REGISTRY AND BROWSER FORENSICS ANALYSIS

Introduction

The window's registry is a database that stores a considerable amount of hardware and software configuration, network connections, user preferences and setup information in a Microsoft Windows Operating System. This information is maintained in a comparable manner to a log file. Registry information is important to a forensic investigator especially when trying to establish a timeline of activities in a system (Harlan, 2011).

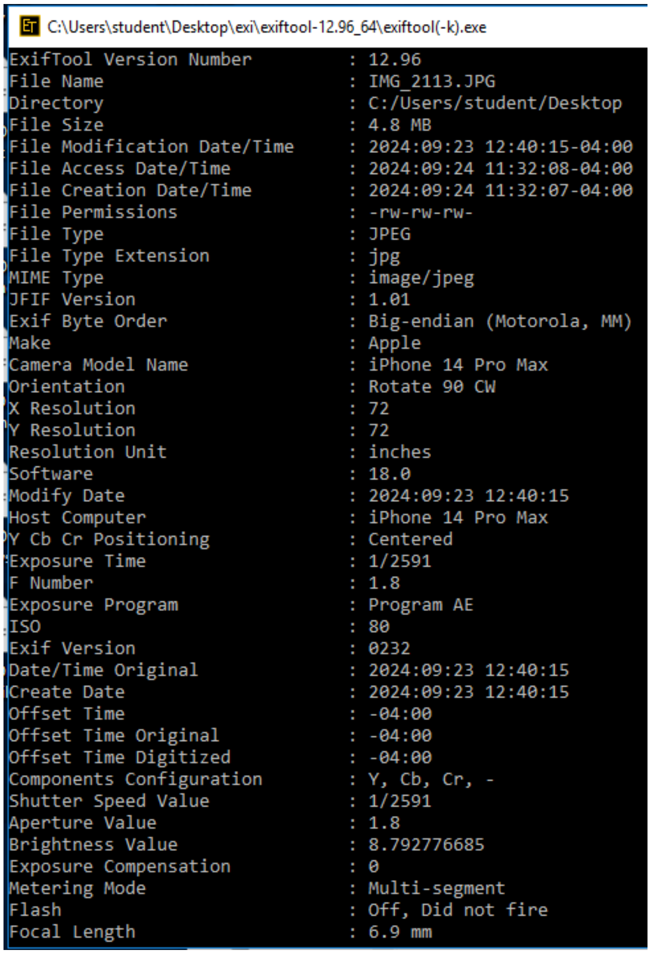
A browser is a software program that is used to present and explore content on the world wide web known as the internet. In our world today the web browser is a universally used tool as users utilize it to perform their daily tasks. These tasks include browsing, email access, downloading files et cetera. Being a useful tool, adversaries can equally misuse it to satisfy their sinister nature. This leaves tracks in the web browser's log files which can be acquired by a forensic examiner for reference as evidence in a case study. This evidence is in browsing history, bookmarks, cookies, and cache (Mayur & Dr. Bandu, 2018).

This lab we will be uploading picture files on the ExifTool by Phil Harvey which will return metadata that we will describe and explain depending on the properties in each file. We took two picture files, one with the GPS on and the other off to show the different details the tool returns. We will thereby compare the two picture file details and validate that indeed the tool used was accurate.

The figures below show a picture file with the GPS (Global positioning system) turned on which we will use to describe the metadata.

Figure 1/GPS on

The above figure shows the actual picture file that gives the details below.


C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe

```
ExifTool Version Number         : 12.96
File Name                       : IMG_2113.JPG
Directory                       : C:/Users/student/Desktop
File Size                       : 4.8 MB
File Modification Date/Time     : 2024:09:23 12:40:15-04:00
File Access Date/Time           : 2024:09:24 11:32:08-04:00
File Creation Date/Time         : 2024:09:24 11:32:07-04:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 14 Pro Max
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 18.0
Modify Date                     : 2024:09:23 12:40:15
Host Computer                   : iPhone 14 Pro Max
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/2591
F Number                        : 1.8
Exposure Program                : Program AE
ISO                             : 80
Exif Version                    : 0232
Date/Time Original              : 2024:09:23 12:40:15
Create Date                     : 2024:09:23 12:40:15
Offset Time                     : -04:00
Offset Time Original            : -04:00
Offset Time Digitized           : -04:00
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/2591
Aperture Value                  : 1.8
Brightness Value                : 8.792776685
Exposure Compensation           : 0
Metering Mode                   : Multi-segment
Flash                           : Off, Did not fire
Focal Length                    : 6.9 mm
```

Figure 2/GPS on one

The figure above shows the basic details of this picture file as follows:

File name – The name of the picture file

Directory – The directory that the image file was saved

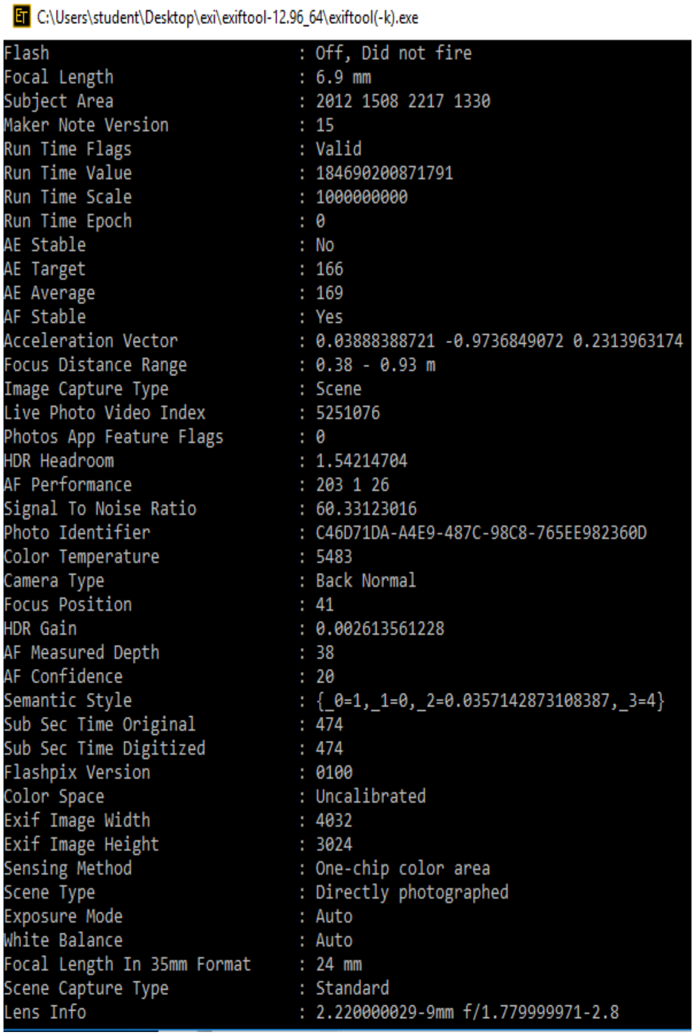
File size – The size in megabytes

File modification, access and creation Date/Time – This shows the specific date and time of the file when it was created, accessed and modified.

File Permissions – This indicated using the -rw attributes where r stands for read and w stands for write.

Type- Then there is the type of the file which determines the extension type to be used to save it.

Camera model, software version, host computer – this is vital information that shows the device used by name, hence showing the version.



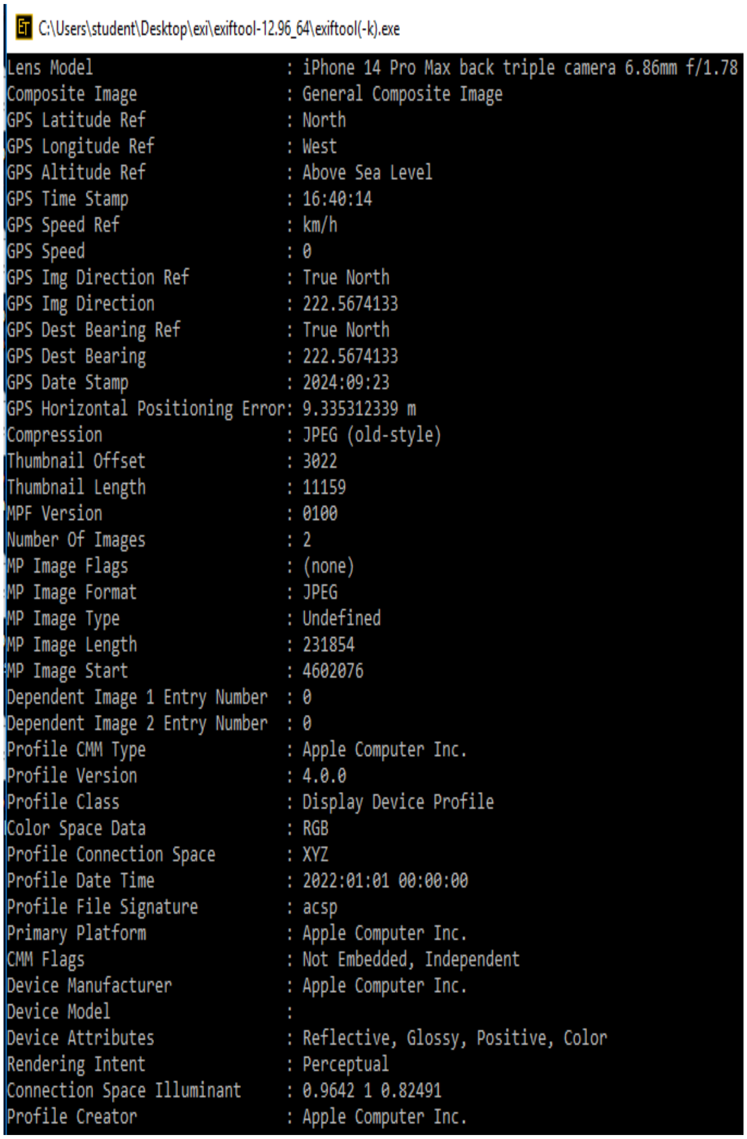
C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe

```
Flash                           : Off, Did not fire
Focal Length                    : 6.9 mm
Subject Area                    : 2012 1508 2217 1330
Maker Note Version              : 15
Run Time Flags                  : Valid
Run Time Value                  : 184690200871791
Run Time Scale                  : 1000000000
Run Time Epoch                  : 0
AE Stable                       : No
AE Target                       : 166
AE Average                      : 169
AF Stable                       : Yes
Acceleration Vector             : 0.03888388721 -0.9736849072 0.2313963174
Focus Distance Range            : 0.38 - 0.93 m
Image Capture Type              : Scene
Live Photo Video Index          : 5251076
Photos App Feature Flags        : 0
HDR Headroom                    : 1.54214704
AF Performance                  : 203 1 26
Signal To Noise Ratio           : 60.33123016
Photo Identifier                : C46D71DA-A4E9-487C-98C8-765EE982360D
Color Temperature               : 5483
Camera Type                     : Back Normal
Focus Position                  : 41
HDR Gain                        : 0.002613561228
AF Measured Depth               : 38
AF Confidence                   : 20
Semantic Style                  : {_0=1,_1=0,_2=0.0357142873108387,_3=4}
Sub Sec Time Original           : 474
Sub Sec Time Digitized          : 474
Flashpix Version                : 0100
Color Space                     : Uncalibrated
Exif Image Width                : 4032
Exif Image Height               : 3024
Sensing Method                  : One-chip color area
Scene Type                      : Directly photographed
Exposure Mode                   : Auto
White Balance                   : Auto
Focal Length In 35mm Format     : 24 mm
Scene Capture Type              : Standard
Lens Info                       : 2.220000029-9mm f/1.779999971-2.8
```

Figure 3/GPS on2.

Focus distance range – this shows the distance the camera was focused on during the capturing of the picture file.

Camera type -This shows the specific camera used to take this picture file.

