Lab 4

Registry and Browser Forensics

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

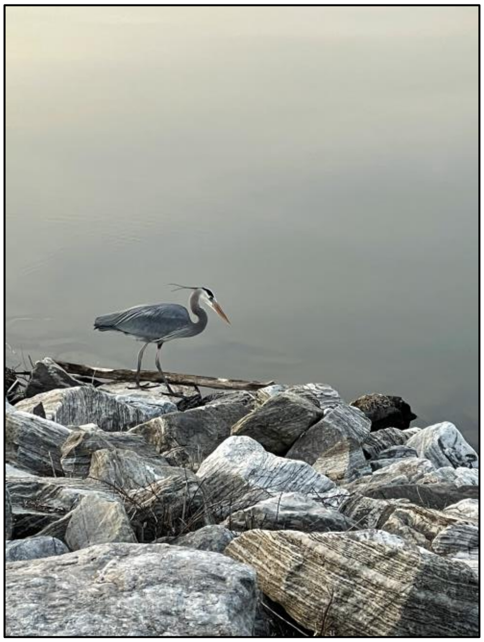
02/26/2025

Introduction

The Windows Registry and browser artifacts are critical sources of forensic evidence, often containing valuable information about user activity, system configurations, and application usage. In this lab, we are analyzing Registry data extracted from a forensic image to uncover potential evidence and system interactions. Additionally, we will examine image files to retrieve metadata, timestamps, and hidden information, which can provide context regarding file origins, modifications, and user behavior. Understanding Registry forensics and image metadata analysis is essential for forensic investigations, helping analysts reconstruct digital events and ensure the integrity of evidence (Carvey, 2018; Nelson et al., 2020).

Pre-Analysis

Metadata analysis is crucial in digital forensics, providing investigators with essential information about digital images, such as device details, timestamps, and GPS coordinates. This lab will analyz image metadata using www.imageforensic.org, allowing students to determine whether their images contain embedded forensic data such as camera type, location, and modification history. By examining the metadata, investigators can understand why certain images retain location data while others do not, which is often influenced by privacy settings, file formats, and metadata removal processes. Mastering image forensics helps forensic analysts verify the authenticity, origin, and integrity of digital images, a crucial skill in both criminal investigations and cybersecurity contexts (Nelson et al., 2020).



In this section of the lab, I conducted image forensic analysis by uploading an image to www.imageforensic.org. This forensic tool provides detailed metadata extraction and analysis, offering various types of information about the uploaded image. Upon uploading the image, I was presented with several forensic data categories, including EXIF (Exchangeable Image File Format), ELA (Error Level Analysis), Signatures, and Map information (Nelson et al., 2020).

Map Information: Displays GPS location data embedded in the image, showing where the picture was taken. If GPS data is absent, it may indicate that location services were disabled at the time the photo was captured or that metadata was stripped during file transfer (Nelson et al., 2020)

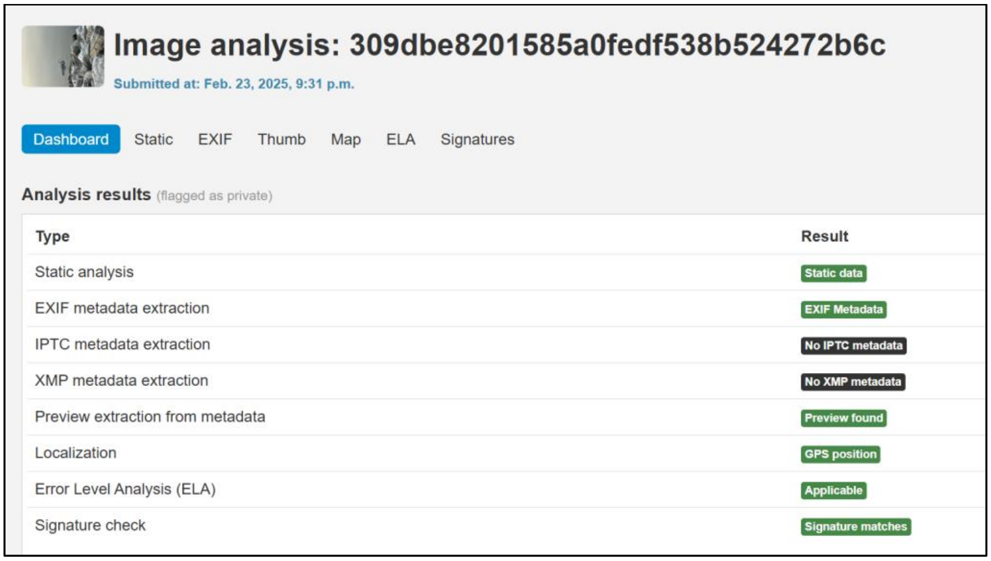


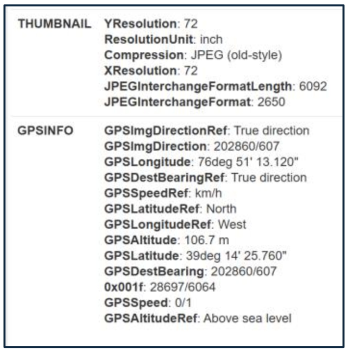
Image analysis: 309dbe8201585a0fedf538b524272b6c

Submitted at: Feb. 23, 2025, 9:31 p.m.

