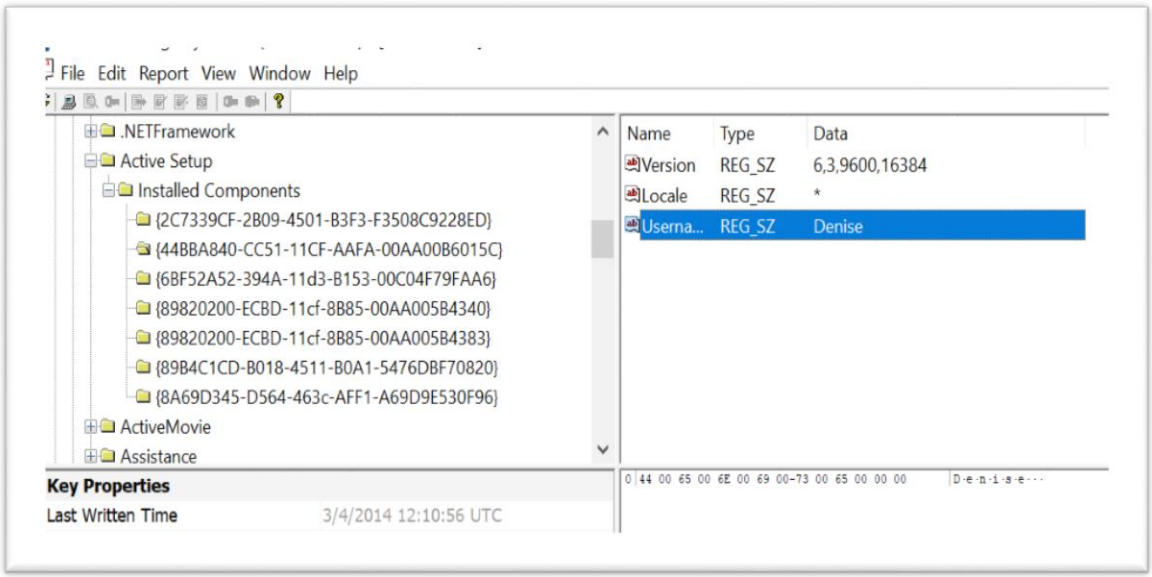
- NTUSER.DAT is a windows generated file and contains information about user account settings. Each user has their own NTUSER.DAT file in user's profile. [2]
- Open the NTUSER.DAT file from the extracted registry files for analysis



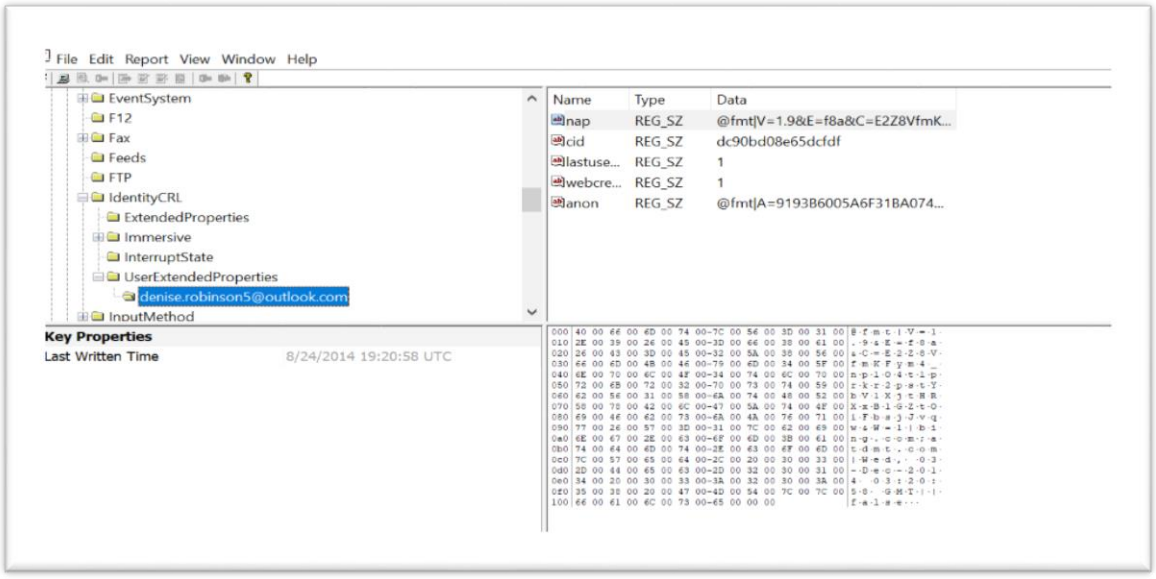
- Click Edit → Find and type Denise into the search bar, click Next and Iterate through the search (by pressing F3) to identify information related to the Denise user account:



1. GUID associated with the username



2. Email account information



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

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

➢ There is no information available for user jfriday after searching. Because while extracting NTUSER.DAT file, I have only extracted file from Denise user profile

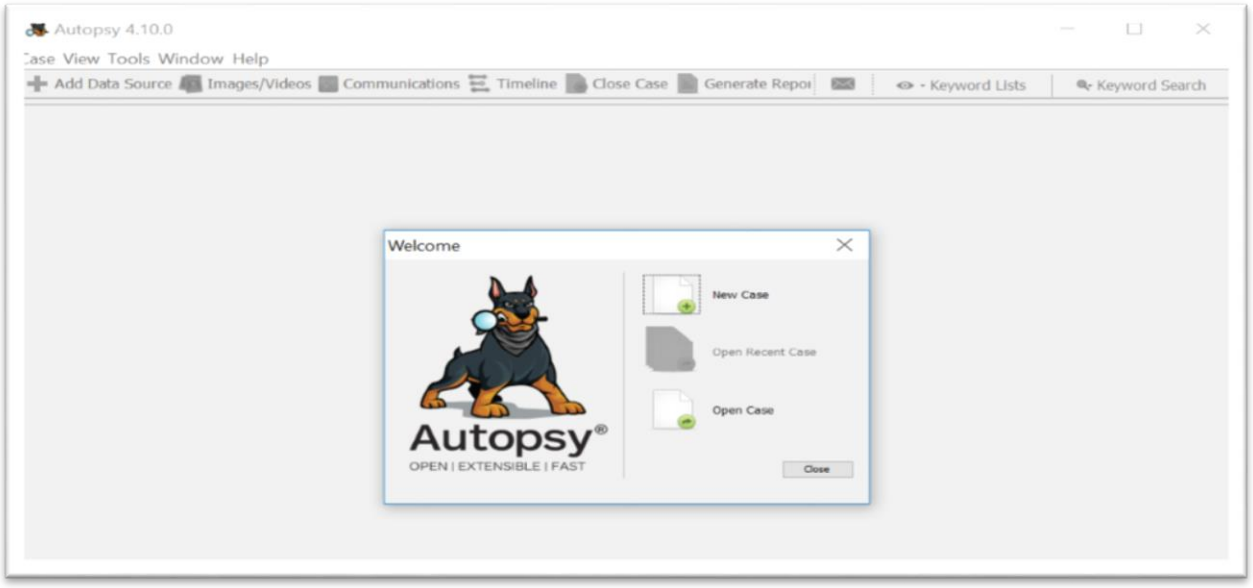
➢ NTUSER.DAT is a windows generated file and contains information about user account settings. Each user has their own NTUSER.DAT file in user’s profile.