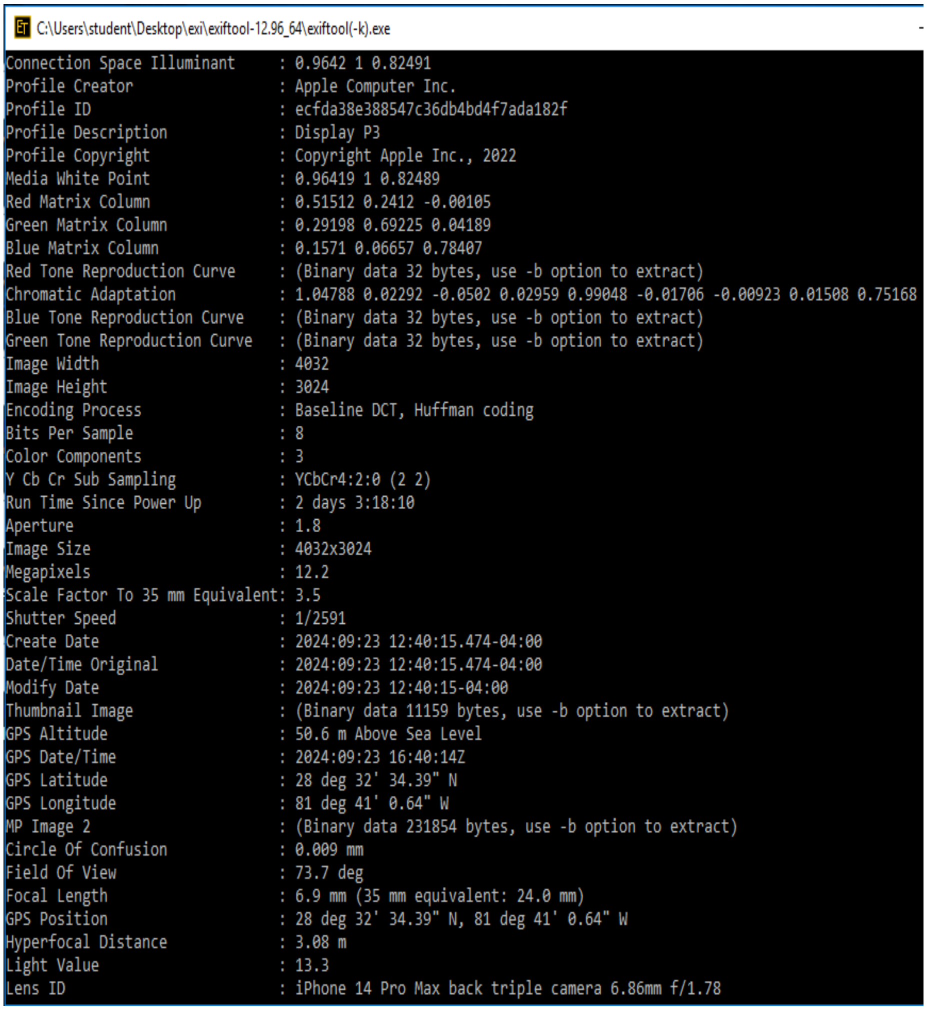


```
C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe
Lens Model                      : iPhone 14 Pro Max back triple camera 6.86mm f/1.78
Composite Image                 : General Composite Image
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 16:40:14
GPS Speed Ref                   : km/h
GPS Speed                       : 0
GPS Img Direction Ref           : True North
GPS Img Direction               : 222.5674133
GPS Dest Bearing Ref            : True North
GPS Dest Bearing                : 222.5674133
GPS Date Stamp                  : 2024:09:23
GPS Horizontal Positioning Error: 9.335312339 m
Compression                     : JPEG (old-style)
Thumbnail Offset                : 3022
Thumbnail Length                : 11159
MPF Version                     : 0100
Number Of Images                : 2
MP Image Flags                  : (none)
MP Image Format                 : JPEG
MP Image Type                   : Undefined
MP Image Length                 : 231854
MP Image Start                  : 4602076
Dependent Image 1 Entry Number  : 0
Dependent Image 2 Entry Number  : 0
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
```

Figure 4/GPS on3.

The figure above shows one of the vital metadata that were trying to assess as gives the GPS details that we will use to verify the specific location the picture file was taken.

More device details are listed to give a wide view of the device used.



C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe

```
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ecfda38e388547c36db4bd4f7ada182f
Profile Description             : Display P3
Profile Copyright               : Copyright Apple Inc., 2022
Media White Point               : 0.96419 1 0.82489
Red Matrix Column               : 0.51512 0.2412 -0.00105
Green Matrix Column             : 0.29198 0.69225 0.04189
Blue Matrix Column              : 0.1571 0.06657 0.78407
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation            : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Blue Tone Reproduction Curve    : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to extract)
Image Width                     : 4032
Image Height                    : 3024
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Run Time Since Power Up         : 2 days 3:18:10
Aperture                        : 1.8
Image Size                      : 4032x3024
Megapixels                      : 12.2
Scale Factor To 35 mm Equivalent: 3.5
Shutter Speed                   : 1/2591
Create Date                     : 2024:09:23 12:40:15.474-04:00
Date/Time Original              : 2024:09:23 12:40:15.474-04:00
Modify Date                     : 2024:09:23 12:40:15-04:00
Thumbnail Image                 : (Binary data 11159 bytes, use -b option to extract)
GPS Altitude                    : 50.6 m Above Sea Level
GPS Date/Time                   : 2024:09:23 16:40:14Z
GPS Latitude                    : 28 deg 32' 34.39" N
GPS Longitude                   : 81 deg 41' 0.64" W
MP Image 2                      : (Binary data 231854 bytes, use -b option to extract)
Circle Of Confusion             : 0.009 mm
Field Of View                   : 73.7 deg
Focal Length                    : 6.9 mm (35 mm equivalent: 24.0 mm)
GPS Position                    : 28 deg 32' 34.39" N, 81 deg 41' 0.64" W
Hyperfocal Distance             : 3.08 m
Light Value                     : 13.3
Lens ID                         : iPhone 14 Pro Max back triple camera 6.86mm f/1.78
```

Figure 5/GPS on4.

The above figure shows more details of the GPS with the specification of the altitude, date/time, latitude and longitude.

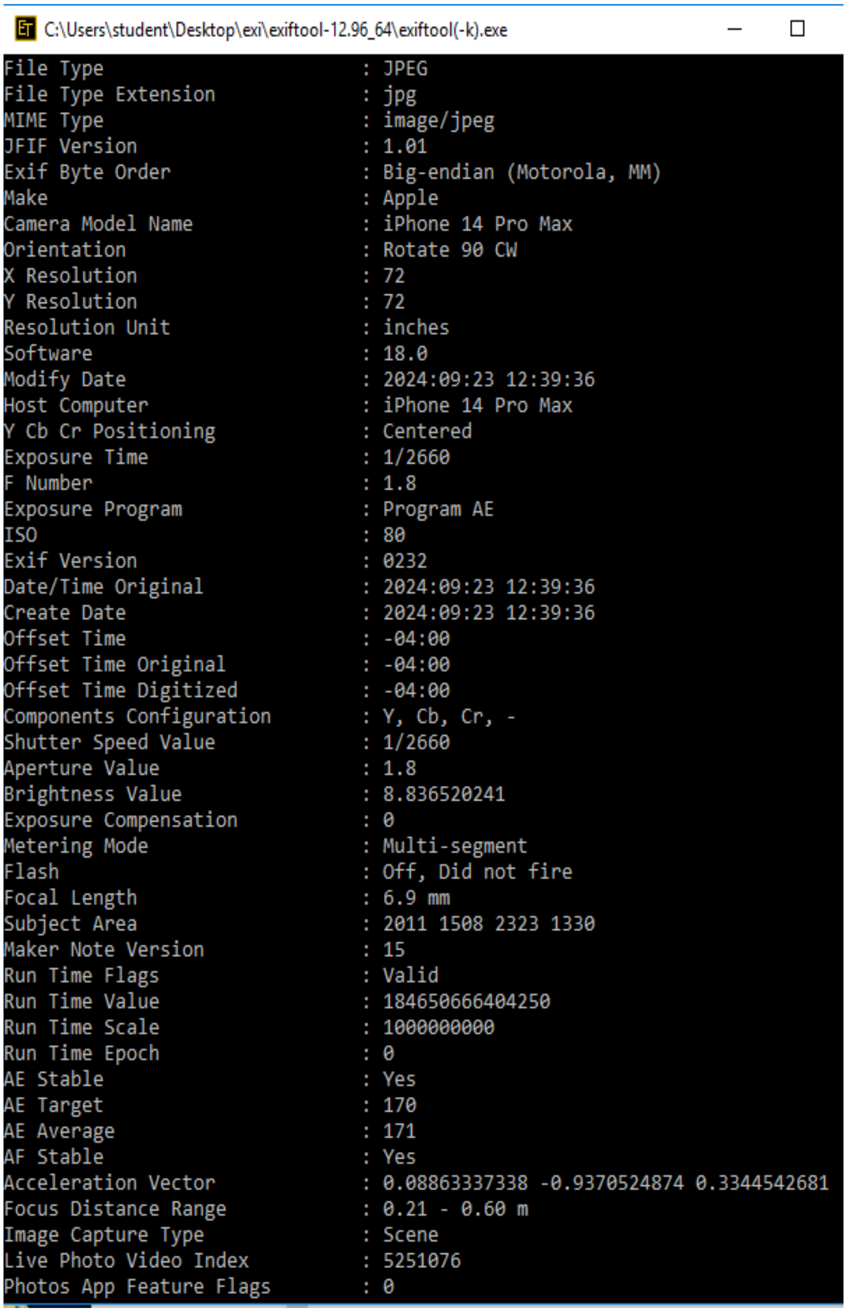
The original date and time – showing the original date and time of when the picture file was created.

The picture file megapixels and size of its width and length.

There is also details of the camera settings used to capture the picture file e.g. Aperture, shutter speed etc.

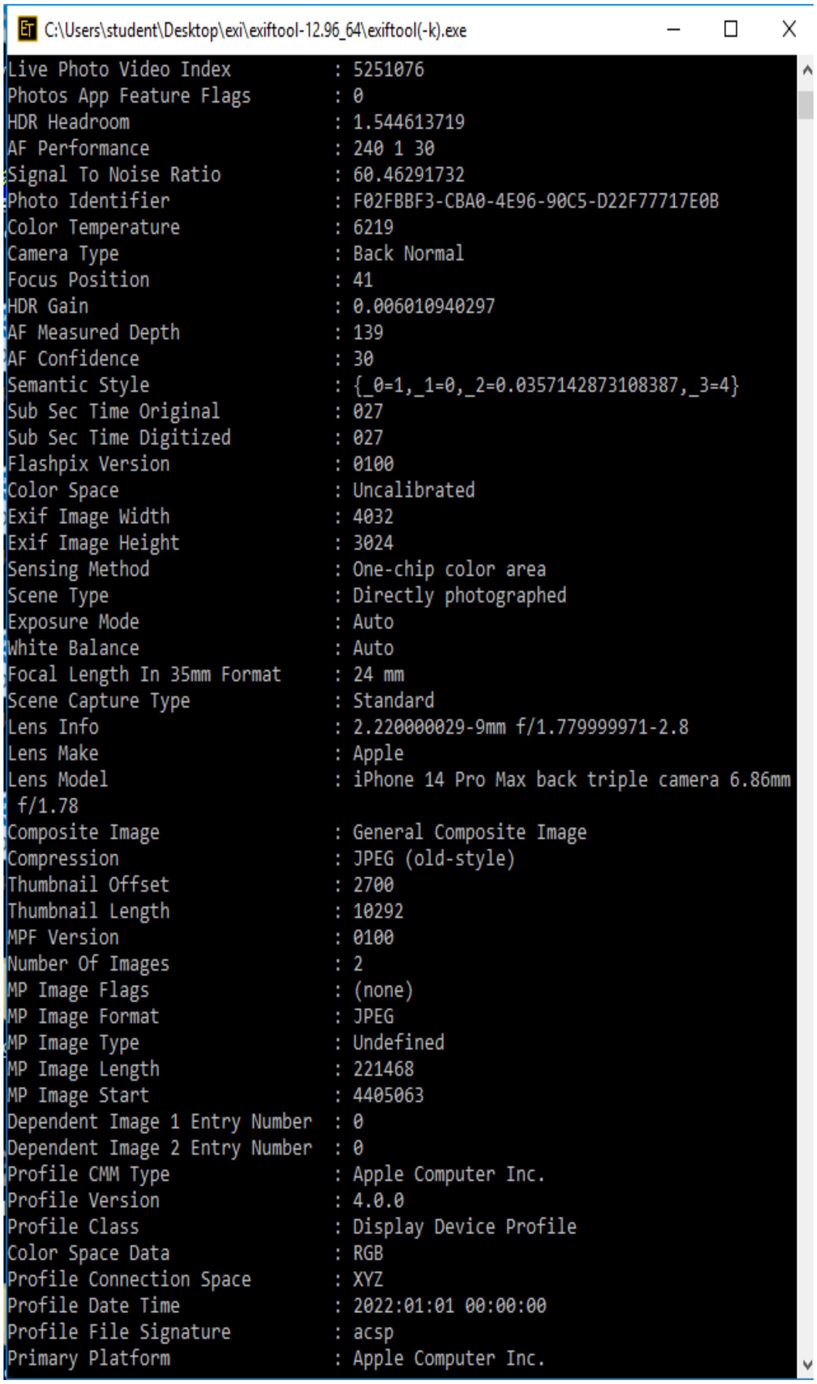
Figure 6/NO GPS

The above picture file shows our second test with the GPS option turned off. The other screenshots below show the same details as the prior ones but without showing any GPS information.


