Stolen Artwork Case Report

Christian Lam

12/09/2022

CECS302: Intro to Computer Forensics

Table of Contents

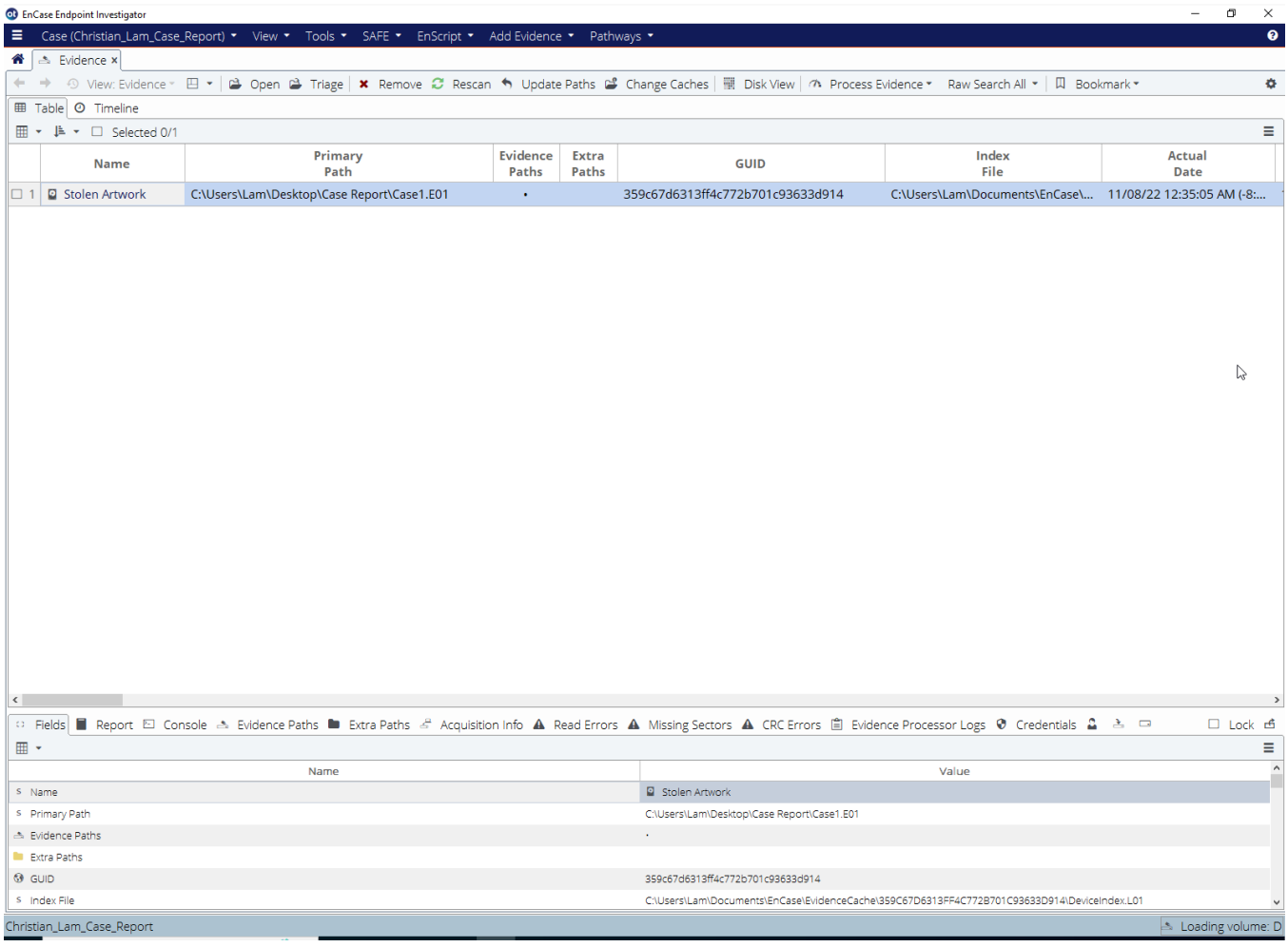
Executive Summary

A student by the name of Ron Atherton has been accused by his Professor Megan Dove of stealing very valuable unique paintings from her computer system. Ms. Dove reported the incident to the IT staff that she had seen possible images of the unique artwork on Mr. Atherton's computer while she was walking around the room during class. Ms. Dove is an upstanding member of the college/community and her word is taken with high regard and seriousness, therefore Mr. Atherton's computer was confiscated along with removable media by the IT Staff of the college/community to be examined and conduct and thorough investigation.