Since I have only extracted NTUSER.DAT file from Denise profile, there is no details available for user jfriday. [2]

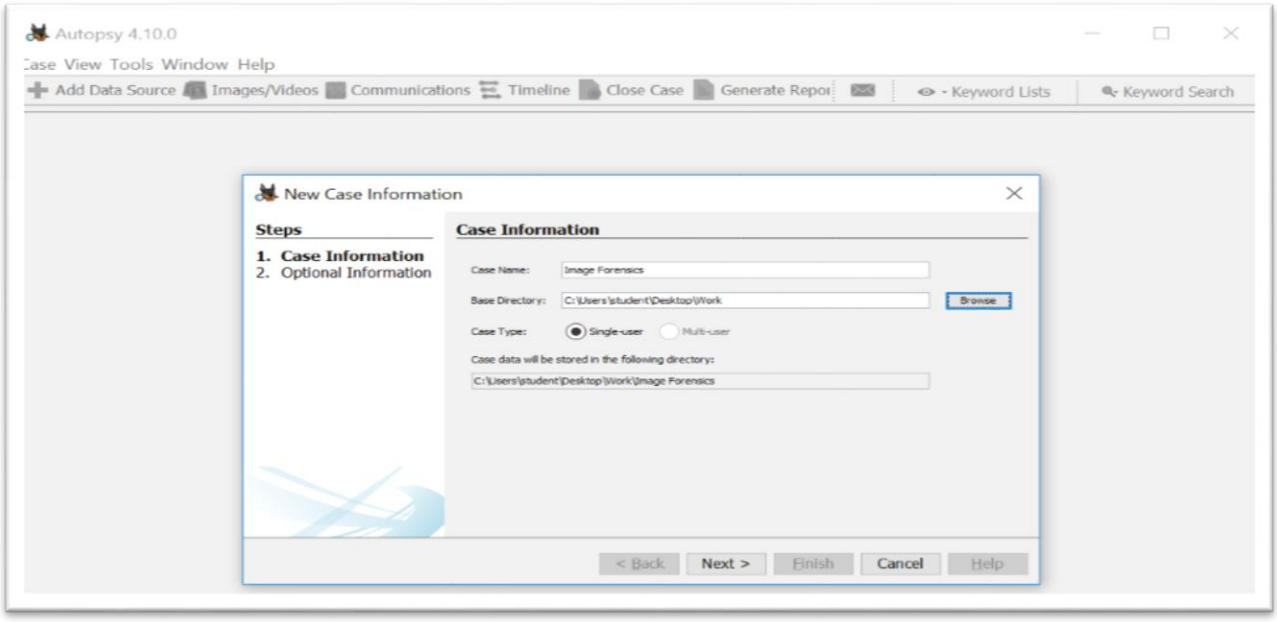
Image Forensics

1. Analysis of Image Files

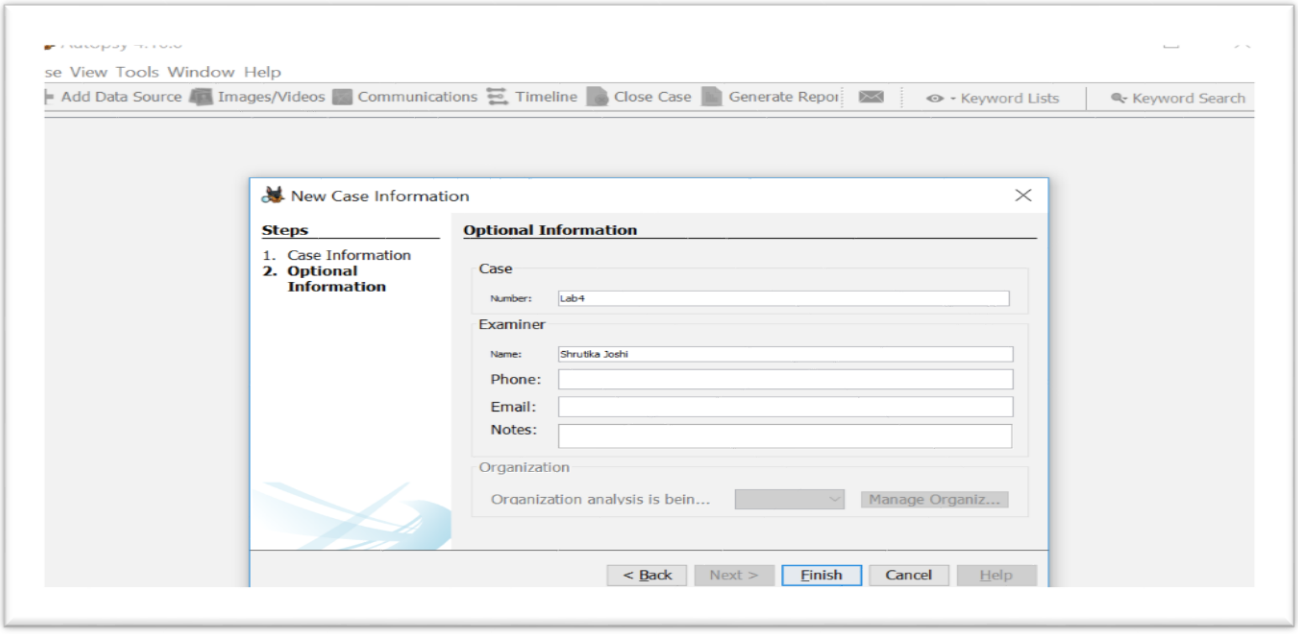
- Open Autopsy and create new case



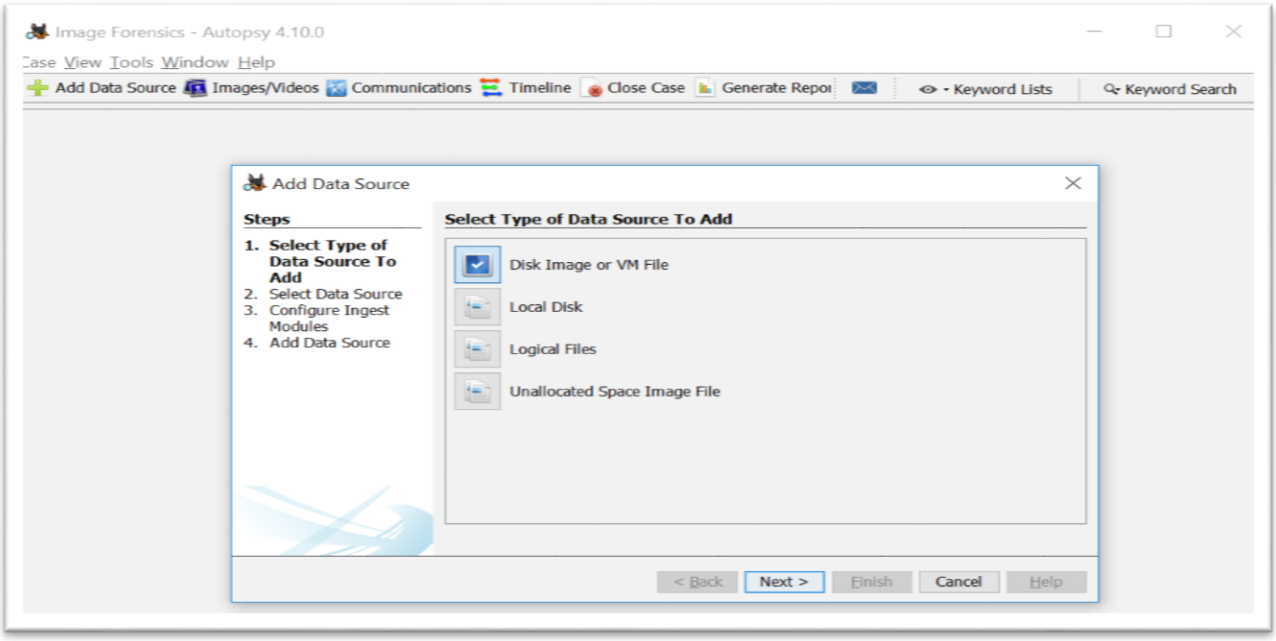
- Run through the new case wizard, add Case name and file destination location and click Next