C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe

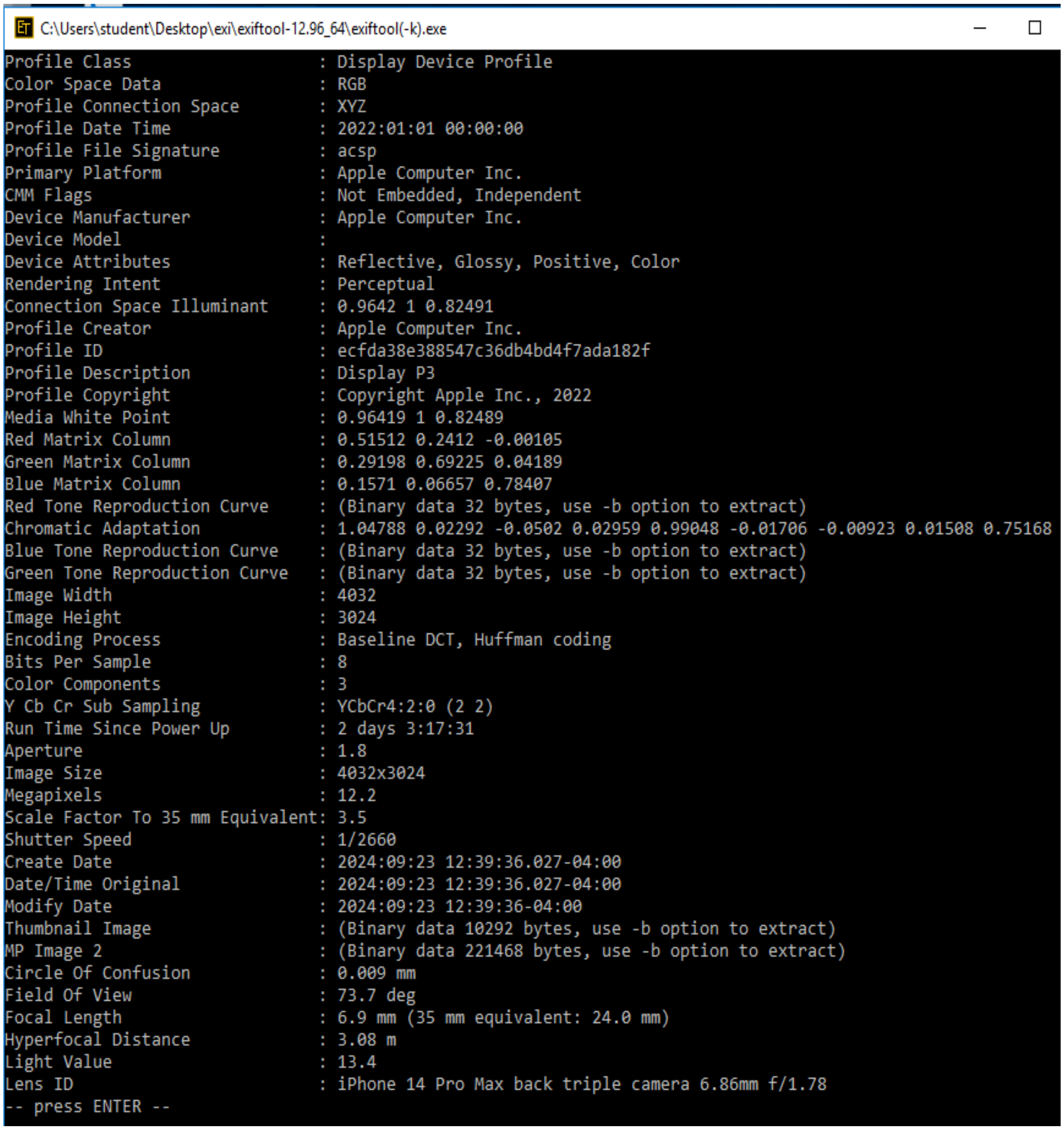
```
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 14 Pro Max
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 18.0
Modify Date                     : 2024:09:23 12:39:36
Host Computer                   : iPhone 14 Pro Max
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/2660
F Number                        : 1.8
Exposure Program                : Program AE
ISO                             : 80
Exif Version                    : 0232
Date/Time Original              : 2024:09:23 12:39:36
Create Date                     : 2024:09:23 12:39:36
Offset Time                     : -04:00
Offset Time Original            : -04:00
Offset Time Digitized           : -04:00
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/2660
Aperture Value                  : 1.8
Brightness Value                : 8.836520241
Exposure Compensation           : 0
Metering Mode                   : Multi-segment
Flash                           : Off, Did not fire
Focal Length                    : 6.9 mm
Subject Area                    : 2011 1508 2323 1330
Maker Note Version              : 15
Run Time Flags                  : Valid
Run Time Value                  : 184650666404250
Run Time Scale                  : 1000000000
Run Time Epoch                  : 0
AE Stable                       : Yes
AE Target                       : 170
AE Average                      : 171
AF Stable                       : Yes
Acceleration Vector             : 0.08863337338 -0.9370524874 0.3344542681
Focus Distance Range            : 0.21 - 0.60 m
Image Capture Type              : Scene
Live Photo Video Index          : 5251076
Photos App Feature Flags        : 0
```

Figure 7/GPS off1.


C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe

```
Live Photo Video Index          : 5251076
Photos App Feature Flags        : 0
HDR Headroom                    : 1.544613719
AF Performance                  : 240 1 30
Signal To Noise Ratio           : 60.46291732
Photo Identifier                : F02FBBF3-CBA0-4E96-90C5-D22F77717E0B
Color Temperature               : 6219
Camera Type                     : Back Normal
Focus Position                  : 41
HDR Gain                        : 0.006010940297
AF Measured Depth               : 139
AF Confidence                   : 30
Semantic Style                  : {_0=1,_1=0,_2=0.0357142873108387,_3=4}
Sub Sec Time Original           : 027
Sub Sec Time Digitized          : 027
Flashpix Version                : 0100
Color Space                     : Uncalibrated
Exif Image Width                : 4032
Exif Image Height               : 3024
Sensing Method                  : One-chip color area
Scene Type                      : Directly photographed
Exposure Mode                   : Auto
White Balance                   : Auto
Focal Length In 35mm Format     : 24 mm
Scene Capture Type              : Standard
Lens Info                       : 2.220000029-9mm f/1.779999971-2.8
Lens Make                       : Apple
Lens Model                      : iPhone 14 Pro Max back triple camera 6.86mm
 f/1.78
Composite Image                 : General Composite Image
Compression                     : JPEG (old-style)
Thumbnail Offset                : 2700
Thumbnail Length                : 10292
MPF Version                     : 0100
Number Of Images                : 2
MP Image Flags                  : (none)
MP Image Format                 : JPEG
MP Image Type                   : Undefined
MP Image Length                 : 221468
MP Image Start                  : 4405063
Dependent Image 1 Entry Number  : 0
Dependent Image 2 Entry Number  : 0
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
```

Figure 8/GPS off2.

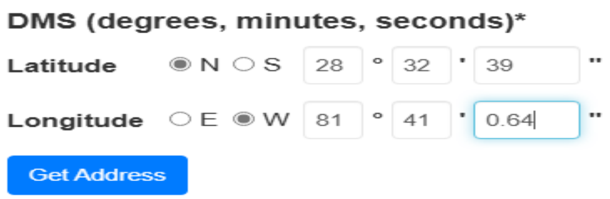


C:\Users\student\Desktop\exi\exiftool-12.96_64\exiftool(-k).exe

```
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ecfda38e388547c36db4bd4f7ada182f
Profile Description             : Display P3
Profile Copyright               : Copyright Apple Inc., 2022
Media White Point               : 0.96419 1 0.82489
Red Matrix Column               : 0.51512 0.2412 -0.00105
Green Matrix Column             : 0.29198 0.69225 0.04189
Blue Matrix Column              : 0.1571 0.06657 0.78407
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation            : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Blue Tone Reproduction Curve    : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to extract)
Image Width                     : 4032
Image Height                    : 3024
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Run Time Since Power Up         : 2 days 3:17:31
Aperture                        : 1.8
Image Size                      : 4032x3024
Megapixels                      : 12.2
Scale Factor To 35 mm Equivalent: 3.5
Shutter Speed                   : 1/2660
Create Date                     : 2024:09:23 12:39:36.027-04:00
Date/Time Original              : 2024:09:23 12:39:36.027-04:00
Modify Date                     : 2024:09:23 12:39:36-04:00
Thumbnail Image                 : (Binary data 10292 bytes, use -b option to extract)
MP Image 2                      : (Binary data 221468 bytes, use -b option to extract)
Circle Of Confusion             : 0.009 mm
Field Of View                   : 73.7 deg
Focal Length                    : 6.9 mm (35 mm equivalent: 24.0 mm)
Hyperfocal Distance             : 3.08 m
Light Value                     : 13.4
Lens ID                         : iPhone 14 Pro Max back triple camera 6.86mm f/1.78
-- press ENTER --
```

Figure 9/GPS off3.

Since the aim of our lab was to verify indeed the GPS information returned by the ExifTool we had to verify using the latitude and longitude dimensions shown in the figures below.

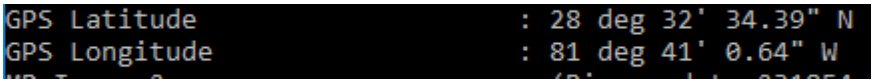


DMS (degrees, minutes, seconds)*

Latitude ● N ○ S 28 ° 32 ' 39 "

Longitude ○ E ● W 81 ° 41 ' 0.64 "

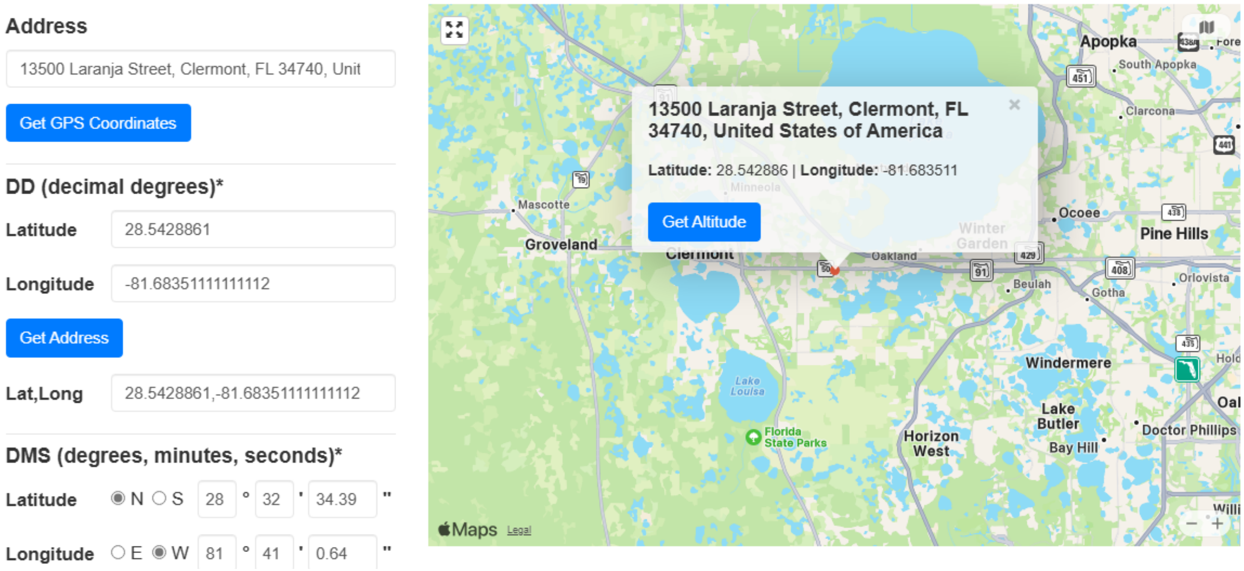
Figure 10/Dimensions.



```
GPS Latitude                    : 28 deg 32' 34.39" N
GPS Longitude                   : 81 deg 41' 0.64" W
```

Figure 11/Metadata.

The dimensions above were utilized to validate that the tool used was accurate as we populated them on a website *https://www.gps-coordinates.net/* which returned the location details below.



Address

13500 Laranja Street, Clermont, FL 34740, Unit

Get GPS Coordinates

DD (decimal degrees)*

Latitude 28.5428861

Longitude -81.68351111111112

Get Address

Lat,Long 28.5428861,-81.68351111111112

DMS (degrees, minutes, seconds)*

Latitude ● N ○ S 28 ° 32 ' 34.39 "

Longitude ○ E ● W 81 ° 41 ' 0.64 "

13500 Laranja Street, Clermont, FL 34740, United States of America

Latitude: 28.542886 | **Longitude:** -81.683511

Get Altitude

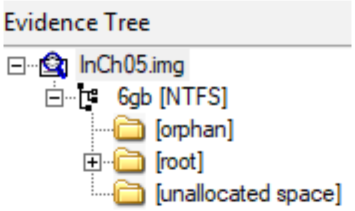
Figure 12/Validation

I hereby validate that the ExifTool was accurate and that it can be relied upon when undertaking an investigation.

Background

Extracting Registry

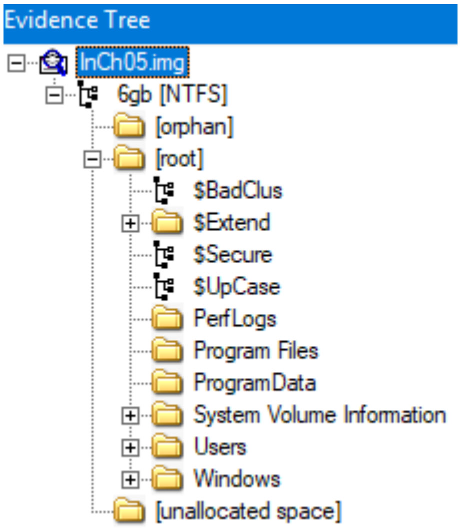
We use FTK Imager to extract our image which shows the folders in the figures below.



```
Evidence Tree
InCh05.img
  6gb [NTFS]
    [orphan]
    [root]
    [unallocated space]
```

Figure 13/InCh05.