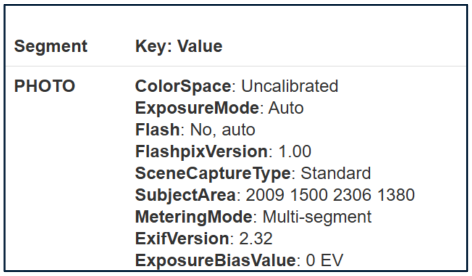
Analysis results (flagged as private)

Type	Result
Static analysis	Static data
EXIF metadata extraction	EXIF Metadata
IPTC metadata extraction	No IPTC metadata
XMP metadata extraction	No XMP metadata
Preview extraction from metadata	Preview found
Localization	GPS position
Error Level Analysis (ELA)	Applicable
Signature check	Signature matches

EXIF (Exchangeable Image File Format) Data: Contains metadata embedded by the camera or smartphone, including device make and model, timestamp, GPS coordinates, shutter speed, aperture settings, and ISO levels. EXIF data is crucial for identifying where, when, and how an image was taken (Casey, 2011).



THUMBNAIL	**YResolution**: 72 **ResolutionUnit**: inch **Compression**: JPEG (old-style) **XResolution**: 72 **JPEGInterchangeFormatLength**: 6092 **JPEGInterchangeFormat**: 2650
GPSINFO	**GPSImgDirectionRef**: True direction **GPSImgDirection**: 202860/607 **GPSLongitude**: 76deg 51' 13.120" **GPSDestBearingRef**: True direction **GPSSpeedRef**: km/h **GPSLatitudeRef**: North **GPSLongitudeRef**: West **GPSAltitude**: 106.7 m **GPSLatitude**: 39deg 14' 25.760" **GPSDestBearing**: 202860/607 **0x001f**: 28697/6064 **GPSSpeed**: 0/1 **GPSAltitudeRef**: Above sea level



Segment	Key: Value
PHOTO	**ColorSpace**: Uncalibrated **ExposureMode**: Auto **Flash**: No, auto **FlashpixVersion**: 1.00 **SceneCaptureType**: Standard **SubjectArea**: 2009 1500 2306 1380 **MeteringMode**: Multi-segment **ExifVersion**: 2.32 **ExposureBiasValue**: 0 EV

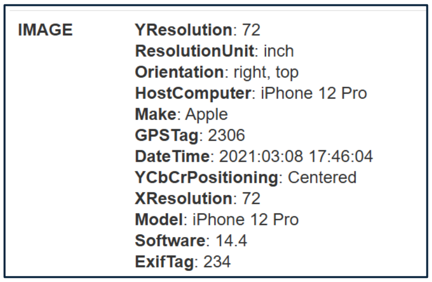
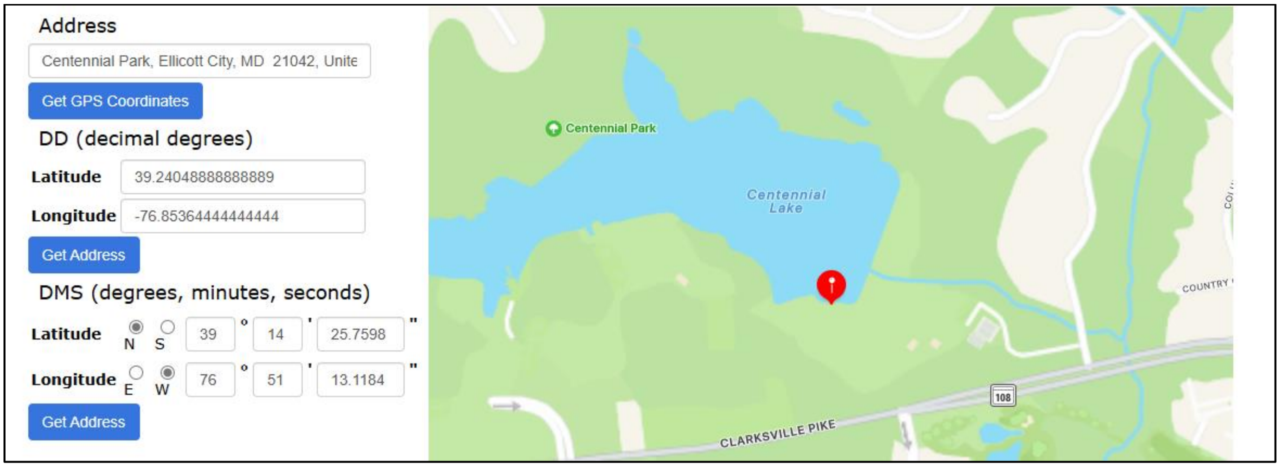