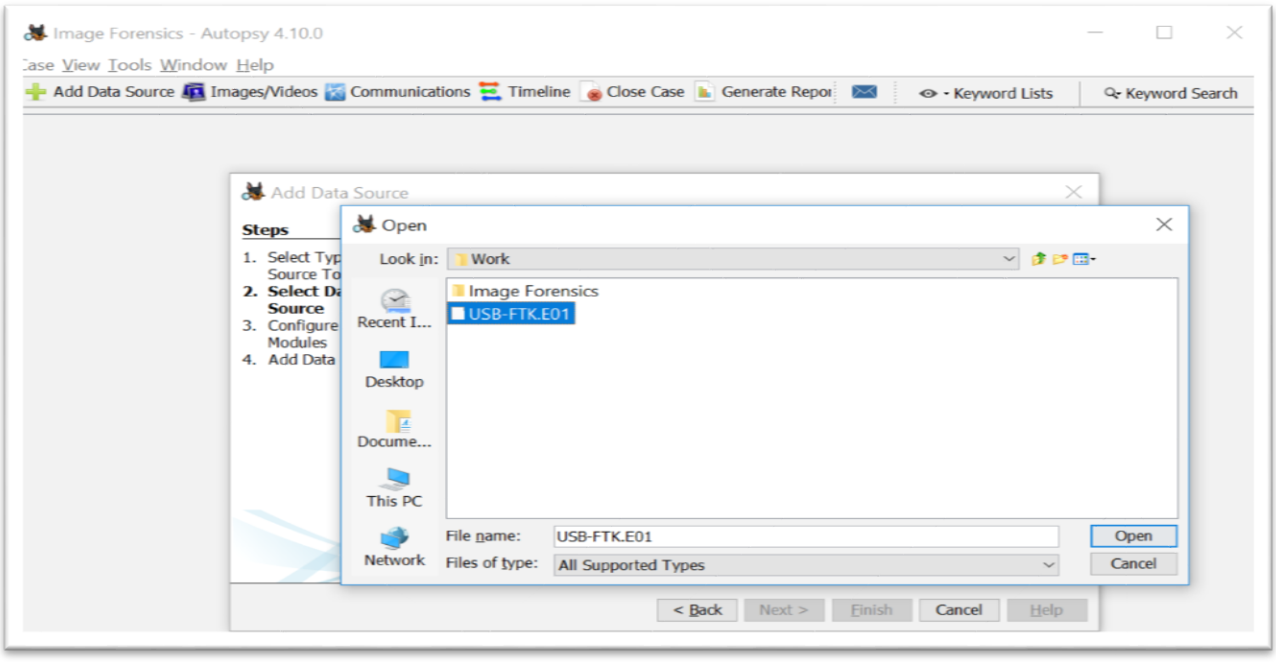
- Now add Case Number and Examiner name in the pop-up window and click Finish



- In the Add Data Source panel, click on Disk Image or VM File option and click Next.

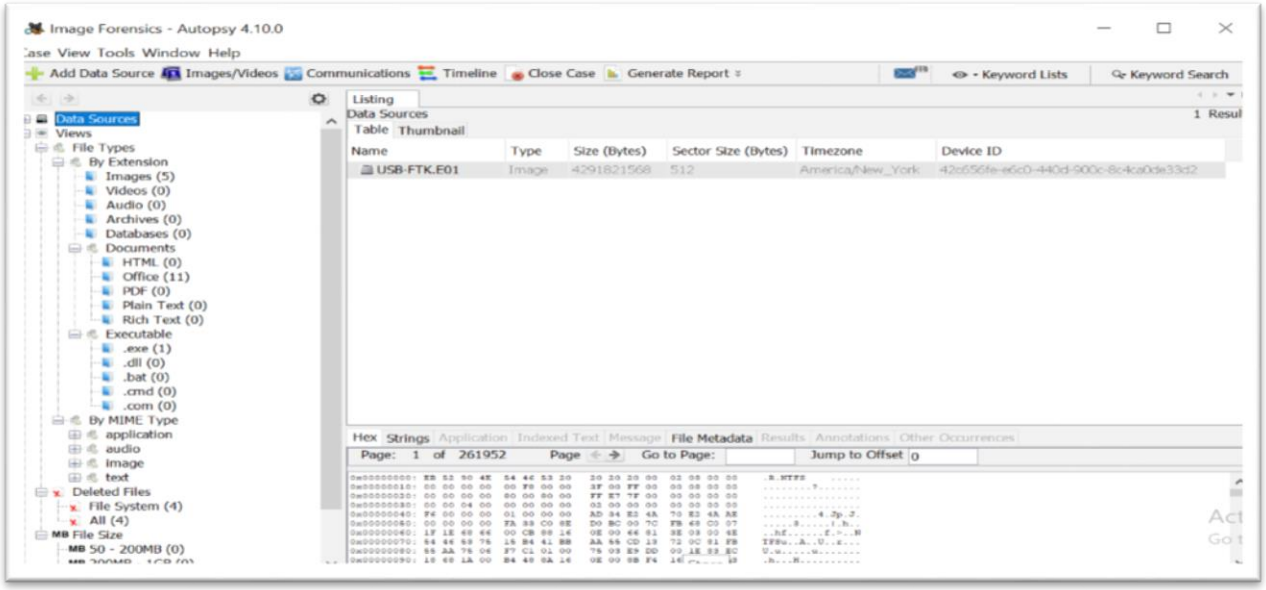


- Browse to one of the USB-FTK images you created in lab 2 (.E01 file format) and click Open.