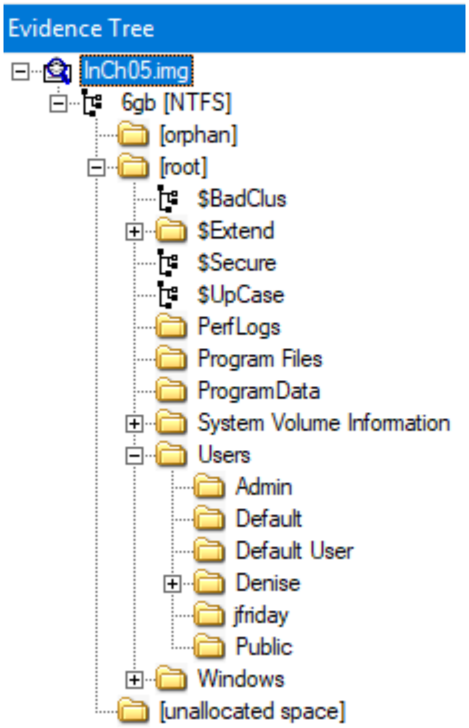
The figure above shows the folder in our image which is 6gb New Technology File System (NTFS). Then we expanded to 6gb NTFS which had three folders as shown above.



```
Evidence Tree
InCh05.img
  6gb [NTFS]
    [orphan]
    [root]
      $BadClus
      $Extend
      $Secure
      $UpCase
      PerfLogs
      Program Files
      ProgramData
      System Volume Information
      Users
      Windows
    [unallocated space]
```

Figure 14/ROOT.

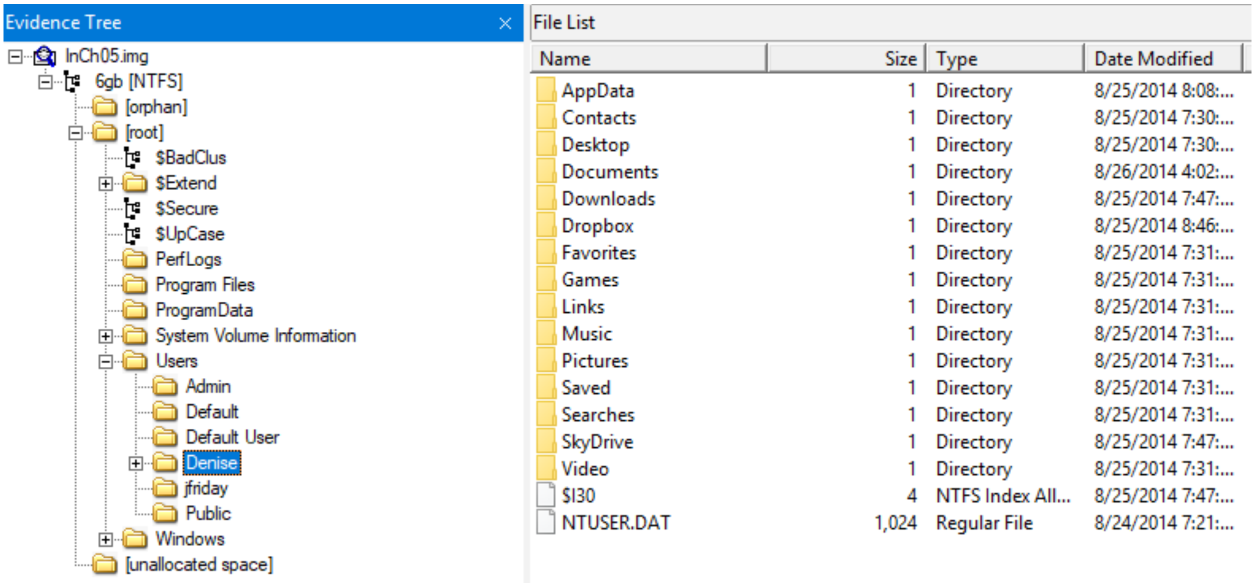
The above figure shows the root folder expanded which displays the various folders.



```
Evidence Tree
⊟ InCh05.img
  ⊟ 6gb [NTFS]
      [orphan]
    ⊟ [root]
        $BadClus
      ⊞ $Extend
        $Secure
        $UpCase
        PerfLogs
        Program Files
        ProgramData
      ⊞ System Volume Information
      ⊟ Users
          Admin
          Default
          Default User
        ⊞ Denise
          jfriday
          Public
      ⊞ Windows
      [unallocated space]
```

Figure 15/Users.

The above figure shows the expanded users folder. We expanded the Denise folder and exported the NTUSER.dat on to our virtual machine that we will utilize later. The figure below shows the contents in the Denise folder.



Evidence Tree

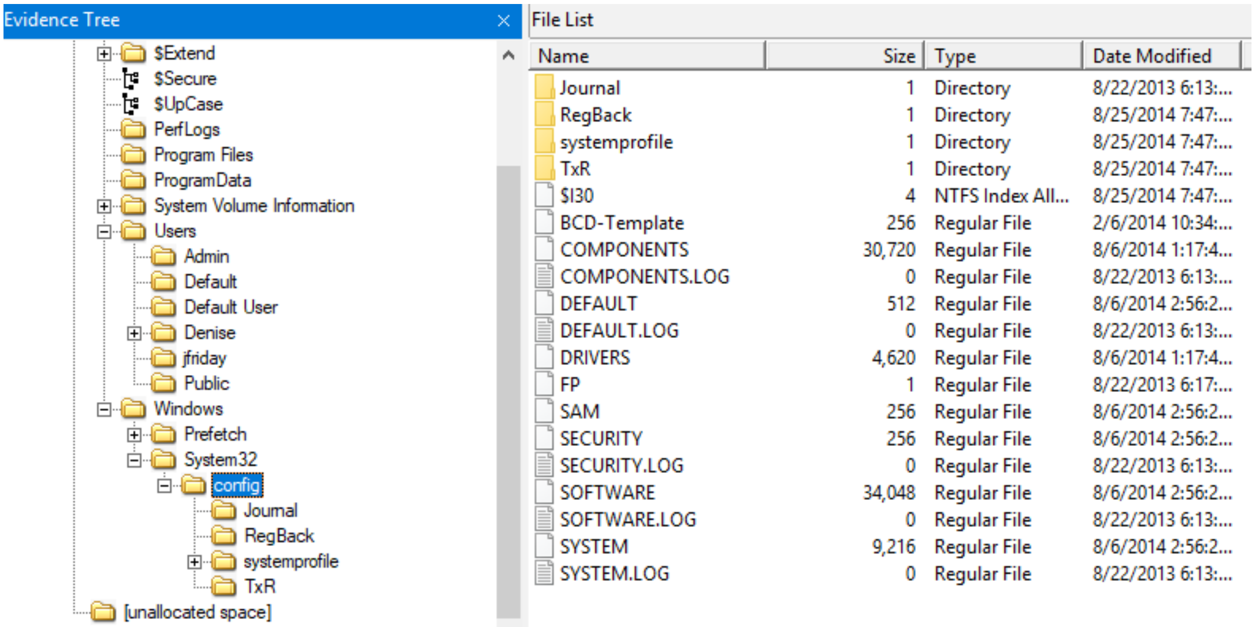
```
InCh05.img
  6gb [NTFS]
    [orphan]
    [root]
      $BadClus
      $Extend
      $Secure
      $UpCase
      PerfLogs
      Program Files
      ProgramData
      System Volume Information
      Users
        Admin
        Default
        Default User
        Denise
        jfriday
        Public
      Windows
    [unallocated space]
```

File List

Name	Size	Type	Date Modified
AppData	1	Directory	8/25/2014 8:08:...
Contacts	1	Directory	8/25/2014 7:30:...
Desktop	1	Directory	8/25/2014 7:30:...
Documents	1	Directory	8/26/2014 4:02:...
Downloads	1	Directory	8/25/2014 7:47:...
Dropbox	1	Directory	8/25/2014 8:46:...
Favorites	1	Directory	8/25/2014 7:31:...
Games	1	Directory	8/25/2014 7:31:...
Links	1	Directory	8/25/2014 7:31:...
Music	1	Directory	8/25/2014 7:31:...
Pictures	1	Directory	8/25/2014 7:31:...
Saved	1	Directory	8/25/2014 7:31:...
Searches	1	Directory	8/25/2014 7:31:...
SkyDrive	1	Directory	8/25/2014 7:47:...
Video	1	Directory	8/25/2014 7:31:...
$I30	4	NTFS Index All...	8/25/2014 7:47:...
NTUSER.DAT	1,024	Regular File	8/24/2014 7:21:...

Figure 16/Denise.

We went further and expanded the windows folder under root, then windows then system 32 and finally config. Under this folder we exported the SAM, DEFAULT, SYSTEM, SOFTWARE and SECURITY to our virtual machine as shown in the figure below.



Evidence Tree

```
      $Extend
      $Secure
      $UpCase
      PerfLogs
      Program Files
      ProgramData
      System Volume Information
      Users
        Admin
        Default
        Default User
        Denise
        jfriday
        Public
      Windows
        Prefetch
        System32
          config
            Journal
            RegBack
            systemprofile
            TxR
    [unallocated space]
```

File List

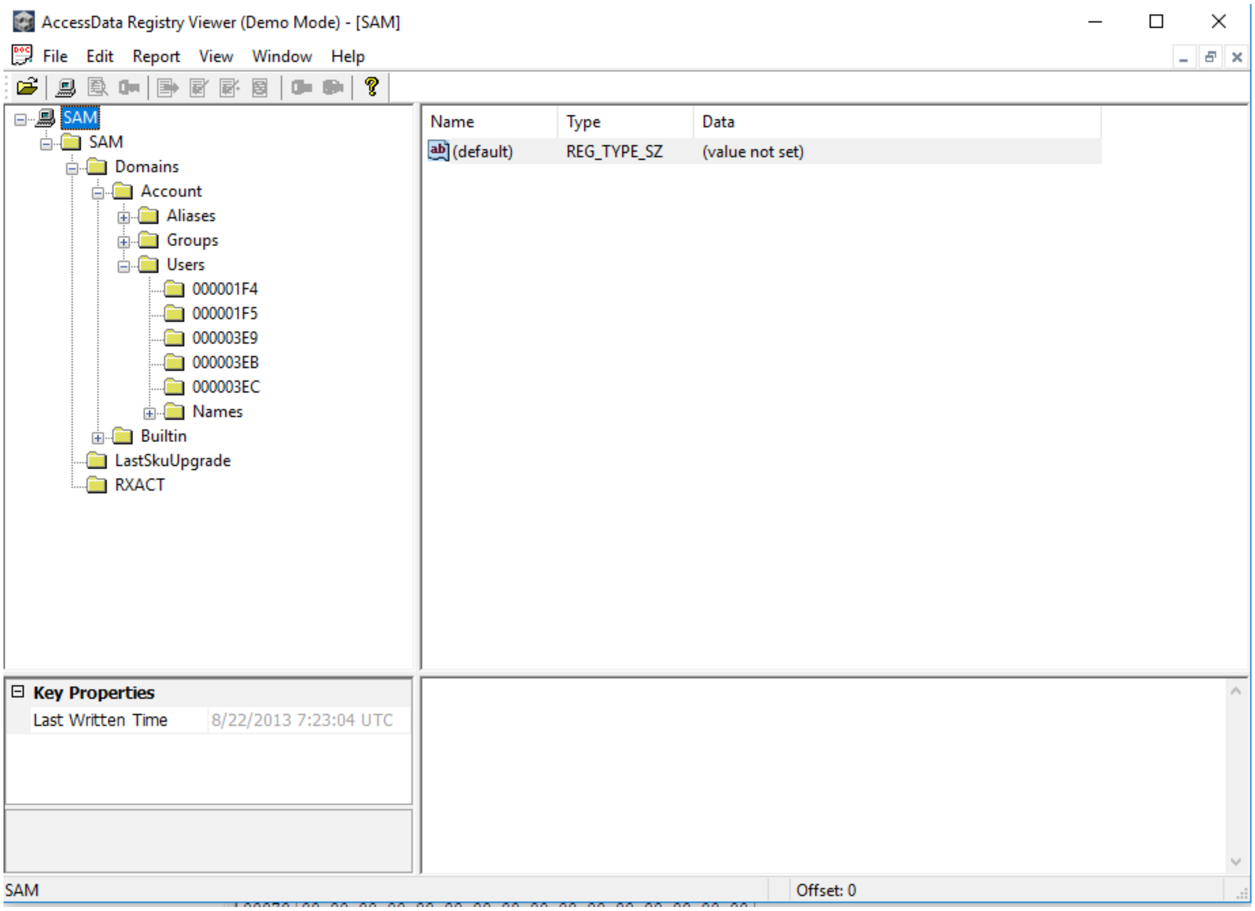
Name	Size	Type	Date Modified
Journal	1	Directory	8/22/2013 6:13:...
RegBack	1	Directory	8/25/2014 7:47:...
systemprofile	1	Directory	8/25/2014 7:47:...
TxR	1	Directory	8/25/2014 7:47:...
$I30	4	NTFS Index All...	8/25/2014 7:47:...
BCD-Template	256	Regular File	2/6/2014 10:34:...
COMPONENTS	30,720	Regular File	8/6/2014 1:17:4...
COMPONENTS.LOG	0	Regular File	8/22/2013 6:13:...
DEFAULT	512	Regular File	8/6/2014 2:56:2...
DEFAULT.LOG	0	Regular File	8/22/2013 6:13:...
DRIVERS	4,620	Regular File	8/6/2014 1:17:4...
FP	1	Regular File	8/22/2013 6:17:...
SAM	256	Regular File	8/6/2014 2:56:2...
SECURITY	256	Regular File	8/6/2014 2:56:2...
SECURITY.LOG	0	Regular File	8/22/2013 6:13:...
SOFTWARE	34,048	Regular File	8/6/2014 2:56:2...
SOFTWARE.LOG	0	Regular File	8/22/2013 6:13:...
SYSTEM	9,216	Regular File	8/6/2014 2:56:2...
SYSTEM.LOG	0	Regular File	8/22/2013 6:13:...

Figure 17/Config.