IMAGE	**YResolution**: 72 **ResolutionUnit**: inch **Orientation**: right, top **HostComputer**: iPhone 12 Pro **Make**: Apple **GPSTag**: 2306 **DateTime**: 2021:03:08 17:46:04 **YCbCrPositioning**: Centered **XResolution**: 72 **Model**: iPhone 12 Pro **Software**: 14.4 **ExifTag**: 234



Address

Centennial Park, Ellicott City, MD 21042, Unite

DD (decimal degrees)

Latitude 39.24048888888889

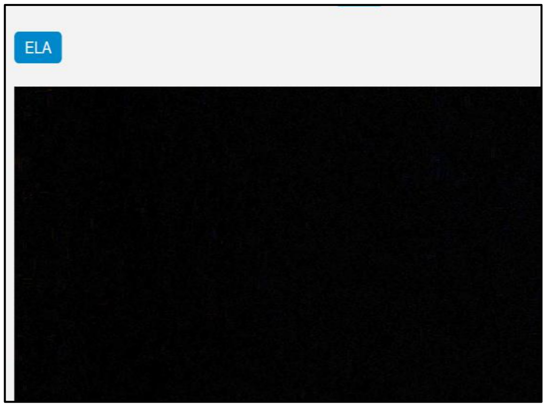
Longitude -76.85364444444444

DMS (degrees, minutes, seconds)

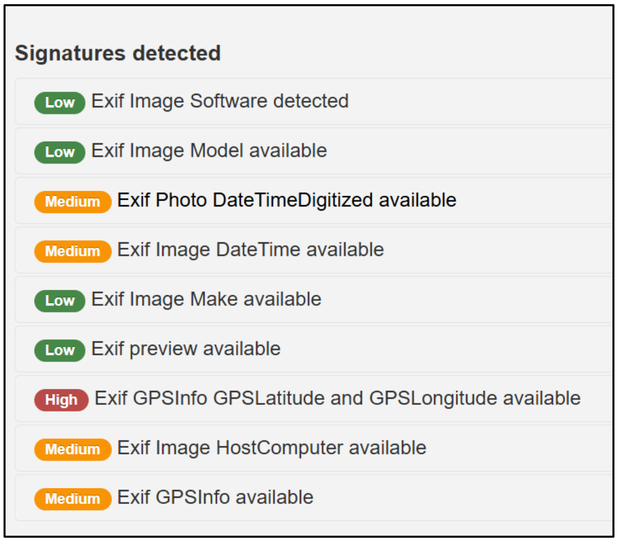
Latitude ● N ○ S 39 ° 14 ' 25.7598 "

Longitude ○ E ● W 76 ° 51 ' 13.1184 "

ELA (Error Level Analysis): Highlights discrepancies in image compression, allowing forensic investigators to detect potential image tampering or alterations. If different areas of the image show inconsistent compression levels, it may indicate modifications, such as digital forgeries or enhancements (Farid, 2009).



Signatures: Examines the unique digital fingerprint of an image to verify its originality. This feature helps forensic analysts determine whether an image matches a known database or has been manipulated in any way.



Signatures detected

- Low Exif Image Software detected
- Low Exif Image Model available
- Medium Exif Photo DateTimeDigitized available
- Medium Exif Image DateTime available
- Low Exif Image Make available
- Low Exif preview available
- High Exif GPSInfo GPSLatitude and GPSLongitude available
- Medium Exif Image HostComputer available
- Medium Exif GPSInfo available

Other components that might be available during image forensics are:

IPTC Metadata

The International Press Telecommunications Council (IPTC) metadata is a standardized format used to embed descriptive and administrative information within an image file. IPTC metadata is widely used in photojournalism, media organizations, and digital asset management to provide essential details about the image's author, copyright information, caption, keywords, and licensing (McHugh, 2013).

XMP Metadata

Extensible Metadata Platform (XMP) is a metadata standard developed by Adobe Systems that provides a more flexible and structured way of embedding metadata into digital files, including images, documents, and multimedia files (Adobe Systems, 2018).

When conducting forensic analysis on an image, certain metadata such as GPS location, camera type, and device information may be missing or altered. This can happen due to various technical, software, or user-related factors that influence how metadata is stored, preserved, or stripped from an image file. Below are the primary reasons why some metadata may not be visible during forensic analysis.