My role in this investigation case is to examine Mr. Atherton's computer system and determine whether the unique images that belong to Ms.Dove are present. I have been tasked to find where Mr.Atherton has hidden the images and whether or not the images were distributed. I have been given access to Mr.Atherton's computer hard drive along with other removable media. The IT department has asked me to perform a thorough analysis of the hard drive and removable media. The analysis will be performed through the software EnCase since the program allows computer forensic experts and me to analyze the data without any modification or jeopardizing it. I created a copy of the hard drive image to EnCase to reduce the risk of any modifications by accident. With the use of EnCase, I can gather evidence on proving that Mr.Atherton has Ms.Dove's unique artwork on his devices.

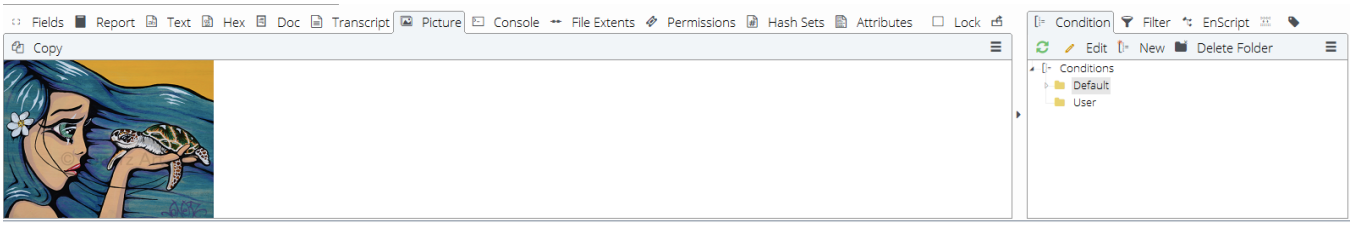
Evidence

For this case, I was given Mr.Atherton's computer hard drive. The hard drive was divided into four image files (Case1.E01, Case1.E02, Case2.E03, Case1.E04). Using the software EnCase I opened a new case and created new evidence using the hard drive for Case1. Then the software processed the drive and displayed a new case title "Stolen Artwork".

