UMGC Lab

Name: Pelumi Johnson
Date: January 14, 2026
Course: CMIT 436 | Cloud Security
Institution: University of Maryland Global Campus (UMGC)
Lab Title: Displaying Metadata Information

Objective

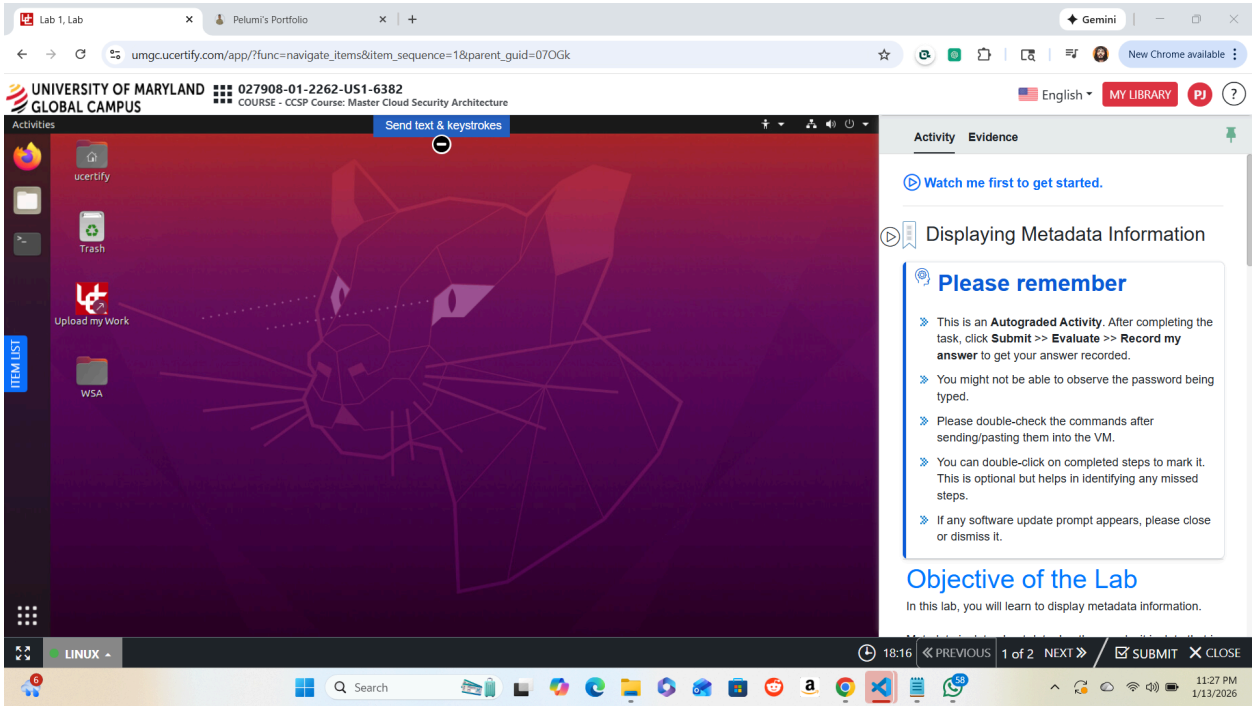
The objective of this lab was to learn how to display, analyze, and modify metadata information stored within image files using ExifTool. This lab focused on understanding file metadata, installing required tools, and verifying metadata changes through command-line analysis.

Tools & Environment Used

- uCertify Virtual Lab (Linux Environment)
- Ubuntu Linux
- Terminal
- ExifTool
- Image file: ubuntu-default-greyscale-wallpaper.png