Examining the SAM Hive

Security Accounts Manager (SAM) is a database where the windows Microsoft operating system stores sensitive information such as user accounts, passwords, and security descriptors (Katie, 2022).

The figure below shows Registry viewer display that we used to open the SAM file that we had exported in the prior steps above. This shows the different users' details that contain vital information.



Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

Key Properties	
Last Written Time	8/22/2013 7:23:04 UTC

Figure 18/Registry Viewer

We used each user’s information to populate the table below.

Name (Full Name)	Hex	Decimal Conversion	SID unique identifier	Password Required	Has Password
HomeGroupUser$ (HomeGroupUser$)	000003EB	1003	1003	True	True for NTLMv2 False LAN Manager
Administrator	000001F4	500	500	True	True for NTLMv2 False LAN Manager
Guest	000001F5	501	501	False	False for NTLMv2 False LAN Manager
Jfriday(jfriday)	000003E9	1001	1001	false	True for NTLMv2 False LAN Manager

Denise (Denise Robinson)	000003EC	1004	1004	True	True for NTLMv2 False LAN Manager

Table 1/User Information

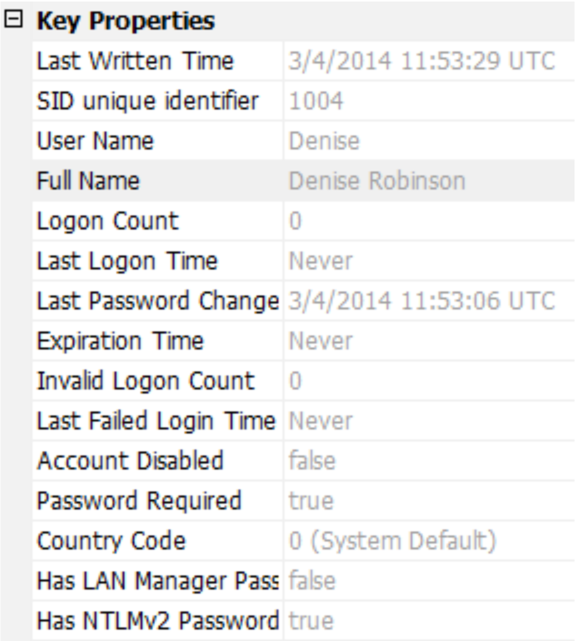
The folder names in hexadecimals when converted to decimal generate a figure that matches the SID unique identifier. This is vital since its comparison associates the folder with a user who has the matched SID unique identifier. SID unique identifier is a unique value used to identify a security entity such as a user account or a security group (Peter, 2022).

From our populated table above jfriday does not require a password while Denise requires one. Both users have passwords set and can be verified from the last password change logs for the users.

Passwords can be set but not required same as in jfriday's scenario where accounts can be set with a password not required flag and they can be able to log into the account with a blank password (Robert, 2024).

Jfriday was the user that logged into system the most with a count of seven. Denise Robinson never logged into the system according to our analysis in the log. Jfriday's account password last set on 2/6/2014 18:44:26 UTC (coordinated universal time).

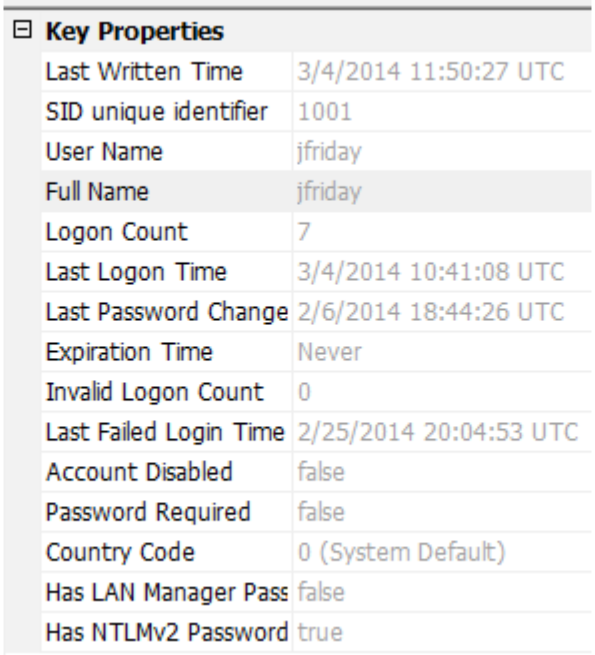
The figures below validate the information we gave in the prior paragraphs.



⊟ **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	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 Pass	false
Has NTLMv2 Password	true

Figure 19/Denise Info



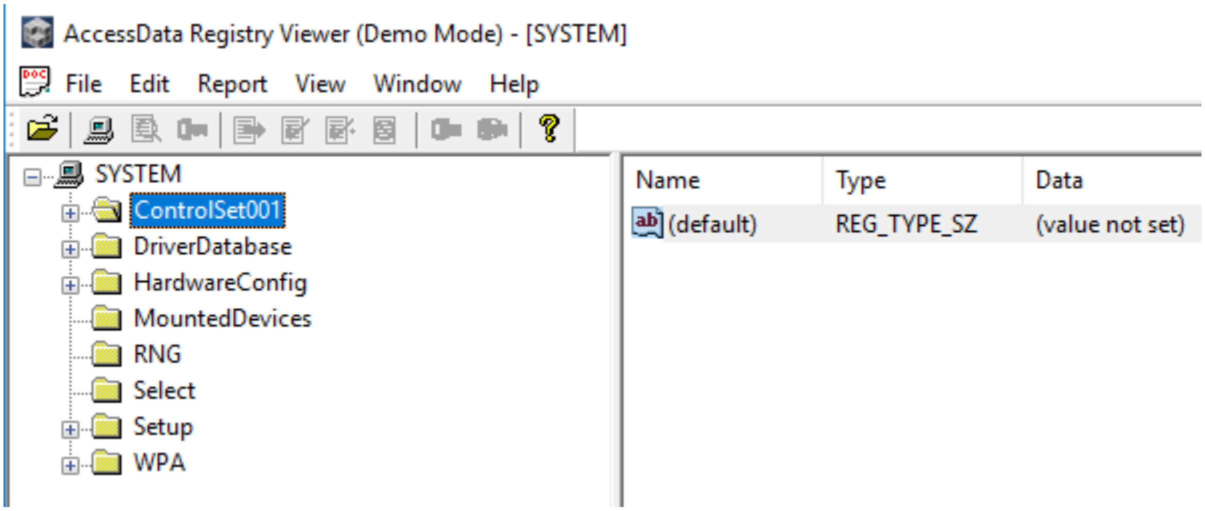
⊟ **Key Properties**

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	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 Pass	false
Has NTLMv2 Password	true

Figure 20/Jfriday Info

Examining the System Hive

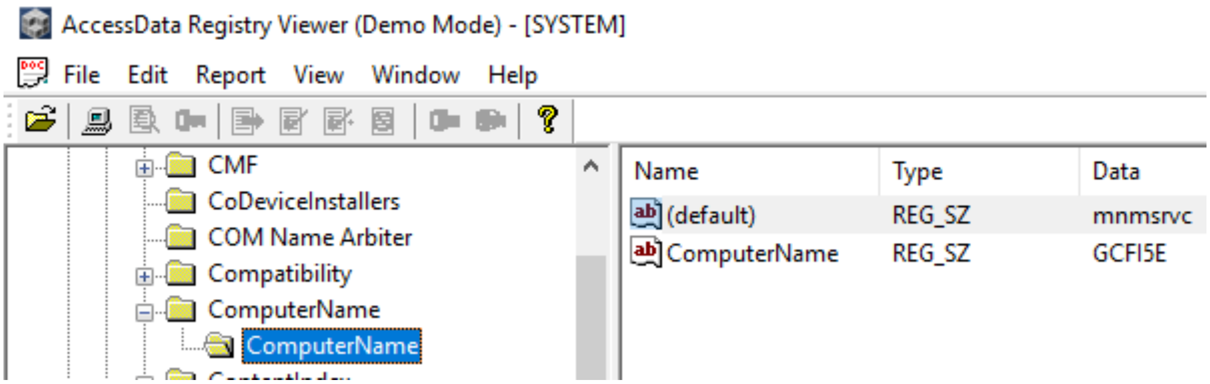
System hive contains information about all the hardware items in the system, including details about its configuration, device drivers, services, and system settings (Chirath, 2019). The figure below shows Registry viewer display that we used to open the SYSTEM file that we had exported earlier in this lab.



Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

Figure 21/System.

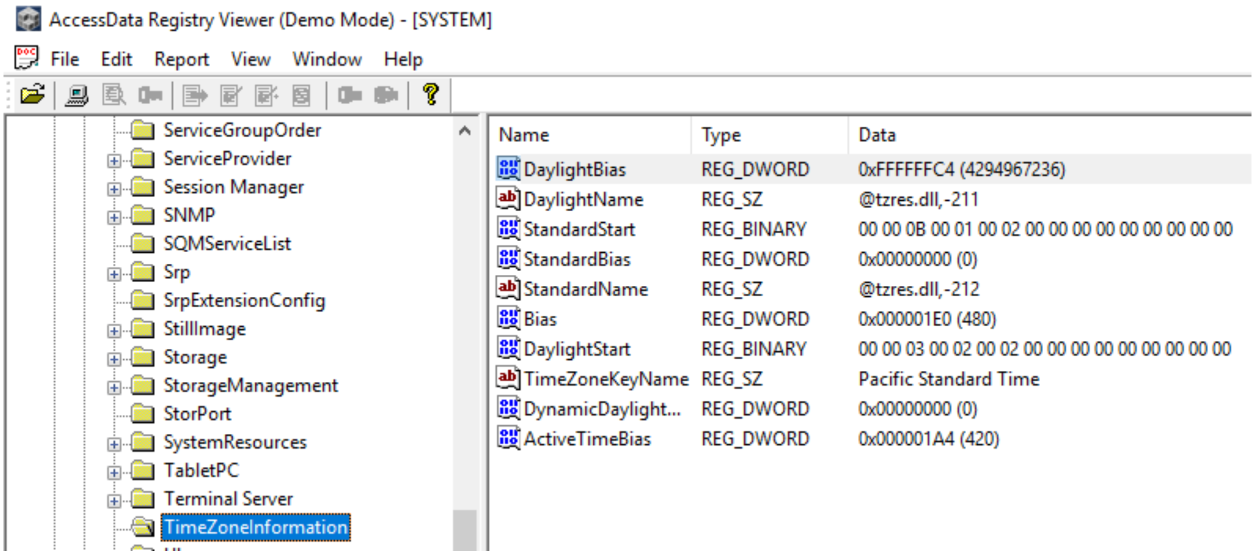
The above figure shows that the current key set is 001.This key simply tells the active configuration settings that the operating system is currently using (Manish, 2024).



Name	Type	Data
(default)	REG_SZ	mnmsrvc
ComputerName	REG_SZ	GCFI5E

Figure 22/Computer name.

The above figure shows the computer name being GCFI53.

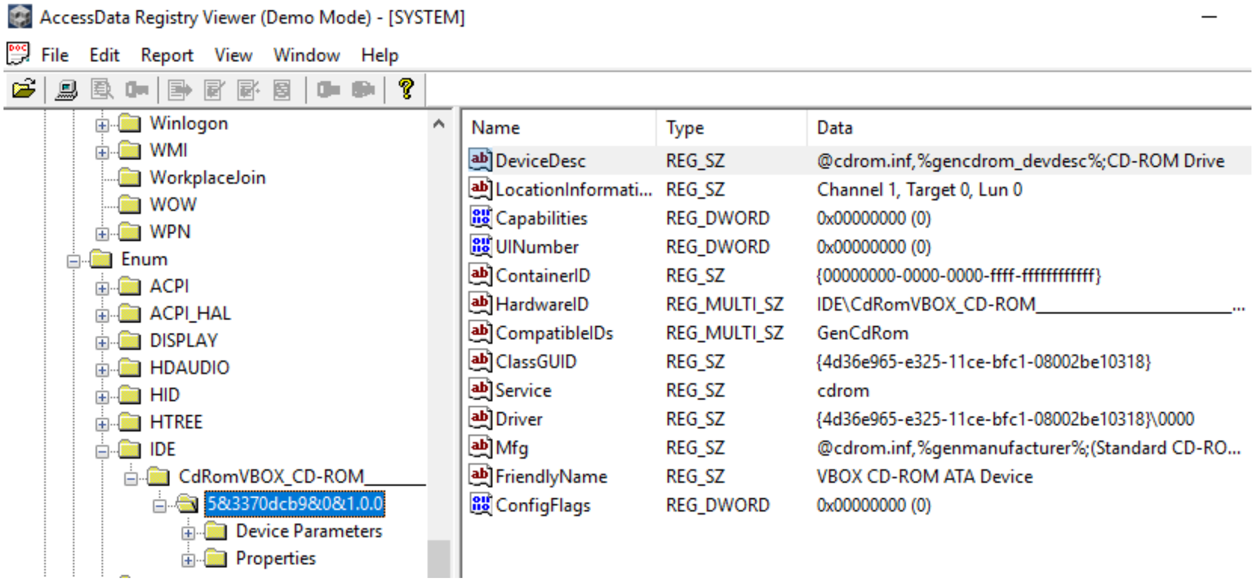


Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-211
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-212
Bias	REG_DWORD	0x000001E0 (480)
DaylightStart	REG_BINARY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

Figure 23/Time zone.

The above figure displays the time zone information of the computer which is set to Pacific Standard Time.