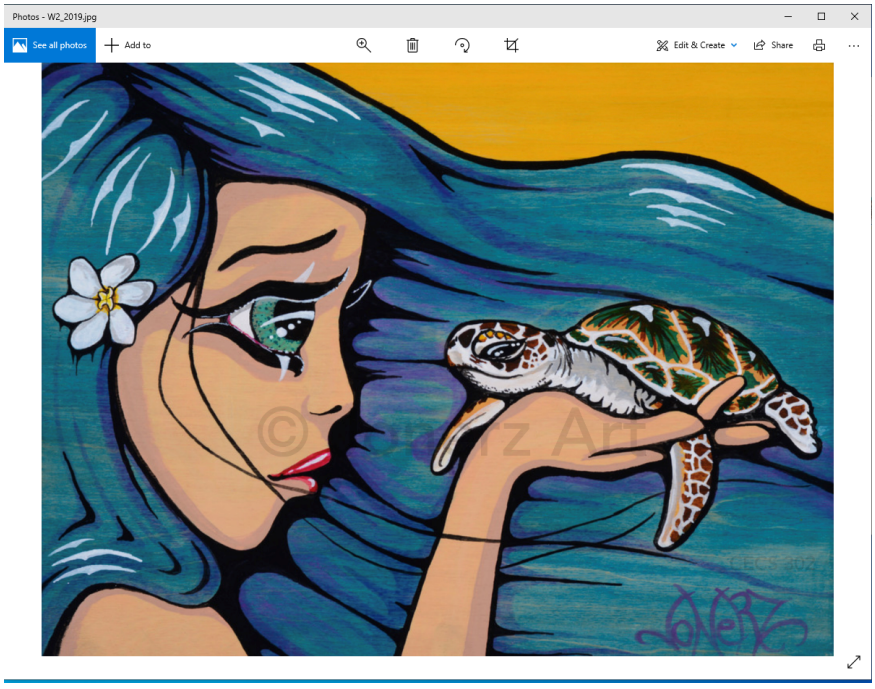


Relevant Findings

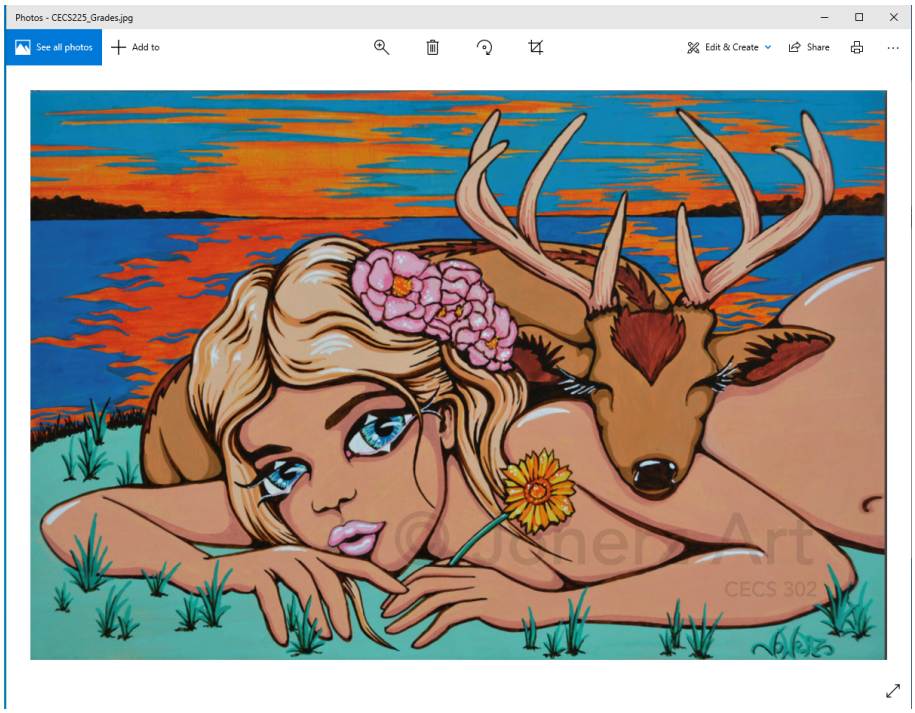
To find some of the artwork on the drive. I examined the D:\ drive and navigated to the user folder labeled Thales. I looked under the folders where most people would store their files and analyzed each file. Since the artwork is an image then I know that if the file I selected displayed the artwork then that file was hiding the stolen artwork. With the help of EnCase by selecting a file, I can select the “Picture” tab and see if the image displays the stolen artwork.



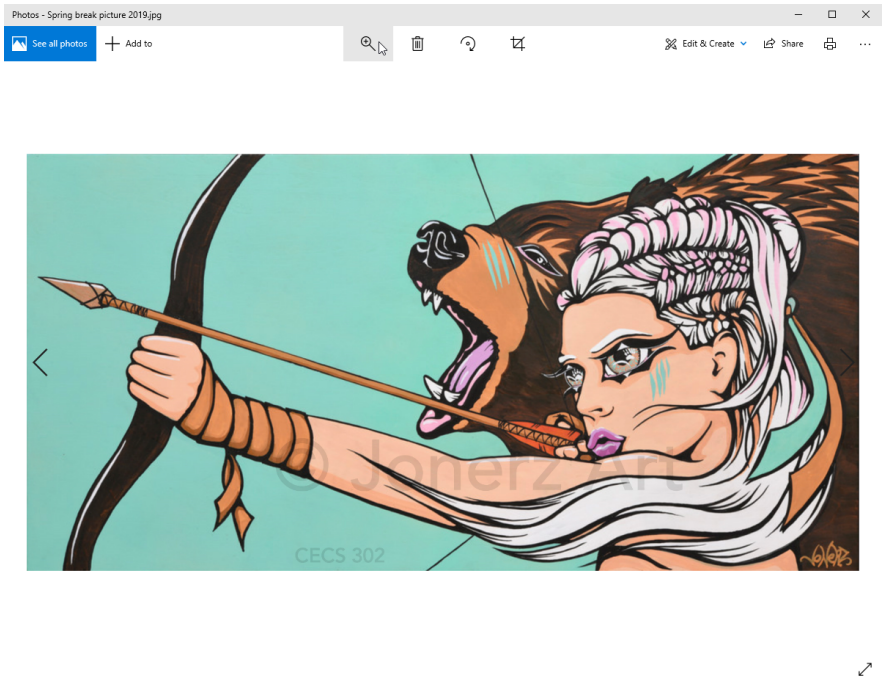
By using this method I was able to find some of the stolen artwork in the desktop, documents, and pictures folder.