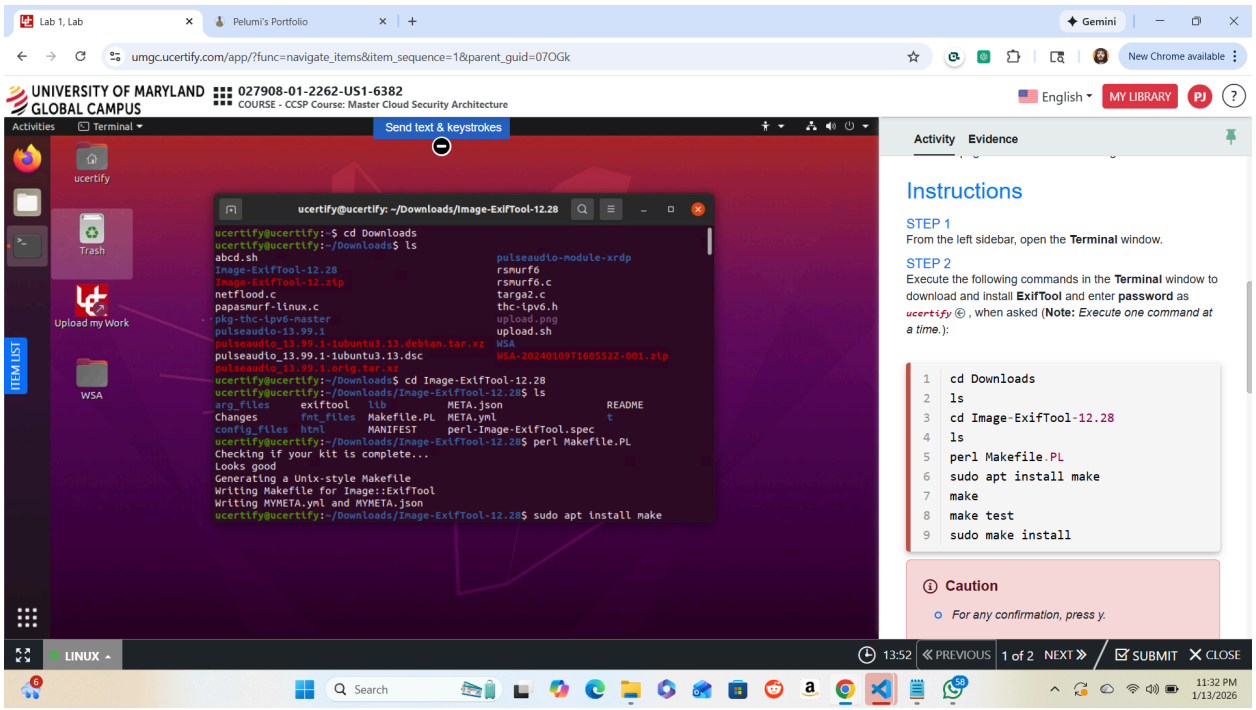
Lab Overview

Metadata is hidden information embedded within files that describes attributes such as file type, size, timestamps, and creation details. In this lab, ExifTool was used to read and modify metadata within an image file, demonstrating how metadata can reveal valuable forensic and security-related information.