- Let Autopsy parse through the image. When finished, expand the Views category and identify all images files. Perform an extraction of the images so you can manually review

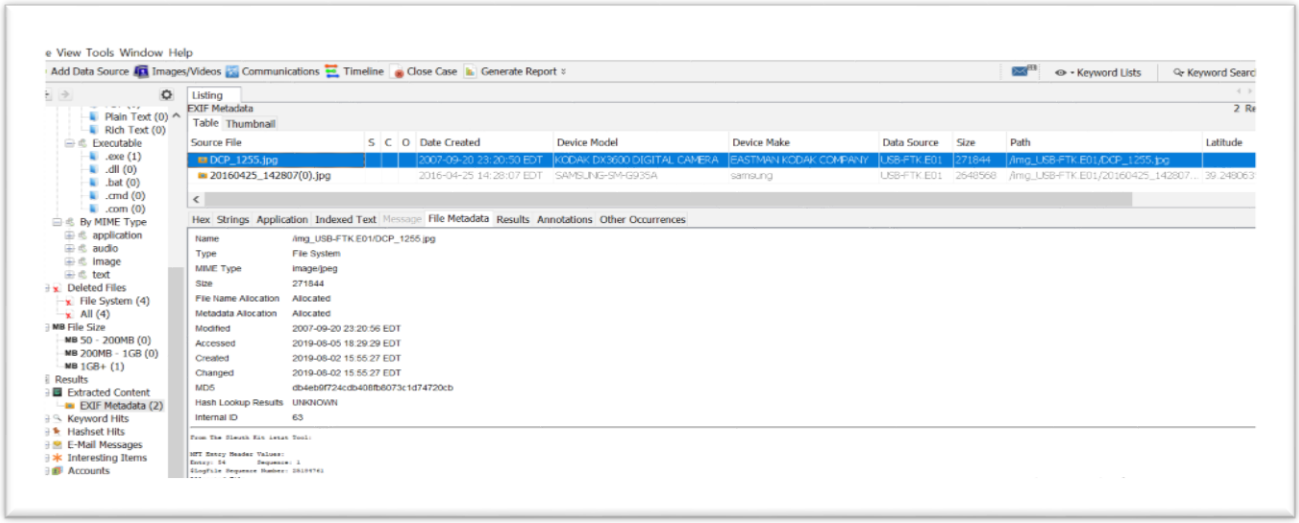
them. (Note you can also see "Deleted Files", which is also helpful to check in a full investigation)

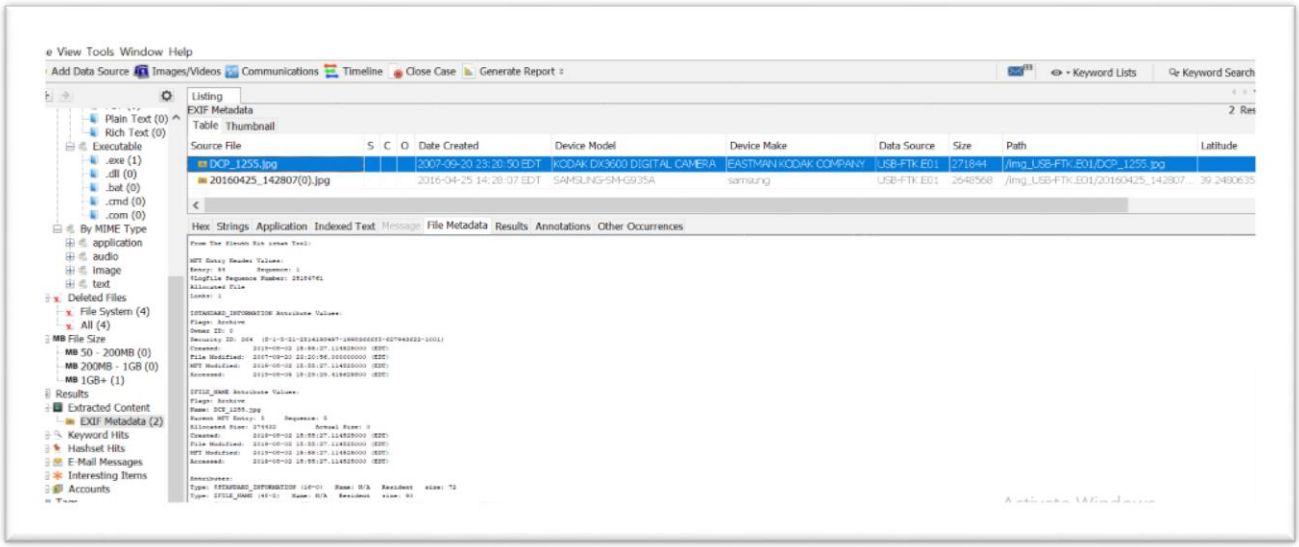


- Expand the Results category - Extracted Content to look at EXIF Metadata.

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

   - From the below image, I could see details EXIF metadata like Source File, Date Created, Device Model, Device Make, Data Source, Size, Path, Latitude, Longitude, and Altitude.
   - Also, from the File Metadata tab, I am able to view important details like File Modified, Access and Change Date, MD5 hash.


e View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Searc
Listing
EXIF Metadata
Table
Thumbnail
Source File
Date Created
Device Model
Device Make
Data Source
Size
Path
Latitude
DCP_1255.jpg
2007-09-20 23:20:50 EDT
KODAK DX3600 DIGITAL CAMERA
EASTMAN KODAK COMPANY
USB-FTK E01
271844
/img_USB-FTK E01/DCP_1255.jpg
20160425_142807(0).jpg
2016-04-25 14:28:07 EDT
SAMSUNG-SM-G935A
samsung
2648568
Hex
Strings
Application
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Name
/img_USB-FTK.E01/DCP_1255.jpg
Type
File System
MIME Type
image/jpeg
Size
271844
File Name Allocation
Allocated
Metadata Allocation
Allocated
Modified
2007-09-20 23:20:56 EDT
Accessed
2019-08-05 18:29:29 EDT
Created
2019-08-02 15:55:27 EDT
Changed
2019-08-02 15:55:27 EDT
MD5
db4eb9f724cdb408fb6073c1d74720cb
Hash Lookup Results
UNKNOWN
Internal ID
63
Plain Text (0)
Rich Text (0)
Executable
.exe (1)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
audio
image
text
Deleted Files
File System (4)
All (4)
File Size
50 - 200MB (0)
200MB - 1GB (0)
1GB+ (1)
Results
Extracted Content
EXIF Metadata (2)
Keyword Hits
Hashset Hits
E-Mail Messages
Interesting Items
Accounts


e View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Listing
EXIF Metadata
Table
Thumbnail
Source File
Date Created
Device Model
Device Make
Data Source
Size
Path
Latitude
DCP_1255.jpg
2007-09-20 23:20:50 EDT
KODAK DX3600 DIGITAL CAMERA
EASTMAN KODAK COMPANY
USB-FTK E01
271844
/img_USB-FTK.E01/DCP_1255.jpg
20160425_142807(0).jpg
2016-04-25 14:28:07 EDT
SAMSUNG-SM-G935A
samsung
2648568
Hex
Strings
Application
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Plain Text (0)
Rich Text (0)
Executable
.exe (1)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
audio
image
text
Deleted Files
File System (4)
All (4)
File Size
50 - 200MB (0)
200MB - 1GB (0)
1GB+ (1)
Results
Extracted Content
EXIF Metadata (2)
Keyword Hits
Hashset Hits
E-Mail Messages
Interesting Items
Accounts