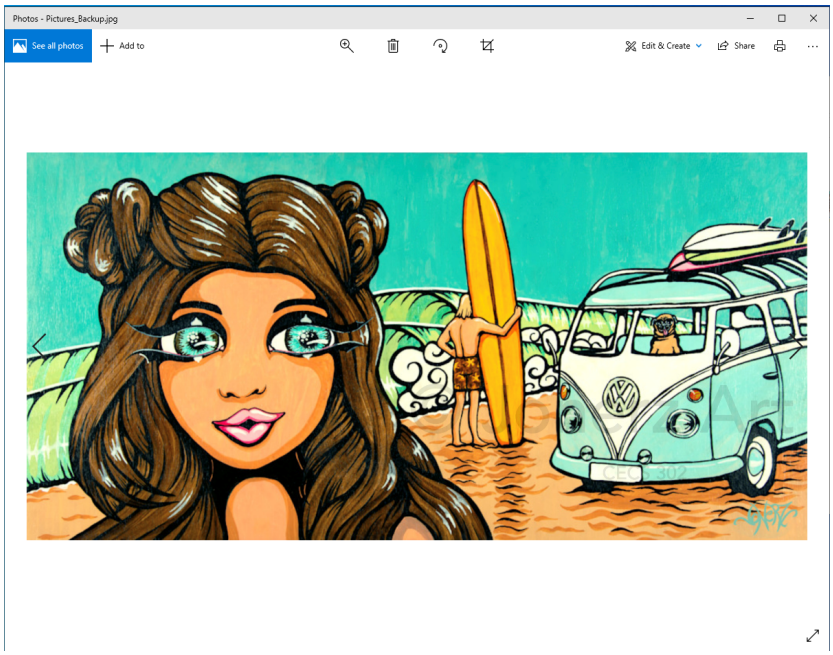
File Path: D:\Users\Thales\Documents\W2_2019.pdf



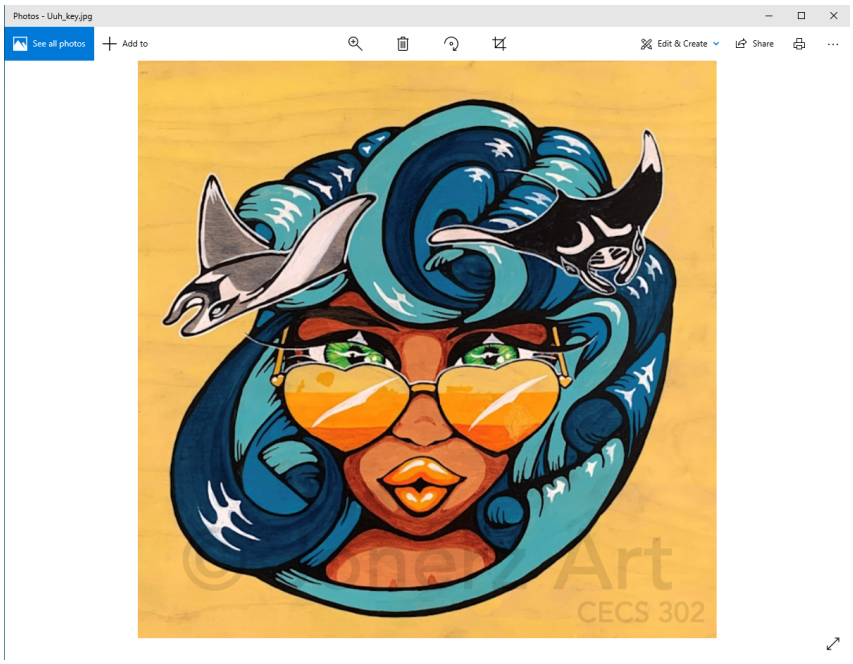
File Path: D:\Users\Thales\Documents\CECS225_Grades.xlsx