We expanded the Enum folder which contains additional details on hardware devices such as mounted USB storage devices, including external memory cards. Then we expanded the IDE (Integrated drive electronics) which stores details of hard drives and optical drives (Lih, 2011). The friendly name is used to display a readable name for a device (imacken, 2017).

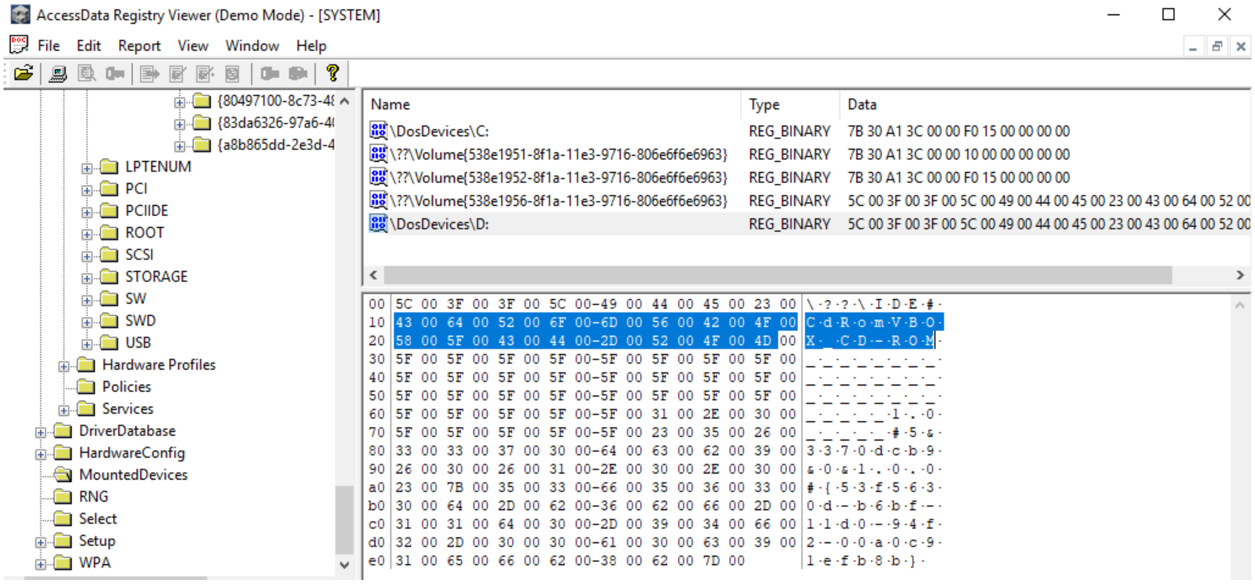


Name	Type	Data
DeviceDesc	REG_SZ	@cdrom.inf,%gencdrom_devdesc%;CD-ROM Drive
LocationInformati...	REG_SZ	Channel 1, Target 0, Lun 0
Capabilities	REG_DWORD	0x00000000 (0)
UINumber	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{00000000-0000-0000-ffff-ffffffffffff}
HardwareID	REG_MULTI_SZ	IDE\CdRomVBOX_CD-ROM_____________________________...
CompatibleIDs	REG_MULTI_SZ	GenCdRom
ClassGUID	REG_SZ	{4d36e965-e325-11ce-bfc1-08002be10318}
Service	REG_SZ	cdrom
Driver	REG_SZ	{4d36e965-e325-11ce-bfc1-08002be10318}\0000
Mfg	REG_SZ	@cdrom.inf,%genmanufacturer%;(Standard CD-RO...
FriendlyName	REG_SZ	VBOX CD-ROM ATA Device
ConfigFlags	REG_DWORD	0x00000000 (0)

Figure 24/Friendly name.

The figure above shows the friendly name as VBOX CD-ROM ATA Device.

We clicked on the mounted devices to determine the letter which the CD ROM was mounted, and it is GUID value as shown in the figure below.



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 23 00 43 00 64 00 52 00
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 64 00 52 00

```
00 5C 00 3F 00 3F 00 5C 00-49 00 44 00 45 00 23 00  \·?·?·\·I·D·E·#·
10 43 00 64 00 52 00 6F 00-6D 00 56 00 42 00 4F 00  C·d·R·o·m·V·B·O·
20 58 00 5F 00 43 00 44 00-2D 00 52 00 4F 00 4D 00  X·_·C·D·-·R·O·M·
30 5F 00 5F 00 5F 00 5F 00-5F 00 5F 00 5F 00 5F 00  _·_·_·_·_·_·_·_·
40 5F 00 5F 00 5F 00 5F 00-5F 00 5F 00 5F 00 5F 00  _·_·_·_·_·_·_·_·
50 5F 00 5F 00 5F 00 5F 00-5F 00 5F 00 5F 00 5F 00  _·_·_·_·_·_·_·_·
60 5F 00 5F 00 5F 00 5F 00-5F 00 31 00 2E 00 30 00  _·_·_·_·_·1·.·0·
70 5F 00 5F 00 5F 00 5F 00-5F 00 23 00 35 00 26 00  _·_·_·_·_·#·5·&·
80 33 00 33 00 37 00 30 00-64 00 63 00 62 00 39 00  3·3·7·0·d·c·b·9·
90 26 00 30 00 26 00 31 00-2E 00 30 00 2E 00 30 00  &·0·&·1·.·0·.·0·
a0 23 00 7B 00 35 00 33 00-66 00 35 00 36 00 33 00  #·{·5·3·f·5·6·3·
b0 30 00 64 00 2D 00 62 00-36 00 62 00 66 00 2D 00  0·d·-·b·6·b·f·-·
c0 31 00 31 00 64 00 30 00-2D 00 39 00 34 00 66 00  1·1·d·0·-·9·4·f·
d0 32 00 2D 00 30 00 30 00-61 00 30 00 63 00 39 00  2·-·0·0·a·0·c·9·
e0 31 00 65 00 66 00 62 00-38 00 62 00 7D 00        1·e·f·b·8·b·}·
```

Figure 25/Drive letter.

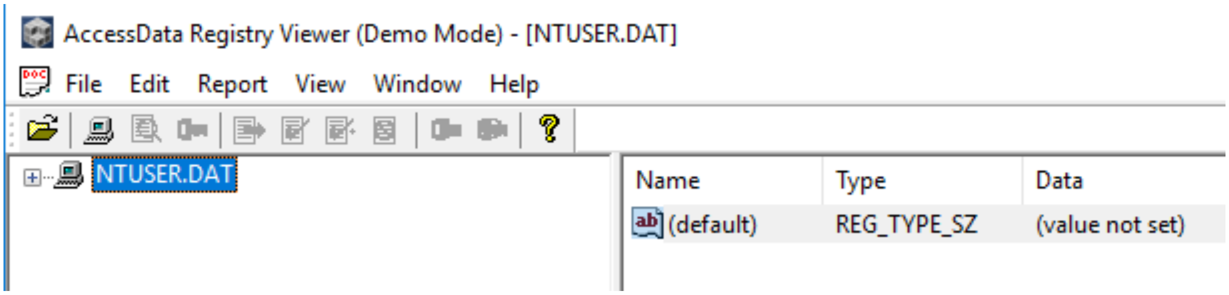
The CD ROM was mounted to drive D as shown above and the GUID value was {53f5630d-b6bf-11d0-94f2-00a0c91efb8b}.

From the figure above there are only two mounted devices assigned to a drive letter which are C and D.

Examining the NTUSER.DAT File

NTUSER.DAT is a registry file where a user profile is loaded from. This file stores the user profile software and operating system settings. This file is usually created for every user on the computer (Random, 2024).

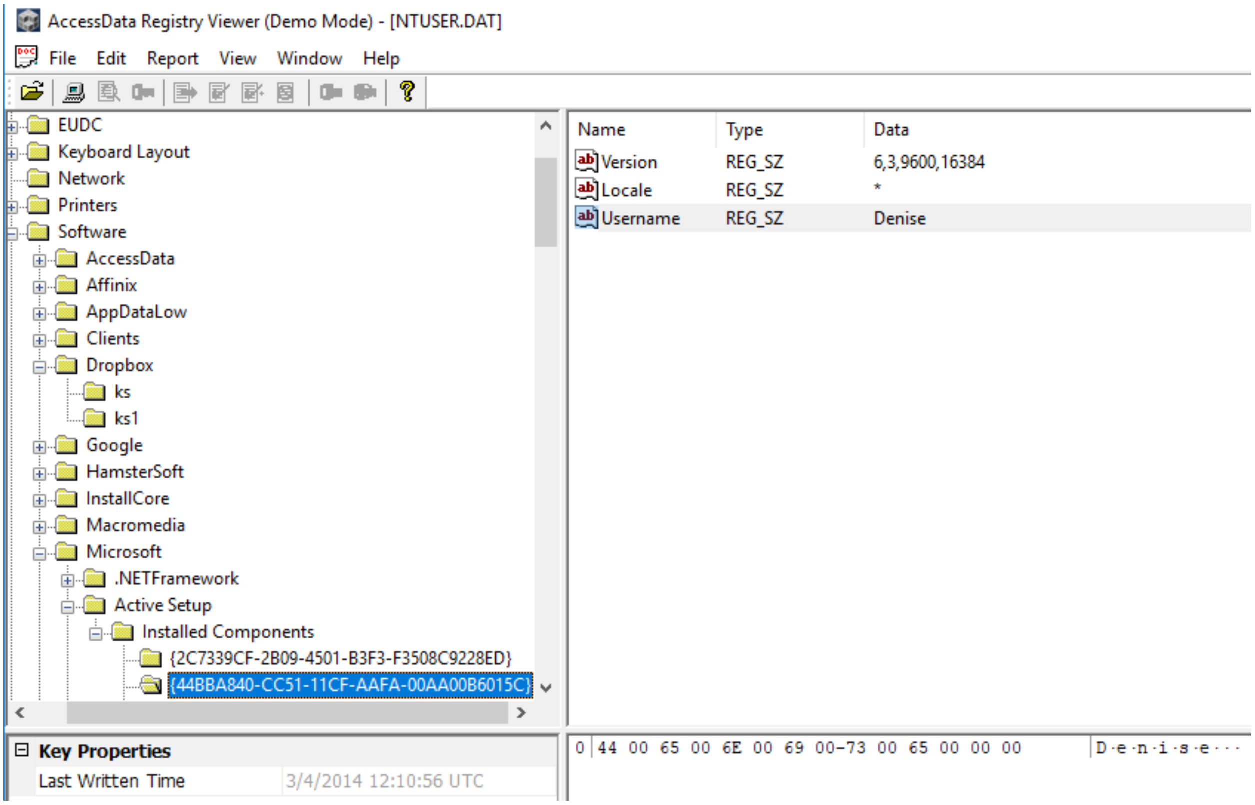
The figure below shows the Registry viewer display that we used to open the NTUSER.DAT file for the user Denise that we had exported earlier in this lab.



Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

Figure 26/Denise.

The installed component GUID is well highlighted in blue in the figure below.



Name	Type	Data
Version	REG_SZ	6,3,9600,16384
Locale	REG_SZ	*
Username	REG_SZ	Denise

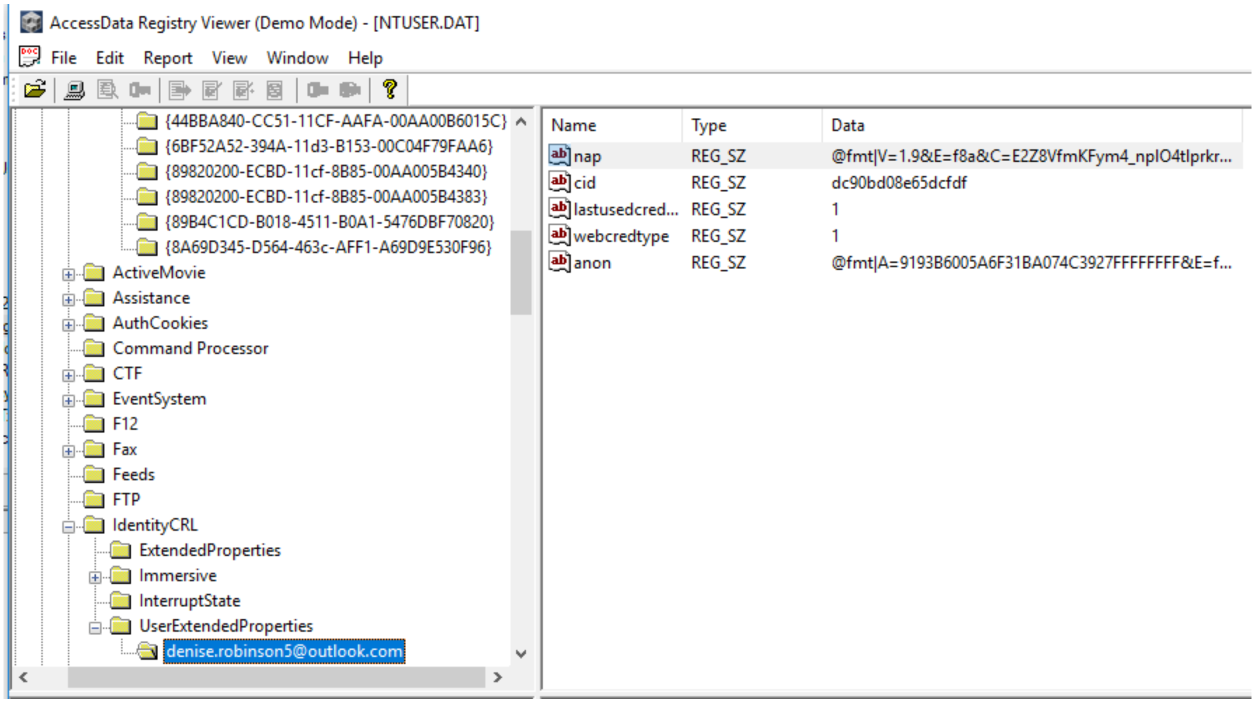
```
0 44 00 65 00 6E 00 69 00-73 00 65 00 00 00      D·e·n·i·s·e···
```

Key Properties

Last Written Time 3/4/2014 12:10:56 UTC

Figure 27/GUID.