1. Many social media platforms and cloud storage services automatically remove metadata from uploaded images to protect user privacy. When an image is uploaded to services like:
    - Facebook, Instagram, Twitter, and WhatsApp, EXIF metadata is stripped to prevent tracking.
    - Google Photos and iCloud retain metadata for organizational purposes but may remove it when the image is downloaded.
2. When an image is edited, resized, or converted to another format, metadata may be lost in the process.

- Cropping or applying filters in editing software (e.g., Photoshop, GIMP) may remove metadata.
- Saving an image in a different format (e.g., converting JPEG to PNG or BMP) may strip EXIF data.
- Exporting images from certain applications (e.g., screenshots from mobile devices) may result in a file that lacks original metadata.

3. Privacy Settings on Mobile Devices & Cameras; Many modern smartphones and digital cameras allow users to disable metadata recording, including:

- Turning off GPS tagging in camera settings.
- Using privacy settings that prevent location tracking.
- Blocking metadata sharing in specific apps.

4. Image Compression & Data Loss; Certain image compression techniques may remove or corrupt metadata, especially when images are:

- Compressed for faster web loading (e.g., automatic resizing by websites).
- Sent via messaging apps like WhatsApp, which compress images and strip EXIF data to reduce file size.
- Stored in lower-resolution formats, which may discard certain metadata fields.

5. Image Was Taken on a Device Without Metadata Capabilities; Older digital cameras, certain low-end smartphones, and security cameras may not embed metadata due to hardware or firmware limitations.

- Basic digital cameras and scanners may not record EXIF data.

- Screenshots typically lack original metadata unless captured metadata is included in the image properties.
- Security footage and surveillance systems often store metadata separately rather than embedding it within image files.

Analysis

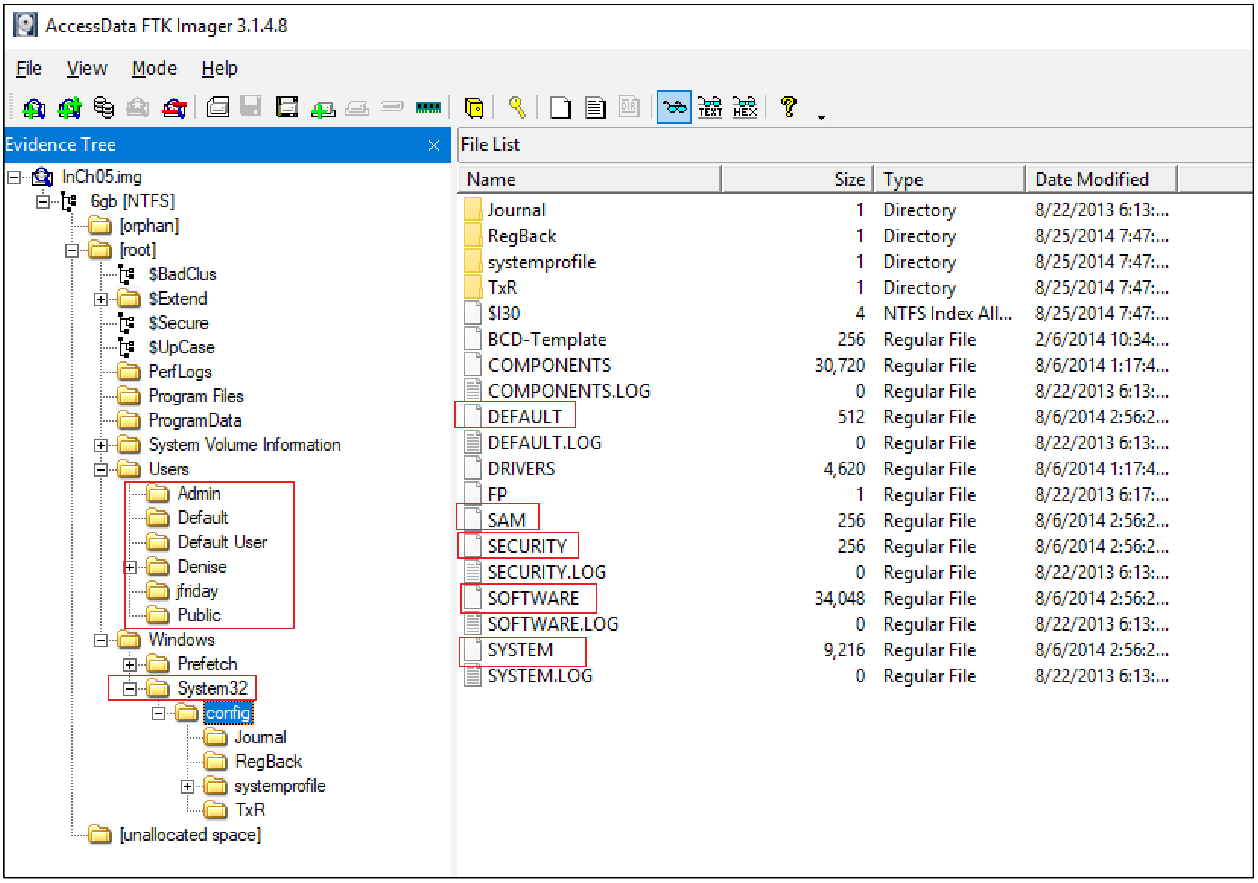
In digital forensic investigations, registry analysis and metadata extraction play a crucial role in uncovering critical systems and user activity. This lab delves deep into registry forensics by examining registry files and images extracted from a Dell Workstation. The forensic image, InCh05.img, stored on the Windows VM (E:\Registry Forensics), will be analyzed using FTK Imager, Registry Viewer, and Autopsy to extract and interpret metadata. This lab provides hands-on experience in registry examination, user activity tracking, and digital artifact recovery, equipping students with the skills necessary for real-world forensic investigations (Nelson et al., 2020).