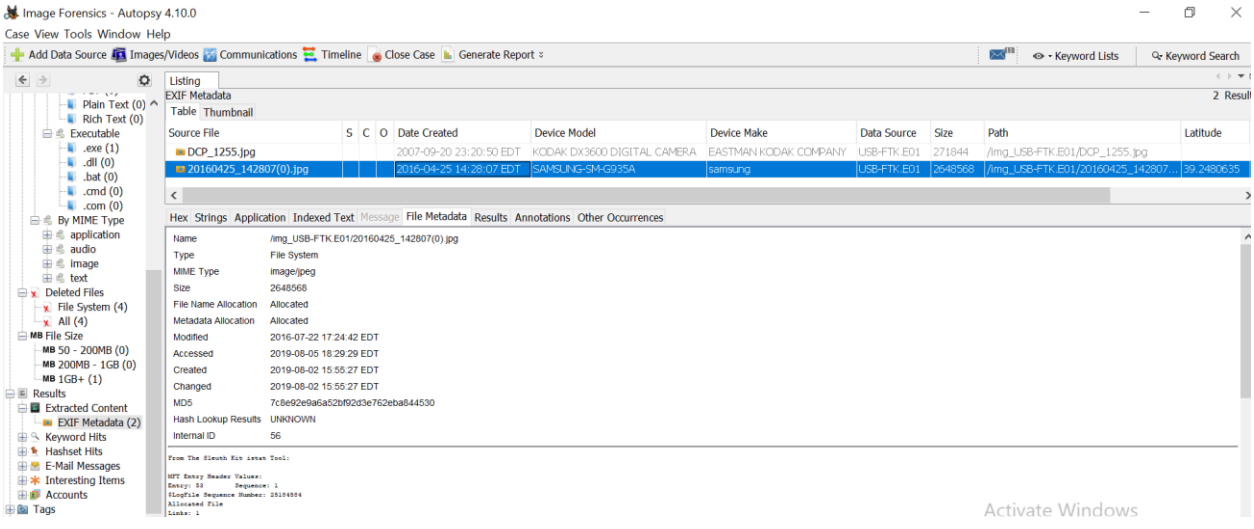
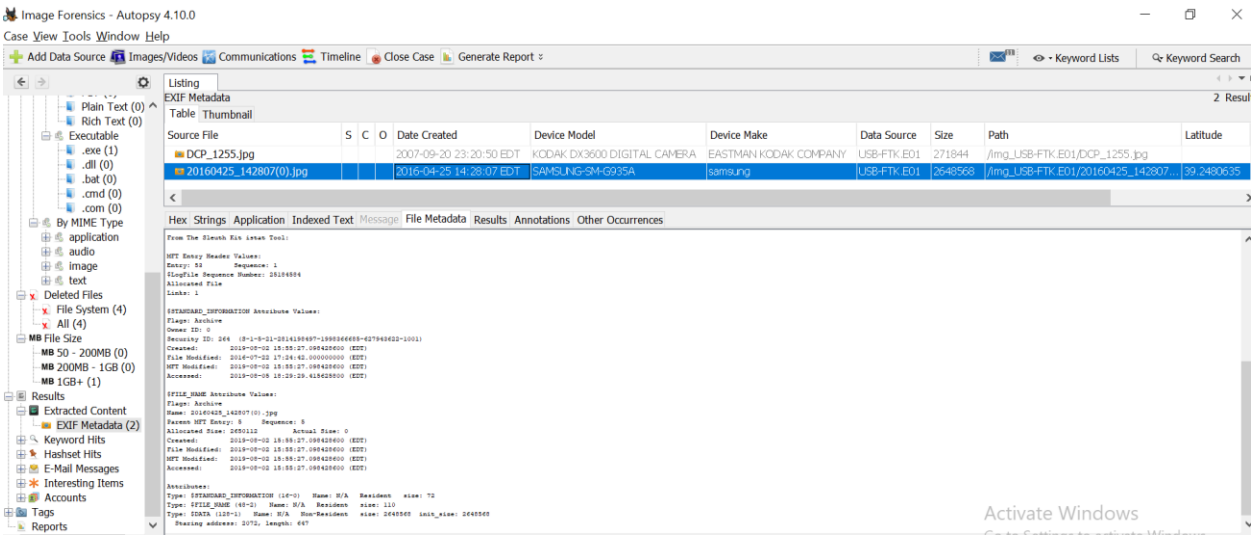
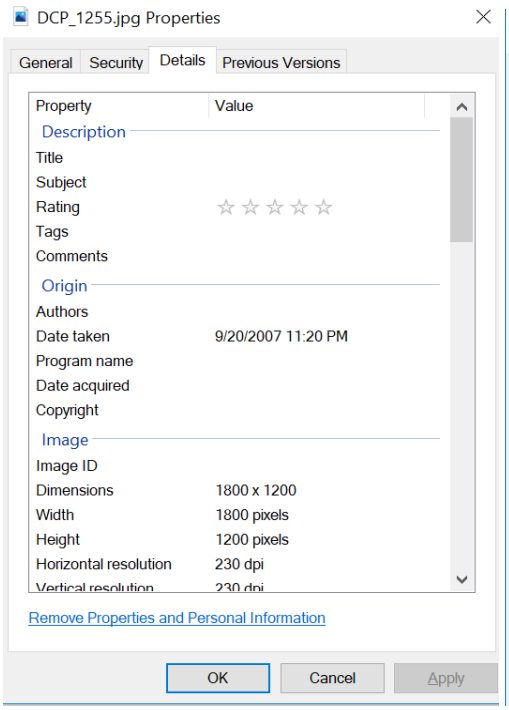


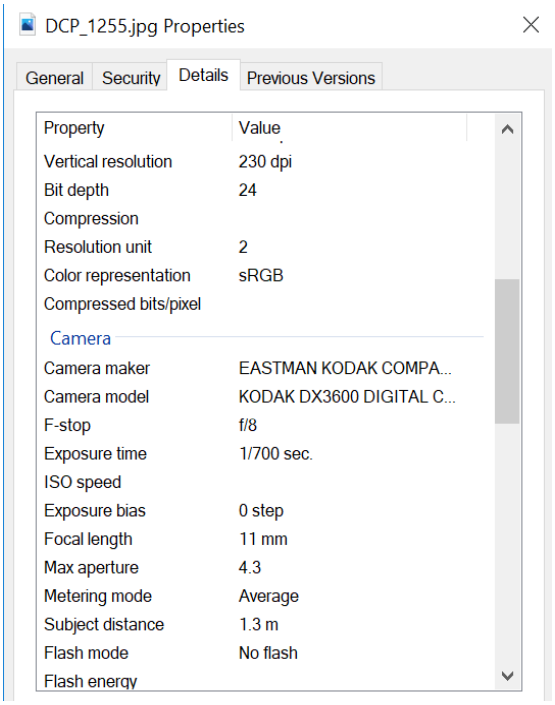
Image Forensics - Autopsy 4.10.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Listing
EXIF Metadata
Table
Thumbnail
Source File
Date Created
Device Model
Device Make
Data Source
Size
Path
Latitude
DCP_1255.jpg
2007-09-20 23:20:50 EDT
KODAK DX3600 DIGITAL CAMERA
EASTMAN KODAK COMPANY
USB-FTK E01
271844
/img_USB-FTK.E01/DCP_1255.jpg
20160425_142807(0).jpg
2016-04-25 14:28:07 EDT
SAMSUNG-SM-G935A
samsung
2648568
39.2480635
Hex
Strings
Application
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Name
/img_USB-FTK.E01/20160425_142807(0).jpg
Type
File System
MIME Type
image/jpeg
Size
2648568
File Name Allocation
Allocated
Metadata Allocation
Allocated
Modified
2016-07-22 17:24:42 EDT
Accessed
2019-08-05 18:29:29 EDT
Created
2019-08-02 15:55:27 EDT
Changed
2019-08-02 15:55:27 EDT
MD5
7c8e92e9a6a52bf92d3e762eba844530
Hash Lookup Results
UNKNOWN
Internal ID
56
Plain Text (0)
Rich Text (0)
Executable
.exe (1)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
audio
image
text
Deleted Files
File System (4)
All (4)
File Size
50 - 200MB (0)
200MB - 1GB (0)
1GB+ (1)
Results
Extracted Content
EXIF Metadata (2)
Keyword Hits
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Activate Windows