Step 1: Opening the Terminal

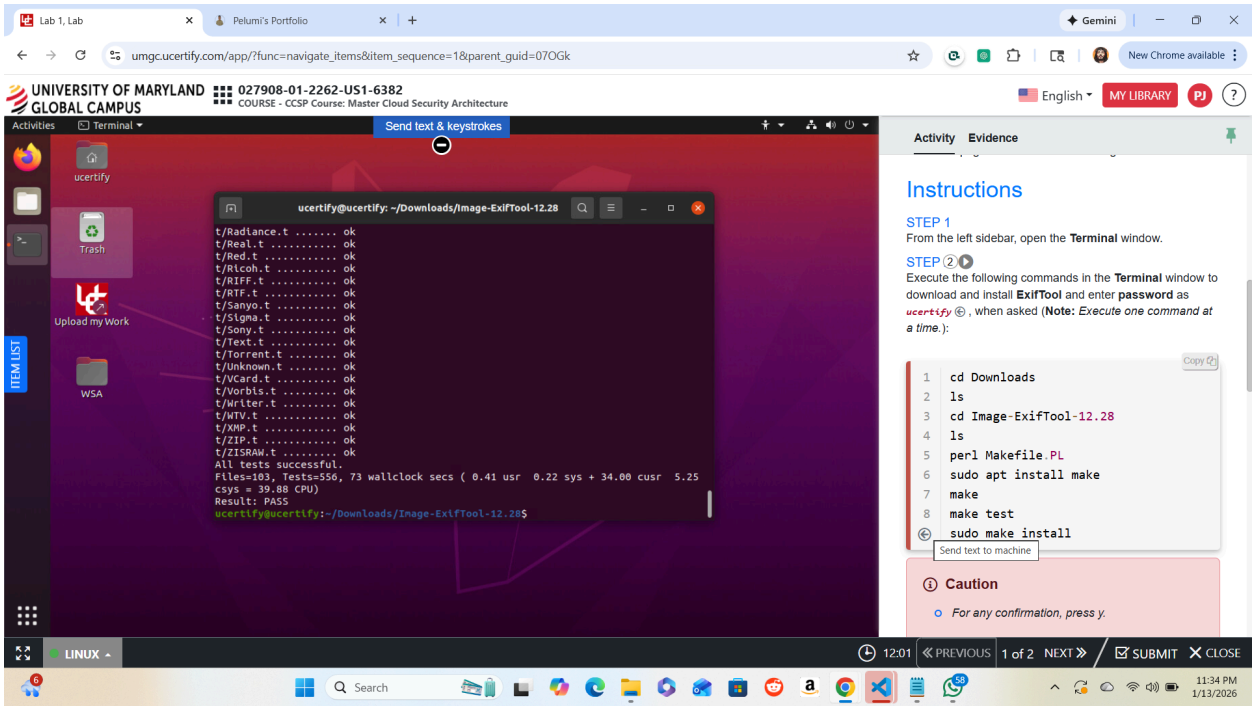
The Terminal window was opened from the left sidebar of the Ubuntu desktop. The terminal was used to execute all required commands for downloading, installing, and running ExifTool.



Step 2: Installing ExifTool

Using the terminal, the Downloads directory was accessed and the ExifTool package was extracted. The following steps were completed to install ExifTool:

- Navigated to the Image-ExifTool directory
- Generated the Makefile using Perl
- Installed required dependencies
- Compiled and installed ExifTool
- Verified installation completion