1. Extracting Registry Files from Disk Image

For this section, launch FTK Imager and navigate to File → Add Evidence Item. Select the InCh05.img forensic image, which is located at E:\Registry Forensics\InCh05.img on the Windows VM. Once the image is loaded, access the System32 directory and export the following registry files: SAM, DEFAULT, SYSTEM, SOFTWARE, and SECURITY. Additionally, locate the NTUSER.dat file within the Users\Denis folder and export it for further analysis.

What are the users folders listed under InCh05.img then 6gb [NTFS] then [root] then Users?

- Admin, Default, Default User, Denis, jfriday, Public



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:...

2. Examining the SAM Hive

In this section, launch Registry Viewer and navigate to File → Open. Locate the registry file exported in the previous step and select SAM to open it for analysis.

Expand SAM --> Domains --> Account --> Users folders.

Full Name	Hex	Decimal Conversion	SID unique ID	Password Required	Has Password
Administrator	000001F4	500	500	true	true
Guest	000001F5	501	501	false	false
jfriday	000003E9	1001	1001	false	true
HomeGroupUser$	000003EB	1003	1003	true	true
Denis Robinson	000003EC	1004	1004	true	true

1. What do you notice about the Folder name when converted to decimal? What is this telling you? Folder name in hex is equivalent to users' SID unique ID
2. Do the user jfriday and Denise have required password? No
3. Do the user jfriday and Denise have password set? Yes
4. If a password is set but not required what does that mean?

   This setting may indicate that a user account was configured for convenience at the expense of security.
5. Which account logged into the system the most? jfriday
6. Has Denise Robinson logged in? No
7. Identify when jfriday's account password was last set? 2/6/2014 18:44:26 UTC

3. Examining the SYSTEM Hive

- What is the Current key set to? 1

Expand SYSTYEM --> ControlSet001 --> Control --> ComputerName --> ComputerName to answer the following:

- What is the computer name this image is from? GCFI5E

Scroll down to TimeZoneInformation folder and select it.

- What is the computer's time zone set to? Pacific Standard Time

Now expand the Enum folder and then IDE folder.

- What is the Friendly Name of the CD ROM? VBOX CD-ROM ATA DEVICE

Click on System --> MountedDevices

- Determine what letter the CD ROM was mounted as and it's GUID value.

  CD ROM was mounted on D drive

  {538e1956-8f1a-11e3-9716-806ef6e6963}

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

  Two (C and D)

4. Examining the NTUSER.DAT File

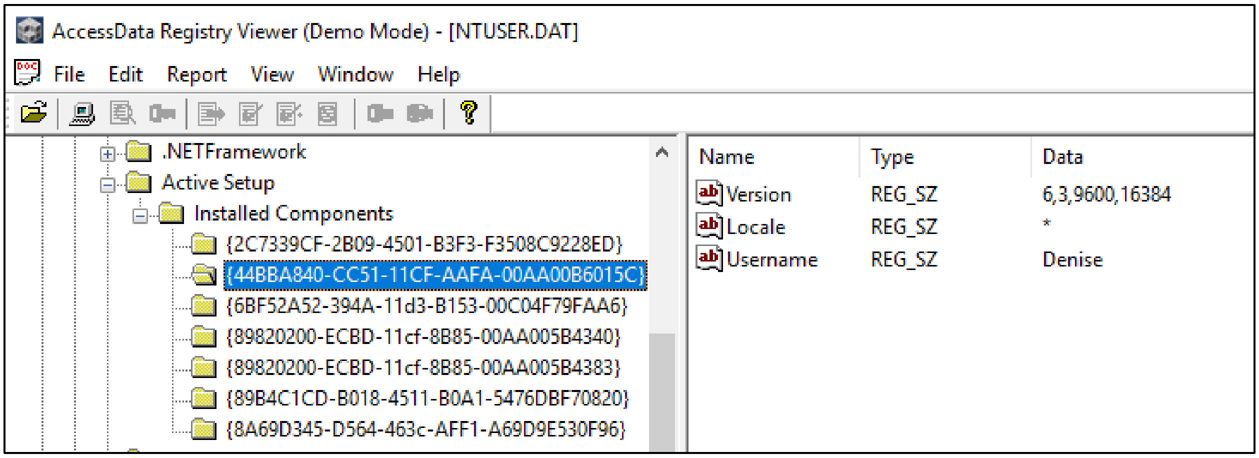
In Registry Viewer, Click File then Open and navigate to the location you exported the registry files to in step 1, select NTUSER.DAT for Denise, then click Open.