The GUID is {44BBA840-CC51-11CF-AAFA-00AA0086015C}



```
{44BBA840-CC51-11CF-AAFA-00AA00B6015C}
{6BF52A52-394A-11d3-B153-00C04F79FAA6}
{89820200-ECBD-11cf-8B85-00AA005B4340}
{89820200-ECBD-11cf-8B85-00AA005B4383}
{89B4C1CD-B018-4511-B0A1-5476DBF70820}
{8A69D345-D564-463c-AFF1-A69D9E530F96}
ActiveMovie
Assistance
AuthCookies
Command Processor
CTF
EventSystem
F12
Fax
Feeds
FTP
IdentityCRL
  ExtendedProperties
  Immersive
  InterruptState
  UserExtendedProperties
    denise.robinson5@outlook.com
```

Name	Type	Data
nap	REG_SZ	@fmt|V=1.9&E=f8a&C=E2Z8VfmKFym4_nplO4tlprkr...
cid	REG_SZ	dc90bd08e65dcfdf
lastusedcred...	REG_SZ	1
webcredtype	REG_SZ	1
anon	REG_SZ	@fmt|A=9193B6005A6F31BA074C3927FFFFFFFF&E=f...

Figure 28/Email.

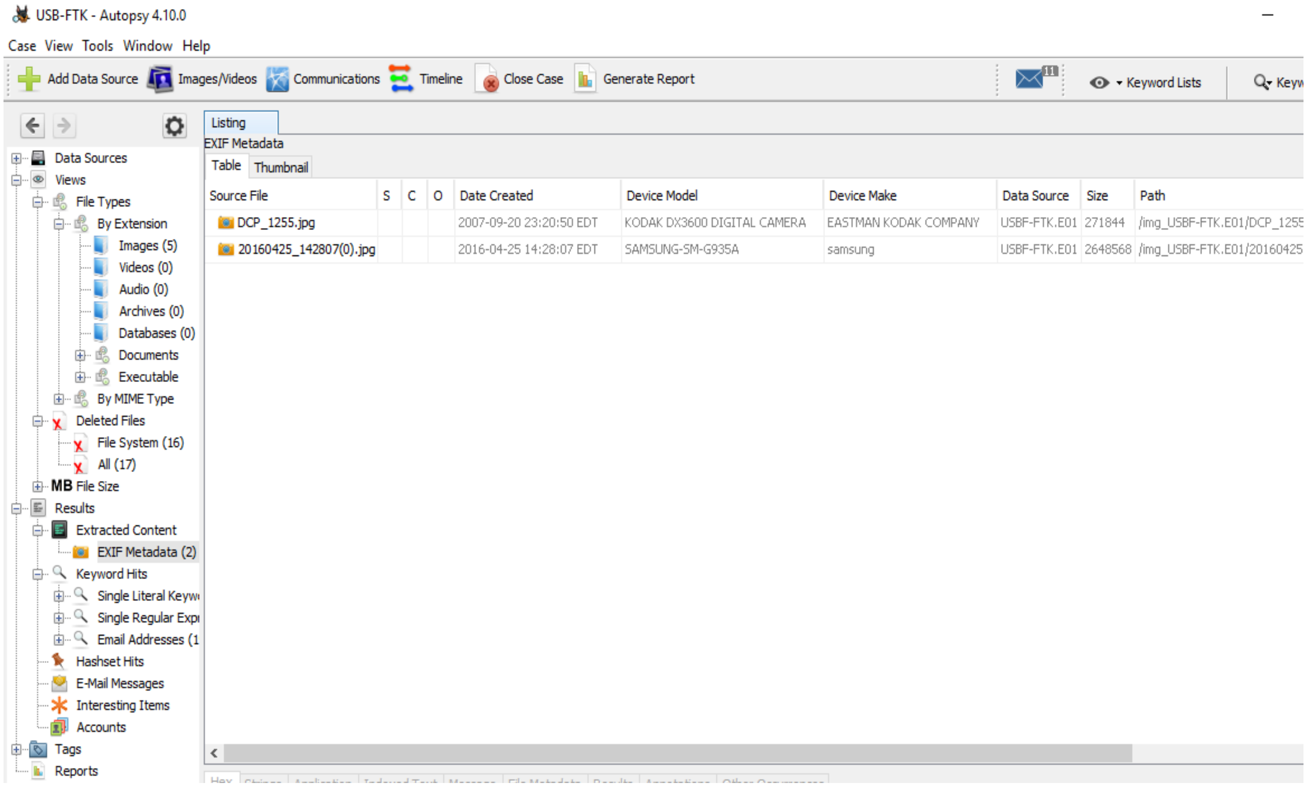
Denise’s email account is denise.robinson5@outlook.com.

There was no information matched with jfriday because each user has a unique copy of their NTUSER.DAT file. To obtain information about jfriday we would have to export a different file associated with the account.

Image forensics

Analysis of image files

We will be using Autopsy to create a new case and browse to an image that we had earlier acquired using the FTK Imager tool. In this lab we selected the USBF image which did not have any picture files deleted but did have two picture that were captured and 3 that were downloaded. The figures below show the results category of the extracted picture files, and the metadata returned.



Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path
DCP_1255.jpg				2007-09-20 23:20:50 EDT	KODAK DX3600 DIGITAL CAMERA	EASTMAN KODAK COMPANY	USBF-FTK.E01	271844	/img_USBF-FTK.E01/DCP_1255
20160425_142807(0).jpg				2016-04-25 14:28:07 EDT	SAMSUNG-SM-G935A	samsung	USBF-FTK.E01	2648568	/img_USBF-FTK.E01/20160425

Figure 29/Autopsy1.

The figure above returns vital information which is discussed below:

Date created- This shows the date and time the picture file was taken.

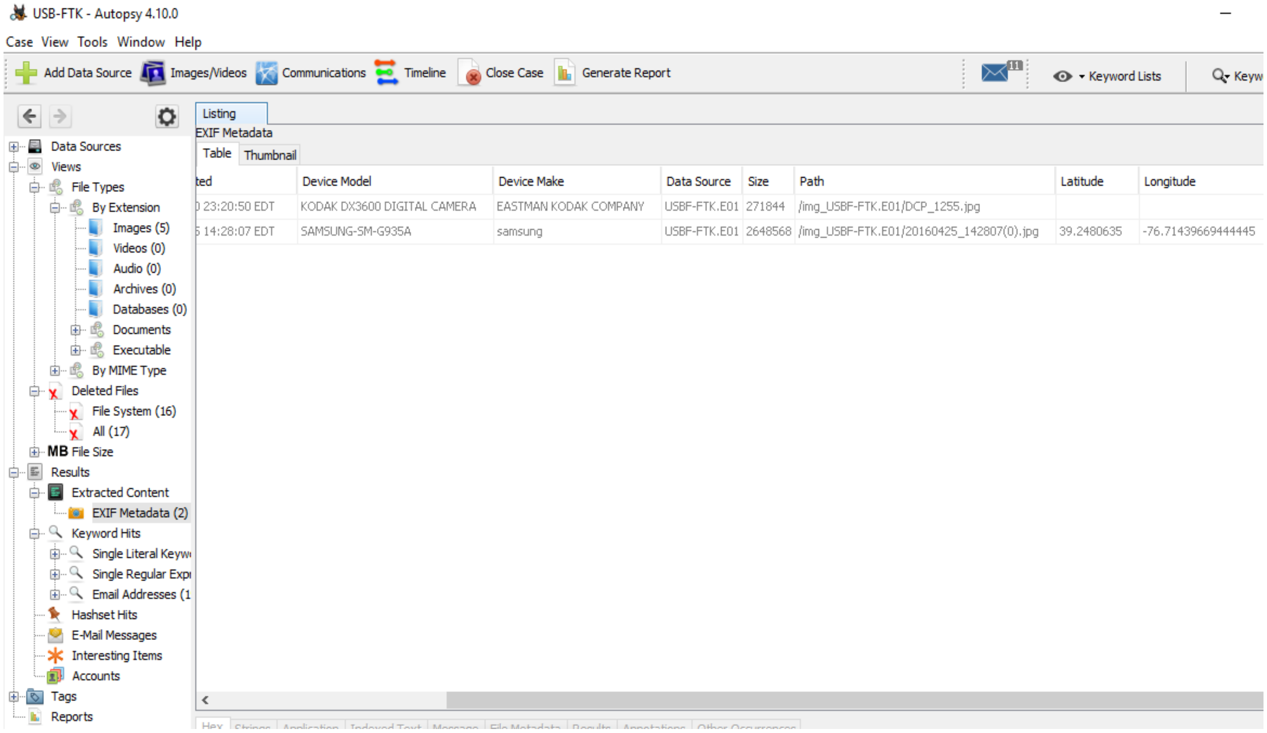
Device Model – This shows the device model used to capture the picture file.

Device make – This shows the device company brand.

Data source – shows the data source which was an image we had acquired earlier using the FTK Imager tool.

Size – This shows the file size in bytes.

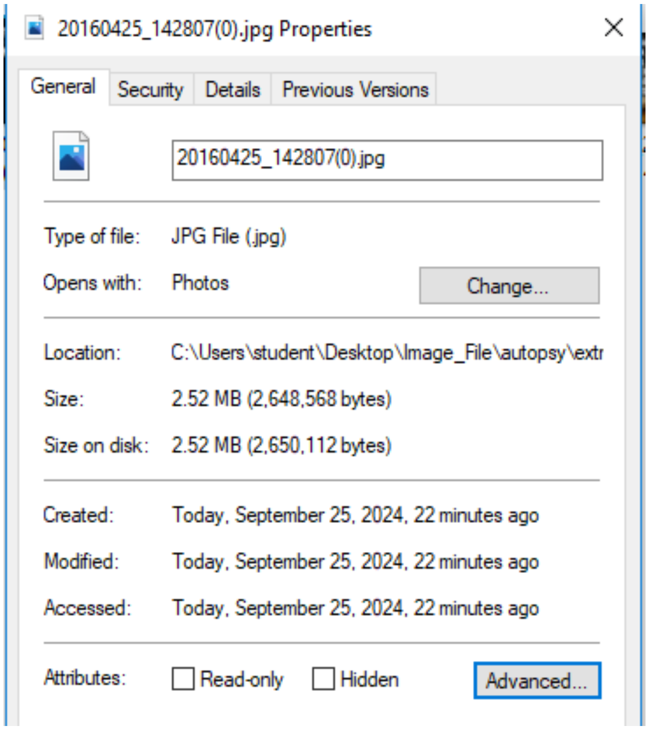
Path – this shows the location path where the file was acquired from.



ted	Device Model	Device Make	Data Source	Size	Path	Latitude	Longitude
0 23:20:50 EDT	KODAK DX3600 DIGITAL CAMERA	EASTMAN KODAK COMPANY	USBF-FTK.E01	271844	/img_USBF-FTK.E01/DCP_1255.jpg		
5 14:28:07 EDT	SAMSUNG-SM-G935A	samsung	USBF-FTK.E01	2648568	/img_USBF-FTK.E01/20160425_142807(0).jpg	39.2480635	-76.71439669444445

The last two columns show the latitude and the longitude coordinates of the picture files.

After manually checking the metadata, we noticed some information that was not available in the autopsy tool above. The following figures show the additional information we discovered.



20160425_142807(0).jpg

Type of file: JPG File (.jpg)

Opens with: Photos

Location: C:\Users\student\Desktop\Image_File\autopsy\extr

Size: 2.52 MB (2,648,568 bytes)

Size on disk: 2.52 MB (2,650,112 bytes)

Created: Today, September 25, 2024, 22 minutes ago

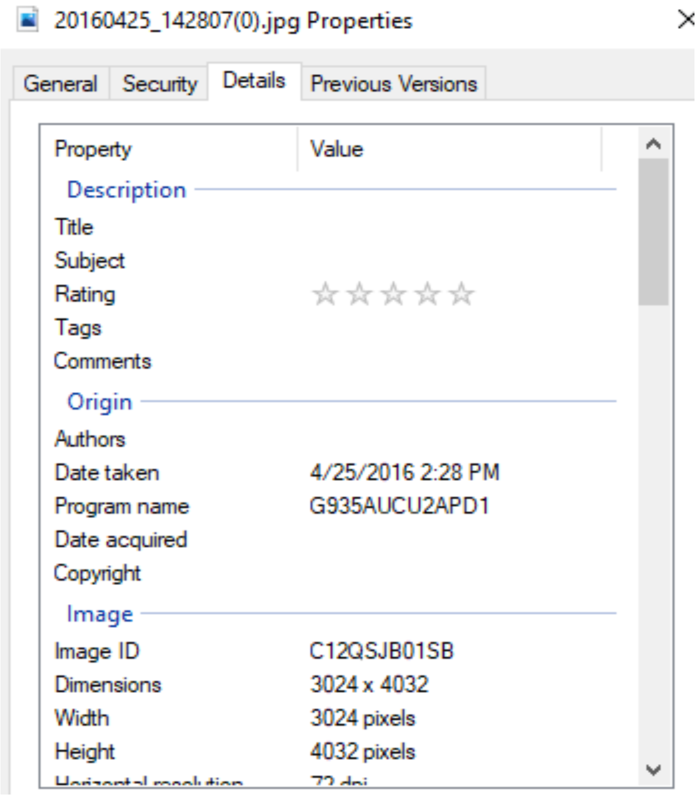
Modified: Today, September 25, 2024, 22 minutes ago

Accessed: Today, September 25, 2024, 22 minutes ago

Attributes: □ Read-only □ Hidden

Figure 30/Details1.