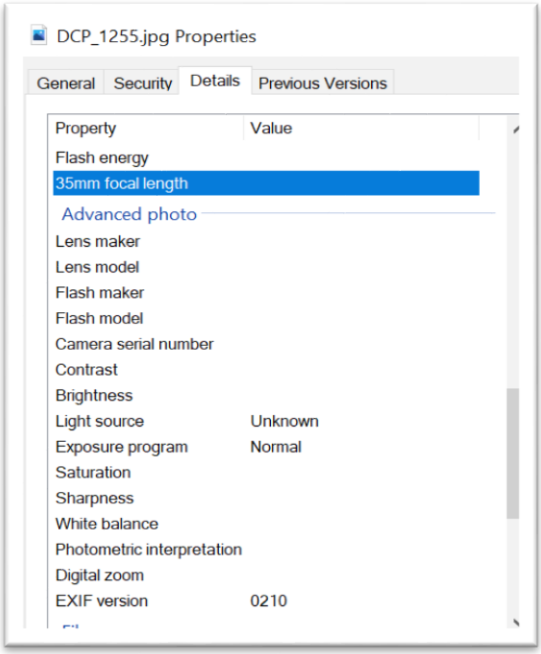


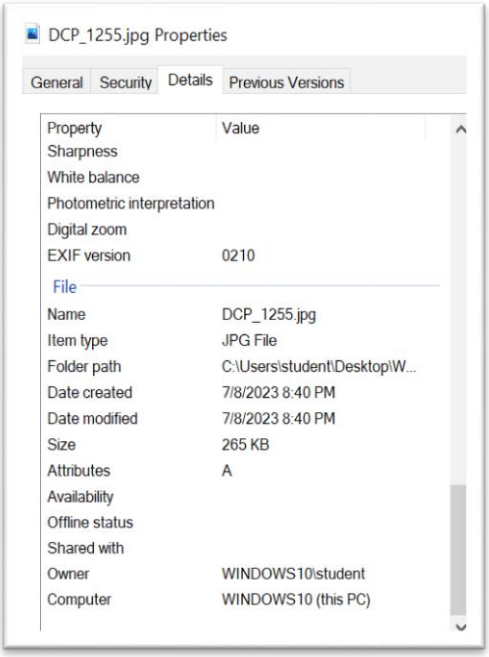
- To manually check the EXIF Metadata, browse to the folder you extracted the image files to previously and then Right Click-Properties on each file.

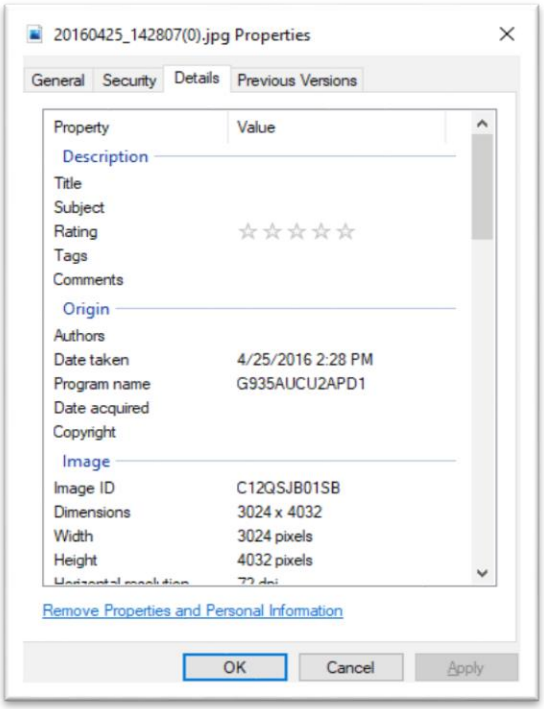
    1. Do you see any additional EXIF Metadata that wasn't present in Autopsy?
        - For both of the images, after manually checking properties I can view, image dimension details as well as more details about the camera properties set during image capture which wasn’t present in Autopsy file metadata details.

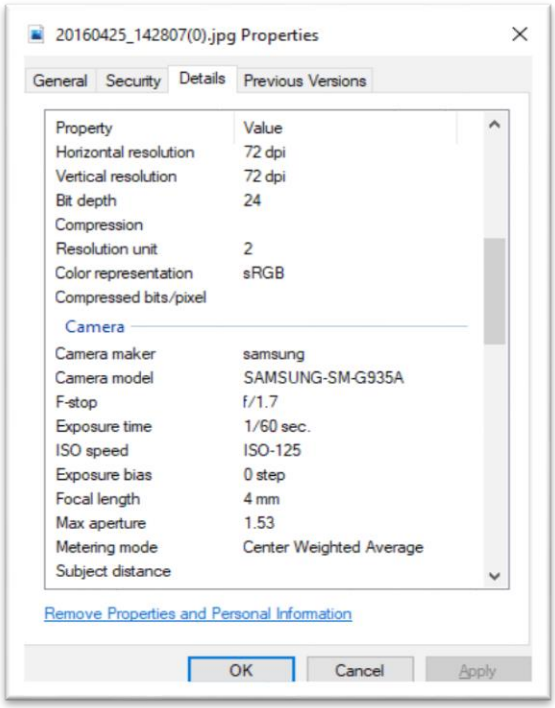

DCP_1255.jpg Properties
General
Security
Details
Previous Versions
Property
Value
Description
Title
Subject
Rating
Tags
Comments
Origin
Authors
Date taken
9/20/2007 11:20 PM
Program name
Date acquired
Copyright
Image
Image ID
Dimensions
1800 x 1200
Width
1800 pixels
Height
1200 pixels
Horizontal resolution
230 dpi
Remove Properties and Personal Information
OK
Cancel
Apply

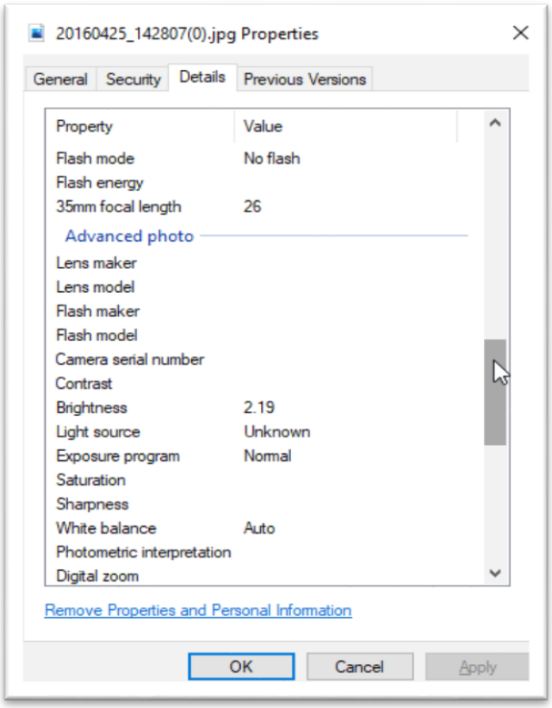

DCP_1255.jpg Properties
General
Security
Details
Previous Versions
Property
Value
Vertical resolution
230 dpi
Bit depth
24
Compression
Resolution unit
2
Color representation
sRGB
Compressed bits/pixel
Camera
Camera maker
EASTMAN KODAK COMPA...
Camera model
KODAK DX3600 DIGITAL C...
F-stop
f/8
Exposure 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