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

Iterate through the search (by pressing F3) to identify information related to the Denise user account:

1. Installed Components GUID is associated with the username

   - 44BBA840-CC51-11CF-AAFA-00AA00B6015C

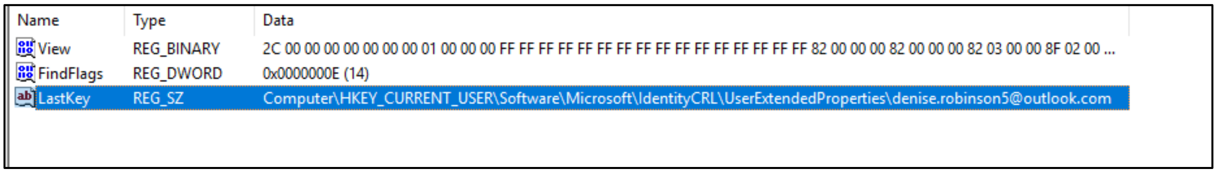


.NETFramework
Active Setup
Installed Components
{2C7339CF-2B09-4501-B3F3-F3508C9228ED}
{44BBA840-CC51-11CF-AAFA-00AA00B6015C}
{6BF52A52-394A-11d3-B153-00C04F79FAA6}
{89820200-ECBD-11cf-8B85-00AA005B4340}
{89820200-ECBD-11cf-8B85-00AA005B4383}
{89B4C1CD-B018-4511-B0A1-5476DBF70820}
{8A69D345-D564-463c-AFF1-A69D9E530F96}

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

2. Email account information can you located for the use

- Denis.robinson5@ourlook.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 82 00 00 00 82 00 00 00 82 03 00 00 8F 02 00 ...
FindFlags	REG_DWORD	0x0000000E (14)
LastKey	REG_SZ	Computer\HKEY_CURRENT_USER\Software\Microsoft\IdentityCRL\UserExtendedProperties\denise.robinson5@outlook.com

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

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

- No information is available for this user in Denis’s Ntuser.Dat
- The NTUSER.DAT file is a Windows registry hive that stores user-specific settings, preferences, and system configurations. This file contains registry data unique to an individual user account, allowing forensic investigators to analyze user behavior, software interactions, and potential security threats. Since the NTUSER.DAT file is associated with a specific user profile, it is not expected to contain data from other user accounts on the system. Each user has a separate NTUSER.DAT file, ensuring that personal settings and activity logs remain isolated within their respective profiles (Carvey, 2018; Nelson et al., 2020).

Analysis of image files

Open Autopsy and create a new case. Run through the new case wizard and when complete, click on Add Data Source.

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

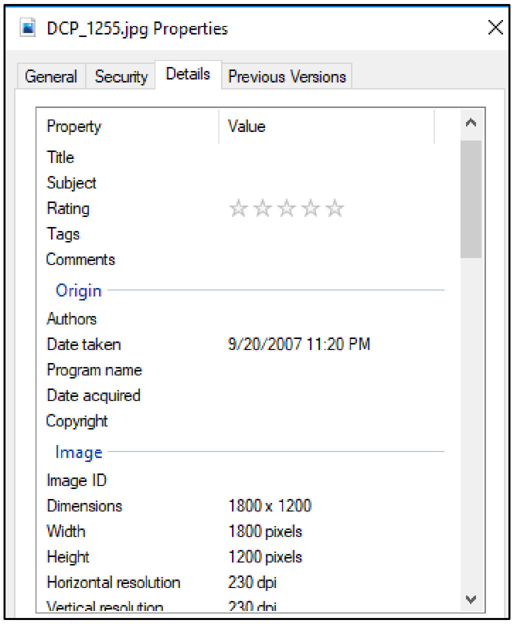
Let Autopsy parse through the image. When finished, expand the Views category and identify all images files.