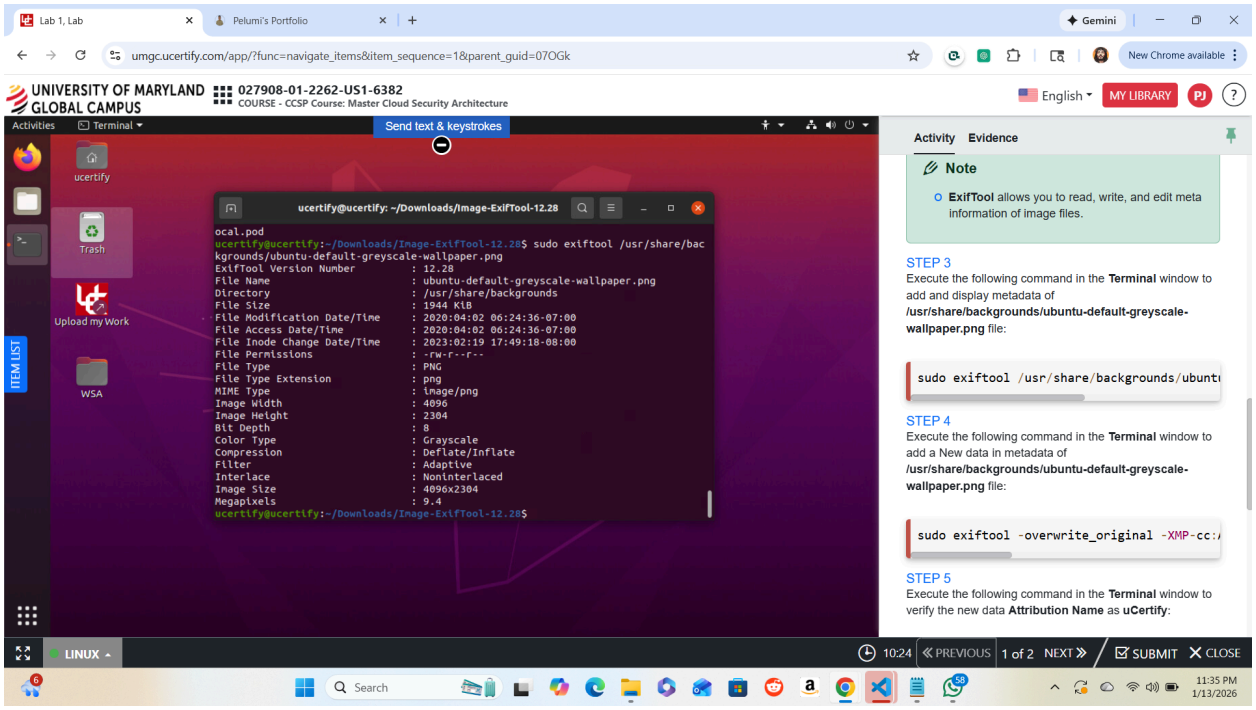


Step 3: Displaying Metadata

ExifTool was executed against the file located at:
/usr/share/backgrounds/ubuntu-default-greyscale-wallpaper.png

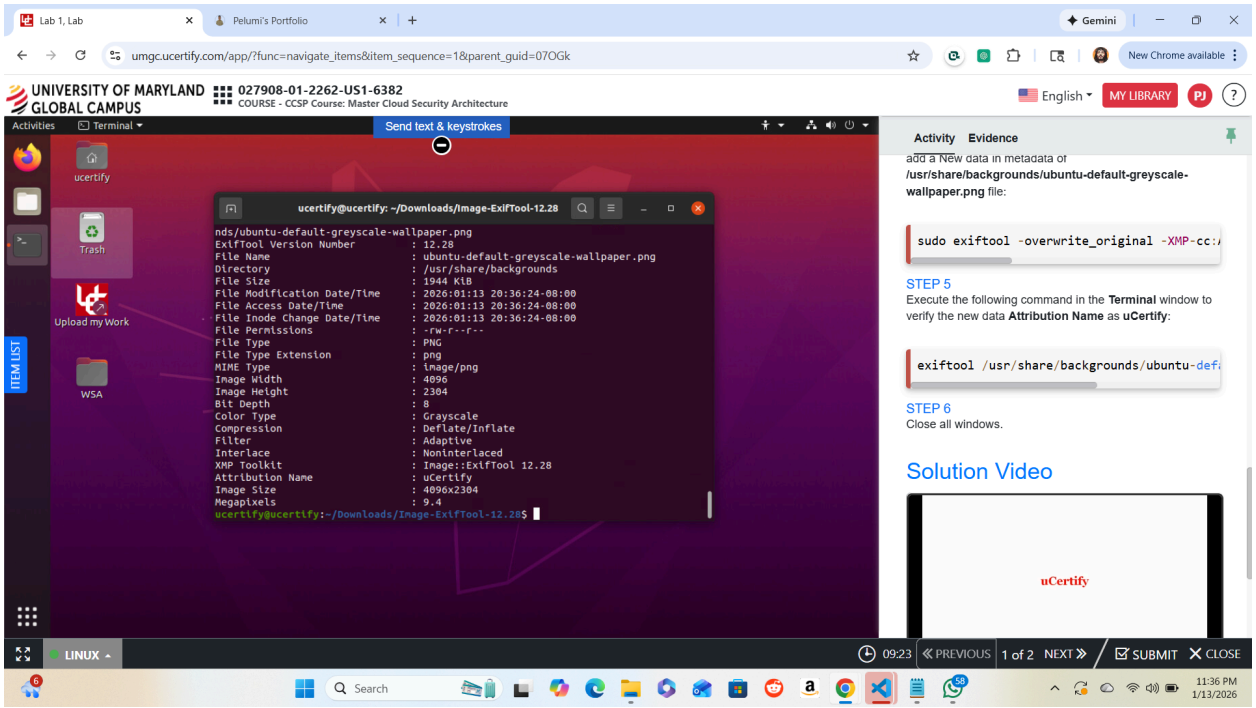
The output displayed detailed metadata including:

- File name and directory
- File size and permissions
- Image dimensions and format
- Modification and access timestamps



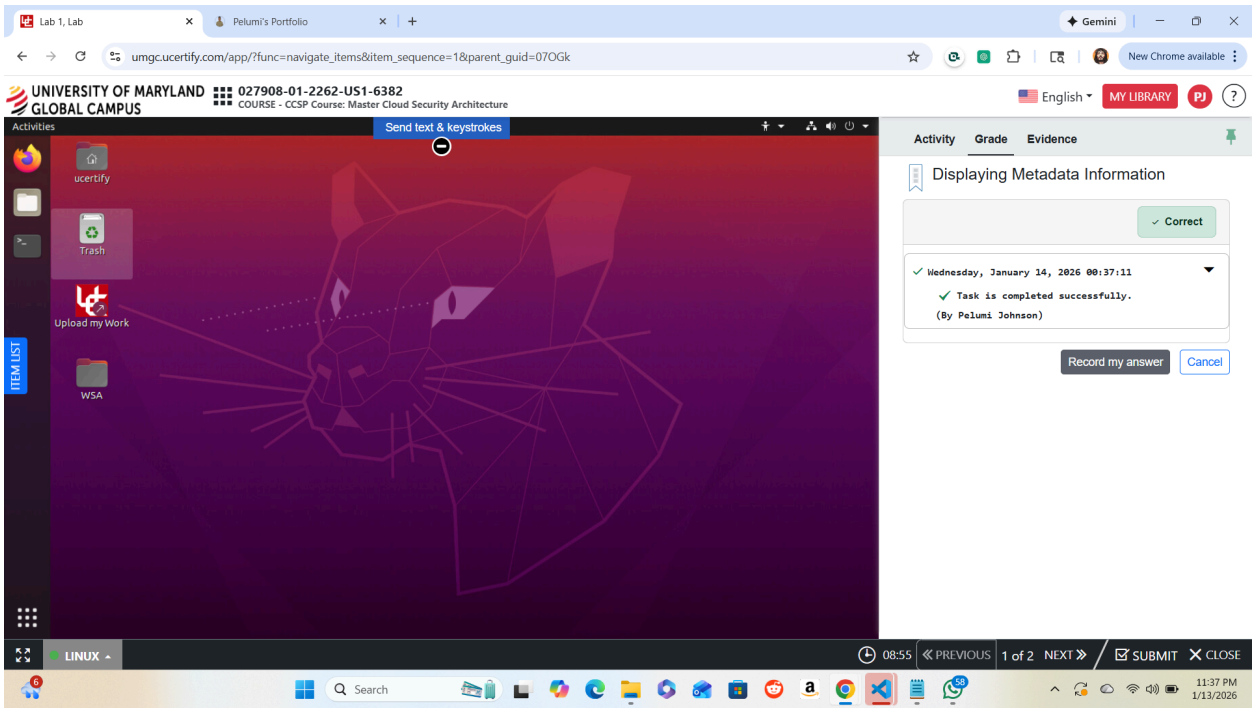
Step 4: Adding Metadata

A new metadata attribute was added to the image file using ExifTool. The attribution name was set to identify uCertify as the source. The original file was overwritten as instructed.



Step 5: Verifying Metadata Changes

ExifTool was run again on the same image file to confirm that the new metadata attribute was successfully added. The output verified that the attribution name was present and correctly recorded.



Results

- ExifTool was successfully installed and executed
- Image metadata was displayed without errors
- A new metadata attribute was added successfully
- Metadata changes were verified using ExifTool

Conclusion

This lab demonstrated how metadata can be accessed and modified using command-line tools. By working with ExifTool, I gained hands-on experience analyzing file metadata, which is an important skill in cloud security, digital forensics, and incident investigations. Understanding metadata helps security professionals identify file origins, changes, and potential indicators of compromise.

Key Takeaways

- Metadata provides hidden but valuable information about files
- ExifTool is a powerful utility for reading and editing metadata
- Command-line analysis is essential for forensic investigations

- Metadata analysis supports cloud security and incident response workflows