The above figure shows additional information for the modification and accessed dates.

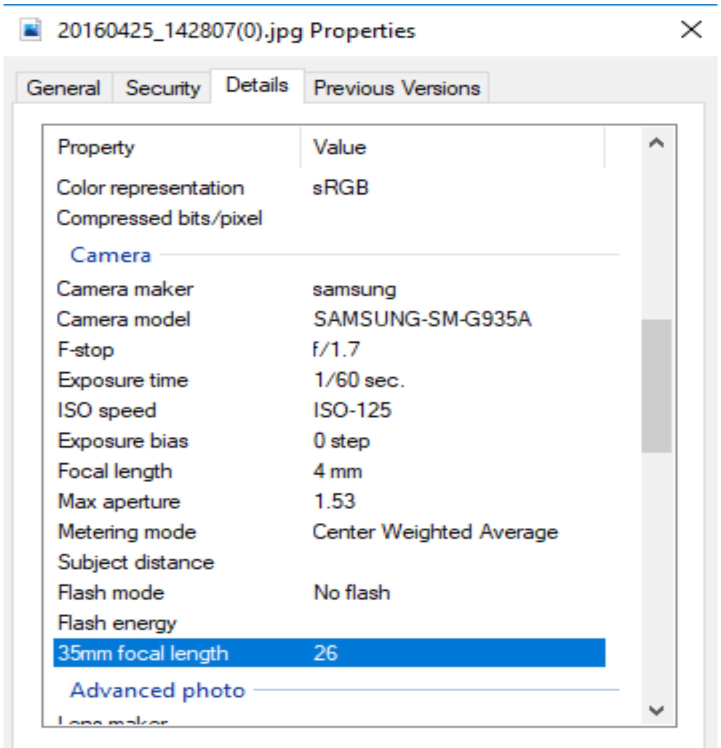


20160425_142807(0).jpg Properties

Property	Value
Description	
Title	
Subject	
Rating	☆☆☆☆☆
Tags	
Comments	
Origin	
Authors	
Date taken	4/25/2016 2:28 PM
Program name	G935AUCU2APD1
Date acquired	
Copyright	
Image	
Image ID	C12QSJB01SB
Dimensions	3024 x 4032
Width	3024 pixels
Height	4032 pixels
Horizontal resolution	72 dpi

Figure 31/Details2.

The additional information given above under the image category was not available in the autopsy.

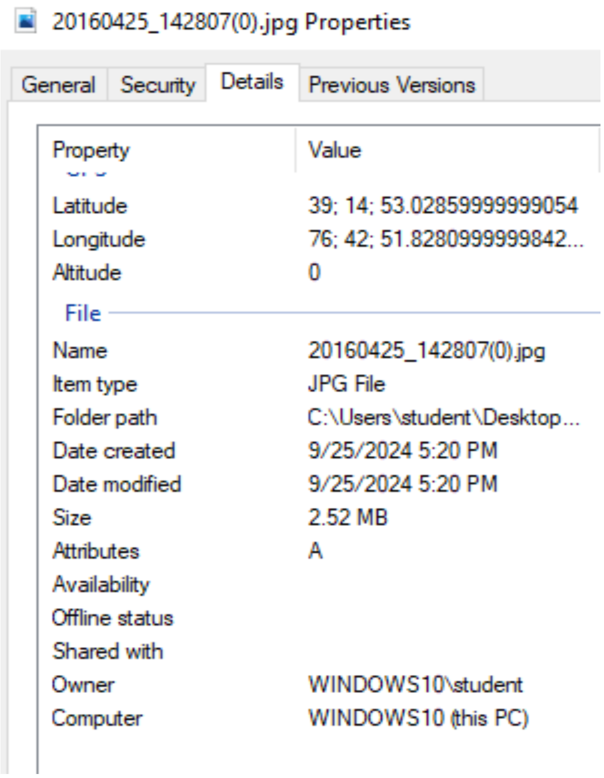


20160425_142807(0).jpg Properties

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	

Figure 32/Details3.

The camera details above contain additional information such as the ISO speed exposure time, Focal length, Max aperture, and metering mode.



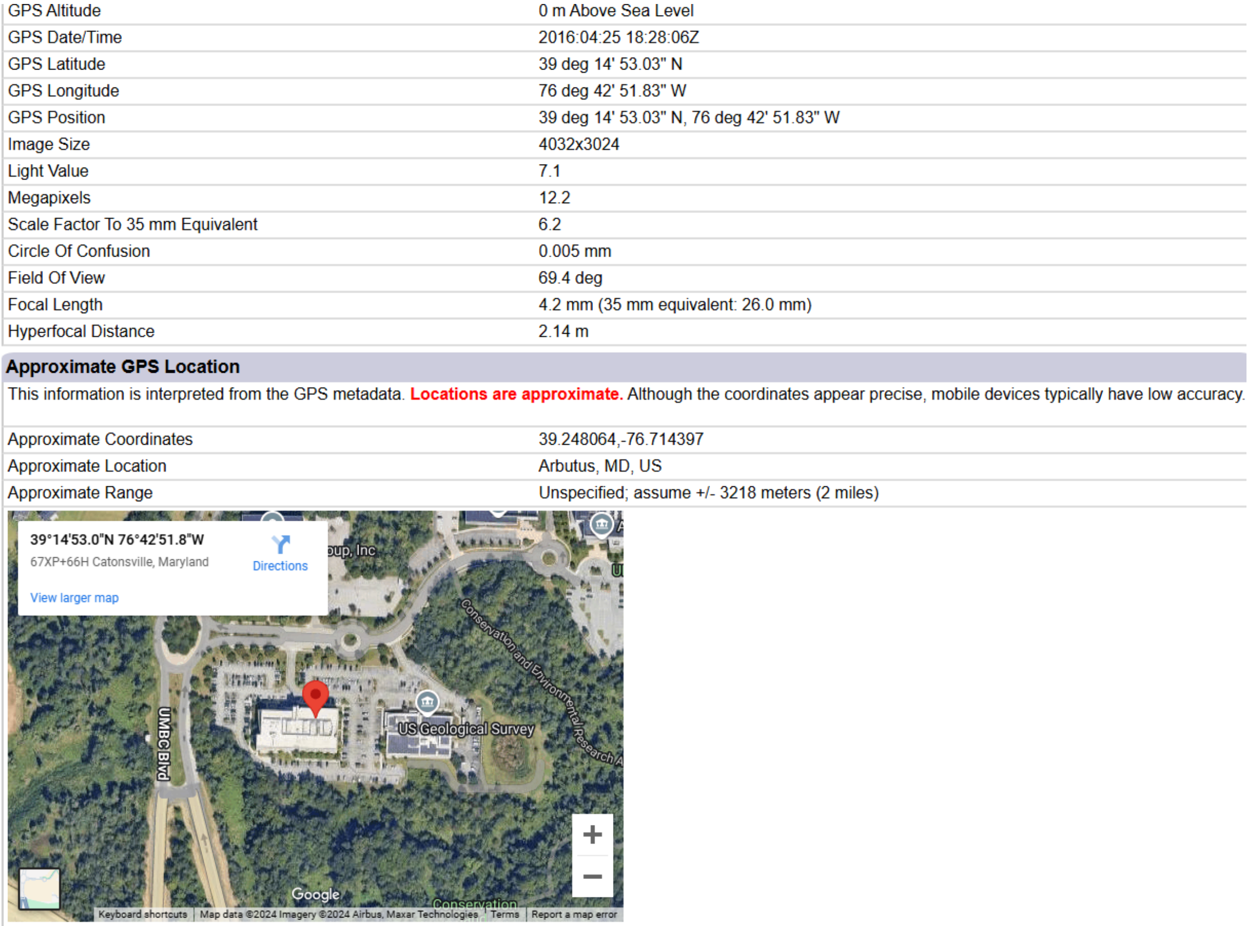
20160425_142807(0).jpg Properties

Property	Value
Latitude	39; 14; 53.02859999999054
Longitude	76; 42; 51.8280999999842...
Altitude	0
File	
Name	20160425_142807(0).jpg
Item type	JPG File
Folder path	C:\Users\student\Desktop...
Date created	9/25/2024 5:20 PM
Date modified	9/25/2024 5:20 PM
Size	2.52 MB
Attributes	A
Availability	
Offline status	
Shared with	
Owner	WINDOWS10\student
Computer	WINDOWS10 (this PC)

Figure 33/Details4.

The above figures were for one of the pictures that had location information returned, and we picked it as our picture file to focus on.

We uploaded the picture on https://fotoforensics.com/ to check for any additional details of the location the file was captured. The figure below shows the approximate location of where the picture file was captured.



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)

39°14'53.0"N 76°42'51.8"W
67XP+66H Catonsville, Maryland
Directions
View larger map
oup, Inc
Conservation and Environmental Research
US Geological Survey
UMBC Blvd
Google
Conservation
Keyboard shortcuts
Map data ©2024 Imagery ©2024 Airbus, Maxar Technologies
Terms
Report a map error

Figure 34/Location.

I would do this if it were legal as it gives me precise information which could be vital in the investigation.

Glossary

Bookmarks – This is a digital pointer that a user can return to a selected file (Margaret, 2017).

Cache – This is a hardware or software that is used to store data temporarily (Ben, 2021).

Cookies – These are small text files that websites send to your device and are used to monitor and remember information about a user (Emily, 2019).

GUID – Stands for Globally unique identifier which is a unique alphanumeric string to identify hardware components (Tim, 2023).

Hard drive – This is an external or internal storage device in computer (Brian, 2023).

NTFS-Stands for New Technology File System which was introduced to cover the limitations of the File allocation system (Ben, 2021) .

Optical drives – This is defined as a device that reads and writes data onto a disc using a laser (Margaret, 2021).

References

Ben, L. (2021, October 04). *Cache*. Retrieved from TechTarget: https://www.techtarget.com/searchstorage/definition/cache

Ben, L. (2021, April). *NTFS (NT File System)*. Retrieved from TechTarget: https://www.techtarget.com/searchwindowsserver/definition/NTFS

Brian, P. (2023 , January 11). *Hard Drive*. Retrieved from TechTerms: https://techterms.com/definition/hard_drive

Chirath, D. A. (2019, April 5). *Windows Registry Analysis 101*. Retrieved from ForensicFocus: https://www.forensicfocus.com/articles/windows-registry-analysis-101/

Emily, S. (2019, December 10). *Why every website wants you to accept its cookies*. Retrieved from Vox: https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy

Harlan, C. (2011). In *Windows Registry Forensics* (pp. 1-2). Burlington: Elsevier.

imacken. (2017, May 8). *Trying to change 'FriendlyName' in registry*. Retrieved from Windowstenforums: https://www.tenforums.com/general-support/83850-trying-change-friendlyname-registry.html

Katie, T. (2022, February 07). *Security Accounts Manager*. Retrieved from TechTarget: https://www.techtarget.com/searchenterprisedesktop/definition/Security-Accounts-Manager#:~:text=The%20Security%20Accounts%20Manager%20%28SAM%29%20is%20a%20database,data%20breach%20in%20case%20the%20system%20is%20stolen.

Lih, W. W. (2011, July 10). *Forensic Analysis of the Windows Registry*. Retrieved from ForensicFocus: https://www.forensicfocus.com/articles/forensic-analysis-of-the-windows-registry/

Manish, S. (2024, June 23). *What is Windows Registry? What are Registry Hives, Keys, Subkeys, Values, Data Types, Value Types?* Retrieved from thePCinsider: https://www.thepcinsider.com/windows-registry-hives-keys-subkeys-values-data-types-value-types/

Margaret, R. (2017, January 27). *What Does Bookmark Mean?* Retrieved from techopedia: https://www.techopedia.com/definition/271/bookmark

Margaret, R. (2021, July 22). *Optical Drive*. Retrieved from Techopedia: https://www.techopedia.com/definition/5308/optical-drive

Mayur, R. J., & Dr. Bandu, B. M. (2018). Web Browser Forensics for Detecting User Activities. *International Research Journal of Engineering and Technology (IRJET)*, 273.

Peter, L. (2022, march 8). *security identifier (SID)*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/security-identifier

Random. (2024, January 27). *What is ntuser.dat and Why is it on My Computer?* Retrieved from TechJunkie: https://www.techjunkie.com/ntuser-dat/

Robert, A. (2024, July 21). *Find Accounts with Password Not Required (Blank Password)*. Retrieved from Active Directory Pro: https://activedirectorypro.com/find-accounts-with-password-not-required-blank-password/

Tim, F. (2023, February 21). *Device Class GUIDs for Common Hardware*. Retrieved from Lifewire: https://www.lifewire.com/device-class-guids-for-most-common-types-of-hardware-2619208