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)

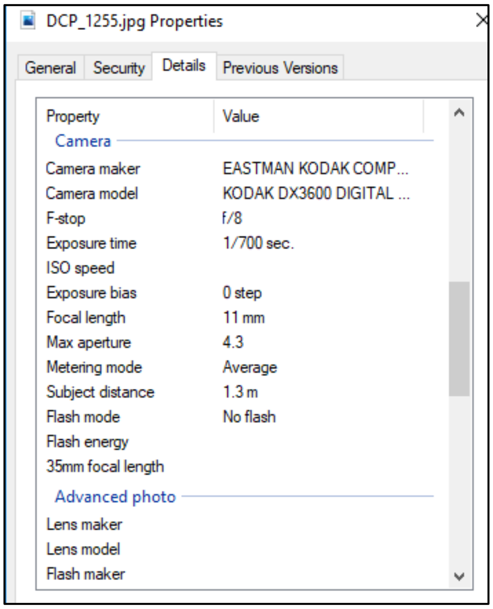
Expand the Results category - Extracted Content to look at EXIF Metadata.

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

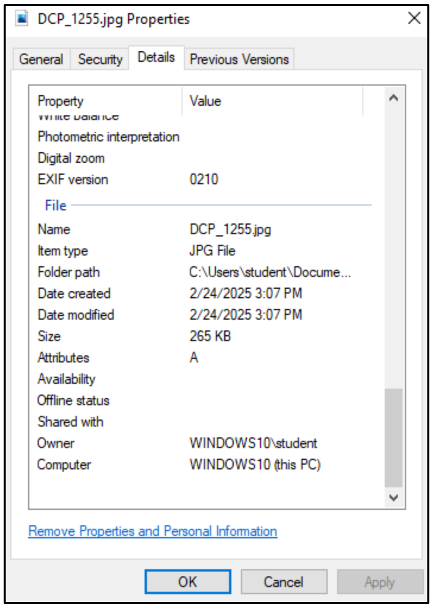
- To manually check the EXIF Metadata, browse to the folder you extracted the image files from previously and then Right Click-Properties on each file.
- Upon examining the images in Autopsy, several key metadata attributes were visible, including:
    - Date Taken: Timestamp indicating when the image was captured.
    - Image Size: Resolution and file size of the image.
    - Camera Make and Model: Details about the device used to take the image
    - Latitude & Longitude (If Available): GPS coordinates embedded in the image, revealing the exact location where it was captured.



Property	Value
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
Vertical resolution	230 dpi



Property	Value
Camera	
Camera maker	EASTMAN KODAK COMP...
Camera model	KODAK DX3600 DIGITAL ...
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	
Lens model	
Flash maker	

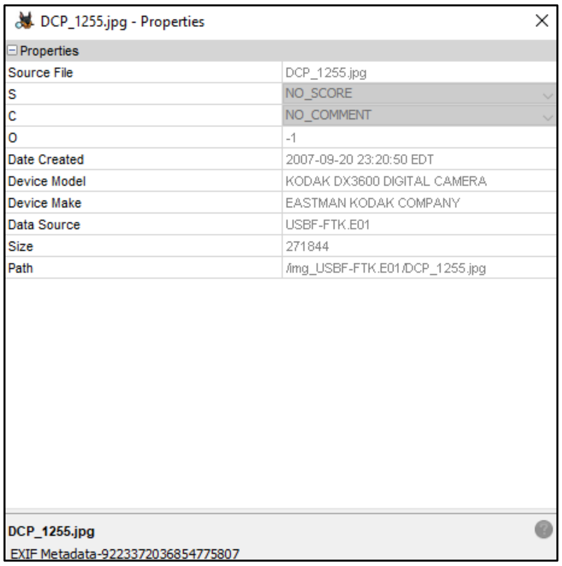


Property	Value
White balance	
Photometric interpretation	
Digital zoom	
EXIF version	0210
File	
Name	DCP_1255.jpg
Item type	JPG File
Folder path	C:\Users\student\Docume...
Date created	2/24/2025 3:07 PM
Date modified	2/24/2025 3:07 PM
Size	265 KB
Attributes	A
Availability	
Offline status	
Shared with	
Owner	WINDOWS10\student
Computer	WINDOWS10 (this PC)

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

- Image detail information such as dimensions
- Focal Length & Aperture Settings: Indicates the zoom and exposure settings of the camera.

- Flash Usage: Specifies whether the flash was fired or disabled when capturing the image.