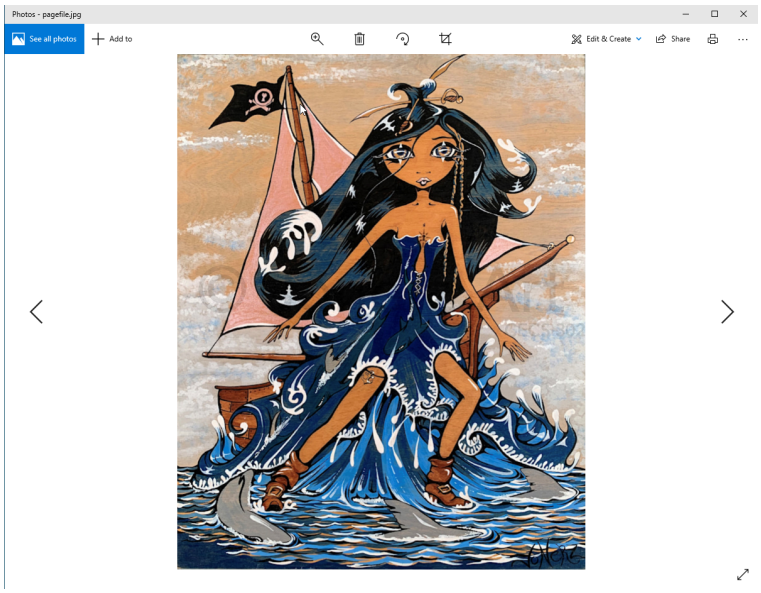
File Path: D:\Users\Thales\Pictures\Spring break picture.7z