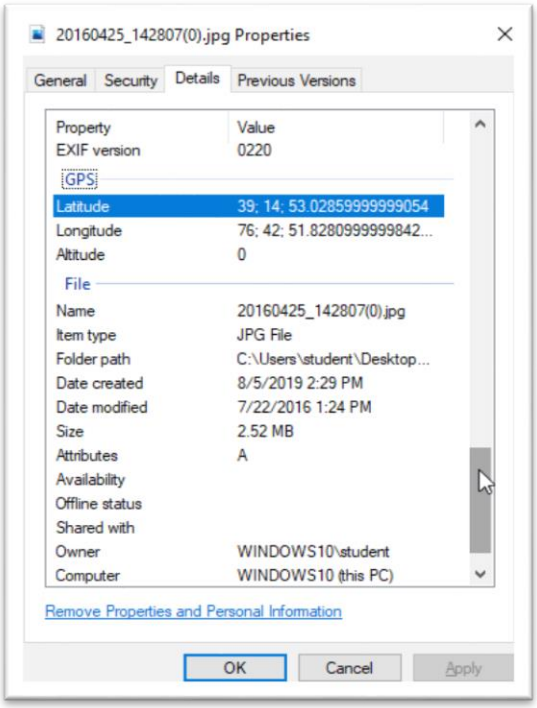

DCP_1255.jpg Properties
General
Security
Details
Previous Versions
Property
Value
Flash energy
35mm focal length
Advanced photo
Lens maker
Lens model
Flash maker
Flash model
Camera serial number
Contrast
Brightness
Light source
Unknown
Exposure program
Normal
Saturation
Sharpness
White balance
Photometric interpretation
Digital zoom
EXIF version
0210


DCP_1255.jpg Properties
General
Security
Details
Previous Versions
Property
Value
Sharpness
White balance
Photometric interpretation
Digital zoom
EXIF version
0210
File
Name
DCP_1255.jpg
Item type
JPG File
Folder path
C:\Users\student\Desktop\W...
Date created
7/8/2023 8:40 PM
Date modified
7/8/2023 8:40 PM
Size
265 KB
Attributes
A
Availability
Offline status
Shared with
Owner
WINDOWS10\student
Computer
WINDOWS10 (this PC)









- Try uploading the images to online resources like fotoforensics.com or imageforensic.org.

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

- I uploaded image onto fotoforensics.com and I could see MORE details shown in the snapshots like approximate Geo Location, MD5 , SHA1, SHA256 hash values and below are the details.

  https://fotoforensics.com/analysis.php?id=1815b008bcc78eeb6e5e2c39fe05b3f5ebc9797a.2648568

  Make : samsung

  Camera Model Name: SAMSUNG-SM-G935A

  Software: G935AUCU2APD1

  Device Type: Cell Phone

  Date/Time Original: 2016:04:25 14:28:07

  Image Unique ID: C12QSJB01SB

  GPS Latitude Ref: North

  GPS Longitude Ref: West

  GPS Altitude Ref: Unknown (1.7)

  GPS Time Stamp: 18:28:06

  GPS Date Stamp: 2016:04:25

  GPS Position 39 deg 14' 53.03" N, 76 deg 42' 51.83" W

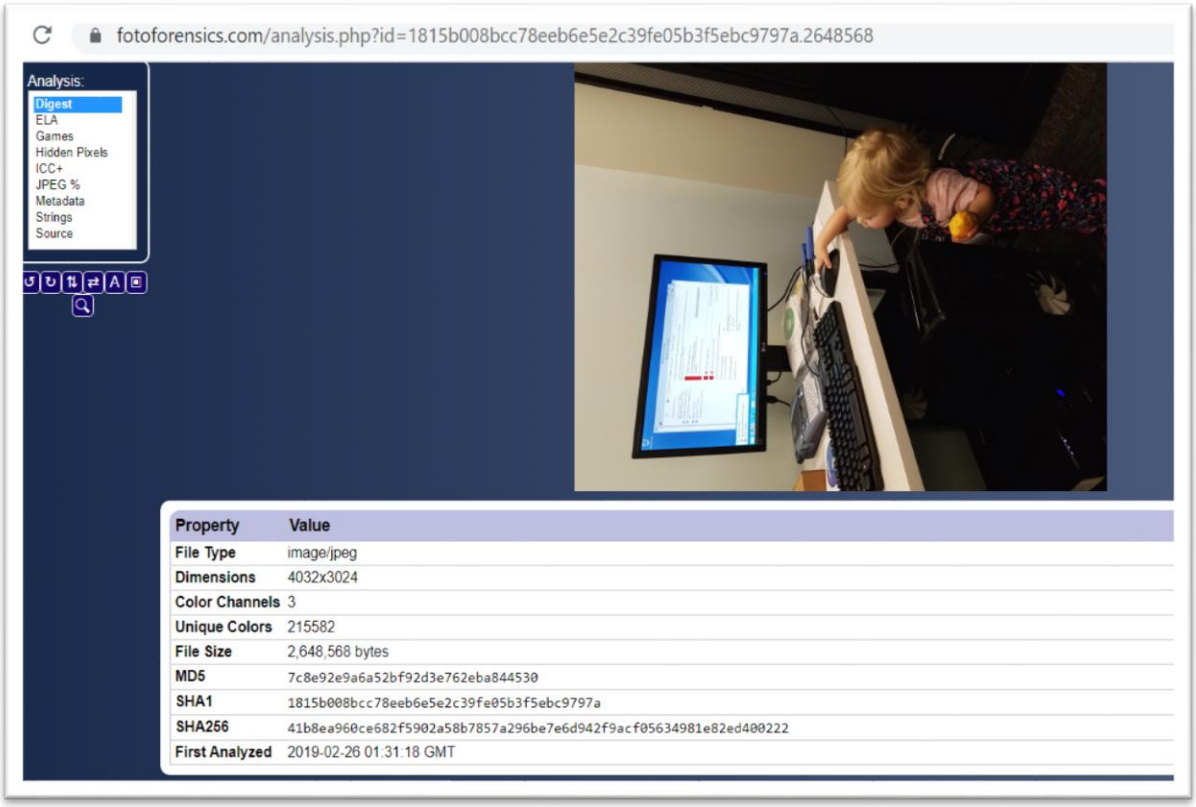
  Approximate Coordinates : 39.248064,-76.714397