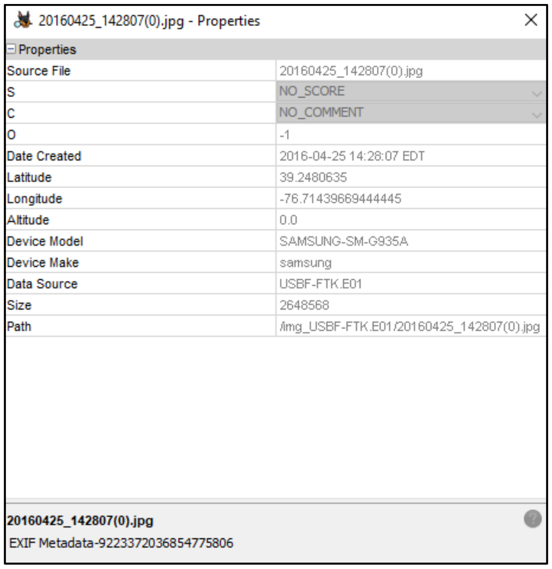


DCP_1255.jpg - Properties

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	USBF-FTK.E01
Size	271844
Path	/img_USBF-FTK.E01/DCP_1255.jpg

DCP_1255.jpg

EXIF Metadata-9223372036854775807



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	USBF-FTK.E01
Size	2648568
Path	/img_USBF-FTK.E01/20160425_142807(0).jpg

20160425_142807(0).jpg

EXIF Metadata-9223372036854775806

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

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

- Precise GPS Coordinates: Some images contained detailed latitude & longitude values, which were mapped to an exact street address or location.
- Device Serial Number: In some cases, forensic tools display a unique device ID, linking the image to a specific camera or smartphone.
- Modification History: If an image was altered, tools detected inconsistencies in compression levels (ELA - Error Level Analysis), indicating potential forgeries or digital manipulations

4. Would you ever do this in a real-world case? Why or why not.

In a real-world forensic investigation, uploading images to online forensic tools should be approached with caution. Key reasons include:

- Uploading forensic evidence to external websites can compromise data integrity and violate chain of custody procedures, making the evidence inadmissible in court (Casey, 2011).
- Online tools may modify image metadata, affecting forensic authenticity.
- If an image is related to a criminal investigation, uploading it to a public tool could expose sensitive details.

Forensic investigators should use offline forensic tools like ExifTool, FTK Imager, or EnCase to extract metadata securely and preserve forensic integrity.

Conclusion

The absence of GPS, camera type, and device metadata in an image can be attributed to social media stripping, image editing, privacy settings, file conversion, compression, or metadata removal tools. Understanding these limitations is crucial in forensic investigations, as missing metadata can make it harder to determine image authenticity, origin, and modifications. In such cases, forensic analysts must utilize alternative techniques, such as file analysis, error level analysis, and timestamp verification, to extract meaningful evidence

The forensic analysis of image files in Autopsy revealed valuable metadata, including timestamps, camera details, and GPS locations, which are essential for digital investigations. Additional metadata, such as modification history and focal length, was retrieved using manual examination and online tools. However, in real-world forensic cases, investigators must ensure data security by avoiding online tools that could compromise the confidentiality and admissibility of evidence. By following proper forensic procedures, metadata analysis can provide critical insights into digital images, user behavior, and potential criminal activities.

Glossary

GUID (Globally Unique Identifier)

A Globally Unique Identifier (GUID) is a 128-bit unique reference number used to identify software components, system objects, and registry entries in Windows operating systems. GUIDs are typically displayed in a standardized hexadecimal

Windows Registry

The Windows Registry is a hierarchical database that stores system settings, user preferences, and application configurations. It contains valuable forensic artifacts such as recently accessed files, installed programs, and USB device history, making it an important resource in forensic investigations (Carvey, 2018).

Metadata

Metadata refers to embedded information within digital files, including timestamps, file authorship, GPS location (for images), and editing history. Forensic investigators analyze metadata to determine file authenticity, modification history, and potential tampering (Nelson et al., 2020).

System 32

System32 is a critical directory in Microsoft Windows operating systems that contains essential system files, drivers, and executable programs necessary for the operating system to function properly (Solomon & Russinovich, 2022).

References

Adobe Systems. (2018). XMP (Extensible Metadata Platform). Retrieved from https://www.adobe.com/products/xmp.html

Carvey, H. (2018). *Windows forensic analysis toolkit: Advanced analysis techniques for Windows 10* (4th ed.). Syngress.

Casey, E. (2011). Digital evidence and computer crime: *Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Farid, H. (2009). A survey of image forgery detection. IEEE Signal Processing Magazine, 26(2), 16-25. https://doi.org/10.1109/MSP.2008.931079

McHugh, S. (2013). *The IPTC metadata standard and its role in digital asset management. Journal of Digital Media Management*, 2(4), 311-322.

Nelson, B., Phillips, A., & Steuart, C. (2020). *Guide to computer forensics and investigations* (6th ed.). Cengage Learning.

Solomon, D. A., & Russinovich, M. E. (2022). *Windows internals* (7th ed.). Microsoft Press.