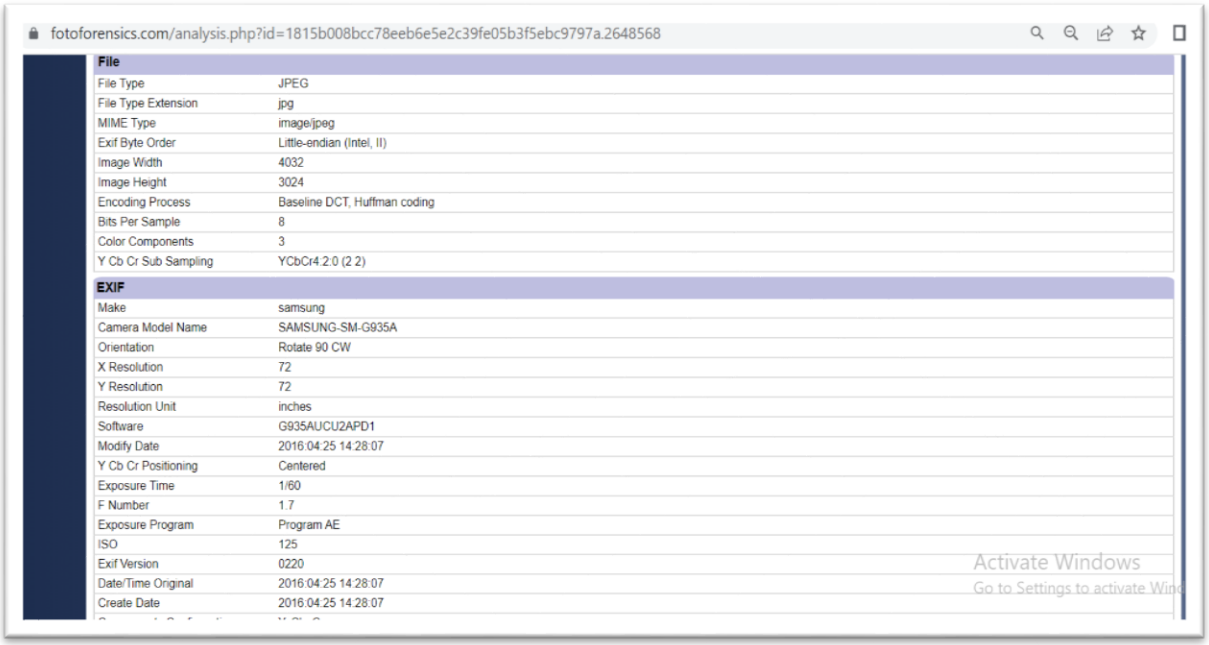
  Approximate Location: Arbutus, MD, US

  File Size: 2,648,568 bytes

  MD5: 7c8e92e9a6a52bf92d3e762eba844530

- However, exposure of such metadata is harmful as it exposes all user details including the machine name, user PII details as well as geo location and hackers can take advantage of such details to design attacks or crack sensitive information. Also, it violates user privacy.





fotoforensics.com/analysis.php?id=1815b008bcc78eeb6e5e2c39fe05b3f5ebc9797a.2648568

Shutter Speed Value	1/60
Aperture Value	1.7
Brightness Value	2.19
Exposure Compensation	0
Max Aperture Value	1.7
Metering Mode	Center-weighted average
Light Source	Unknown
Flash	No Flash
Focal Length	4.2 mm
User Comment	.
Flashpix Version	0100
Color Space	sRGB
Exif Image Width	4032
Exif Image Height	3024
Interoperability Index	R98 - DCF basic file (sRGB)
Interoperability Version	0100
Sensing Method	One-chip color area
Scene Type	Directly photographed
Exposure Mode	Auto
White Balance	Auto
Focal Length In 35mm Format	26 mm
Scene Capture Type	Standard
Image Unique ID	C12QSJB01SB
GPS Latitude Ref	North
GPS Longitude Ref	West
GPS Altitude Ref	Unknown (1.7)
GPS Time Stamp	18:28:06
GPS Date Stamp	2016:04:25
Compression	JPEG (old-style)

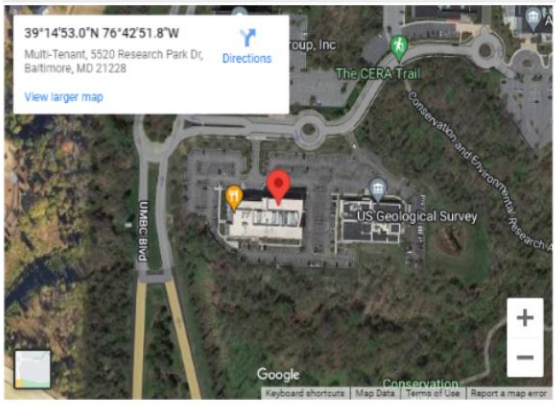
fotoforensics.com/analysis.php?id=1815b008bcc78eeb6e5e2c39fe05b3f5ebc9797a.2648568

GPS Date Stamp	2016:04:25
Compression	JPEG (old-style)
Thumbnail Offset	6150
Thumbnail Length	13480
Thumbnail Image	(Binary data 13480 bytes)
MakerNotes	
Maker Note Version	0100
Device Type	Cell Phone
Raw Data Byte Order	Little-endian (Intel, II)
Raw Data CFA Pattern	Swap
Face Detect	Off
Time Stamp	2016:04:25 18:28:07+00:00
Composite	
Aperture	1.7
Shutter Speed	1/60
GPS Altitude	0 m Above Sea Level
GPS Date/Time	2016:04:25 18:28:06Z
GPS Latitude	39 deg 14' 53.03" N
GPS Longitude	76 deg 42' 51.83" W
GPS Position	39 deg 14' 53.03" N, 76 deg 42' 51.83" W
Image Size	4032x3024
Light Value	7.1
Megapixels	12.2
Scale Factor To 35 mm Equivalent	6.2
Circle Of Confusion	0.005 mm
Field Of View	69.4 deg
Focal Length	4.2 mm (35 mm equivalent: 26.0 mm)
Hyperfocal Distance	2.14 m

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)



Glossary –

1. **MD5 hash – (**Message Digest Algorithm) it is a cryptographic function that takes input of any length and convert it into 128 bit hash values.
2. **GPS –** (Global Positioning System)It is navigating system using satellites, a receiver and algorithm to synchronize location, velocity and time data for air, sea and land level.
3. **Hive –** Logical group of keys, subkeys and values in registry
4. **EXIF Metadata – (**Exchangeable Image File Format) It holds information about the image itself.
5. **GUID –** (Globally unique Identifier) it is a 128 bit string that represents identification (ID)

Citations –

1. Khanse, A. (2022, October 20). Where are the Windows Registry files located in Windows 7? The Windows Club. Retrieved from https://www.thewindowsclub.com/where-are-the-windows-registry-files-located-in-windows-7
2. Hendrickson, J. (2019, January 18). What Is the NTUSER.DAT File? How-To Geek. Retrieved July 6, 2023, from https://www.howtogeek.com/401365/what-is-the-ntuser.dat-file/
3. TechTarget. (n.d.). Security Accounts Manager (SAM). SearchEnterpriseDesktop. Retrieved July 6, 2023, from https://www.techtarget.com/searchenterprisedesktop/definition/Security-Accounts-Manager by Katie Terrell Hanna
4. Hany Farid. (n.d.). FotoForensics. Retrieved July 6, 2023, from https://fotoforensics.com/

5. Heddings, L. (2019, April 30). Using Windows Admin Tools Like a Pro: Lesson 5 - Using Event Viewer to Troubleshoot Problems. How-To Geek. Retrieved from https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson5/