File Path: D:\Users\Thales\Pictures\Pictures_Backup.7z

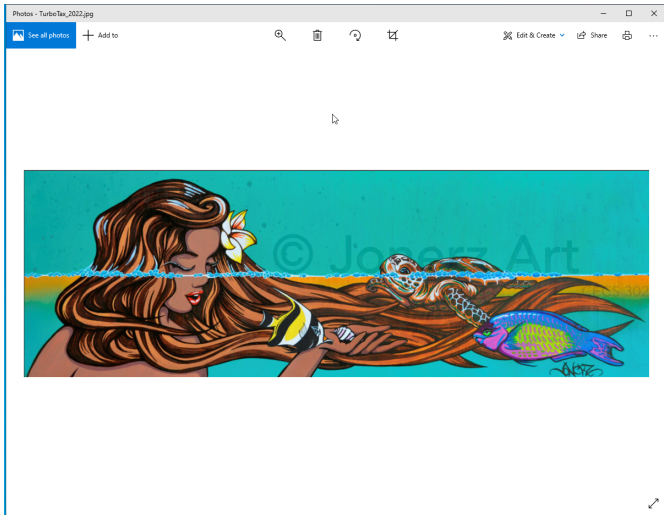


File Path: D:\Users\Thales\Desktop\Keys\Uuh_key.pfx

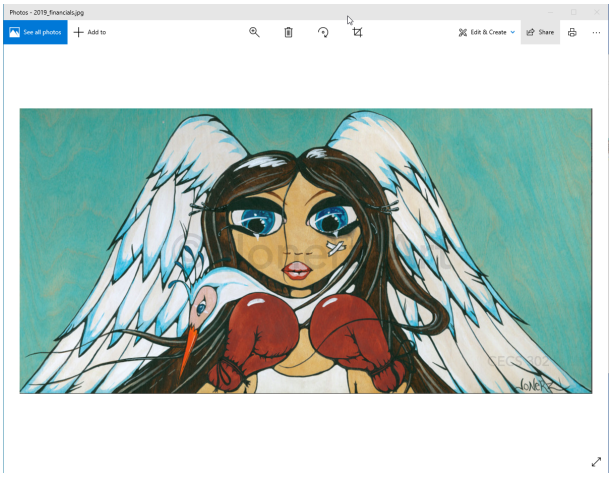


File Path: D:\pagefile.sys

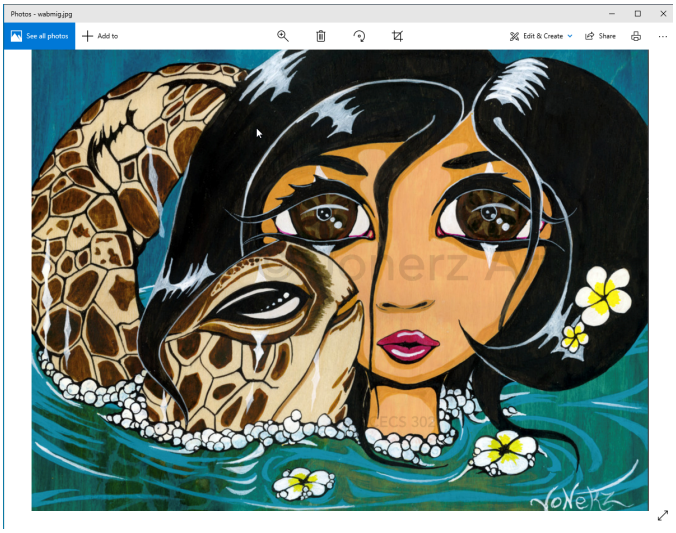
The method I conducted to obtain the following images, was to check the files in the locations where users store their files such as desktop, mail, and documents. In these folders, I checked every file and analyzed the hex of the file. If the file contained the JPG signature but is not in the correct file signature location. This gave me a suspicion that the file could be a JPG of the stolen artwork. Once I located a file containing a JPG signature, I copied the file to my desktop and used a hex editor to remove the excess values to correct the file signature to start with the JPG signature.



File Path: D:\Users\Thales\Documents\TurboTax_2022.pdf

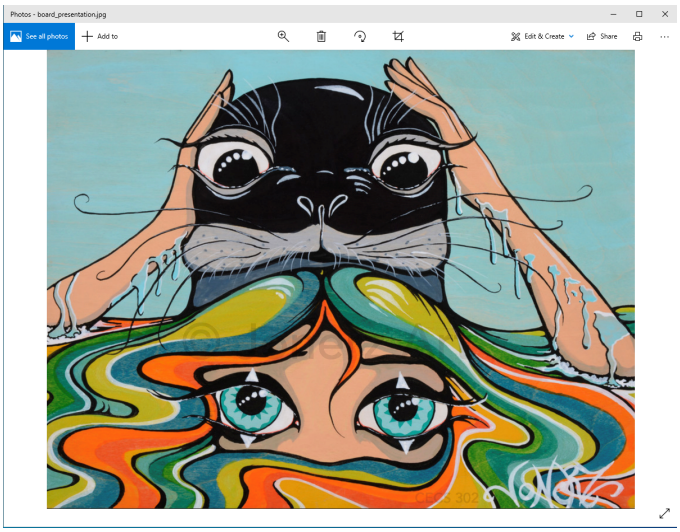


File Path: D:\Users\Thales\Documents\2019_financials.xlsx

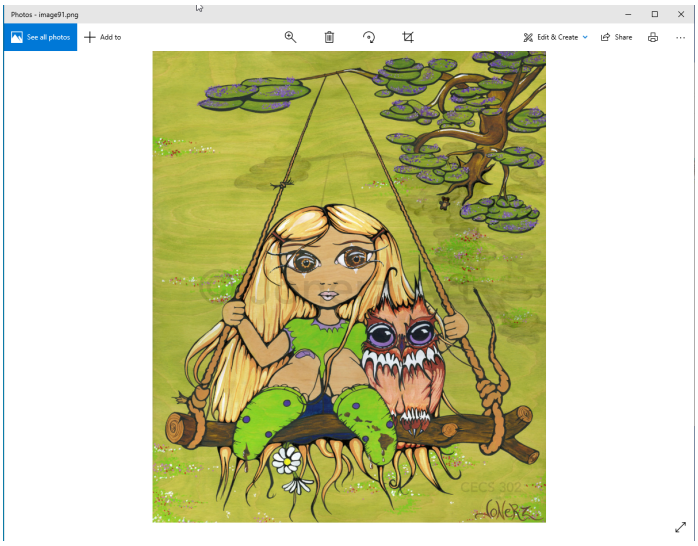


File Path: D:\Program Files\Windows Mail\wabmig.exe

The next method I conducted was to take a look at the PowerPoint and quiz files since the image could be stored on those documents. I copied the file over and extracted the file to obtain an image folder for each quiz and PowerPoint to find the image of the stolen artwork. For one of the quizzes, there was an image that could not be viewed, so I took the file and view the hex to find that the JPG signature was incorrectly placed. I fixed the file signature to obtain the image of the stolen artwork on the quiz file.



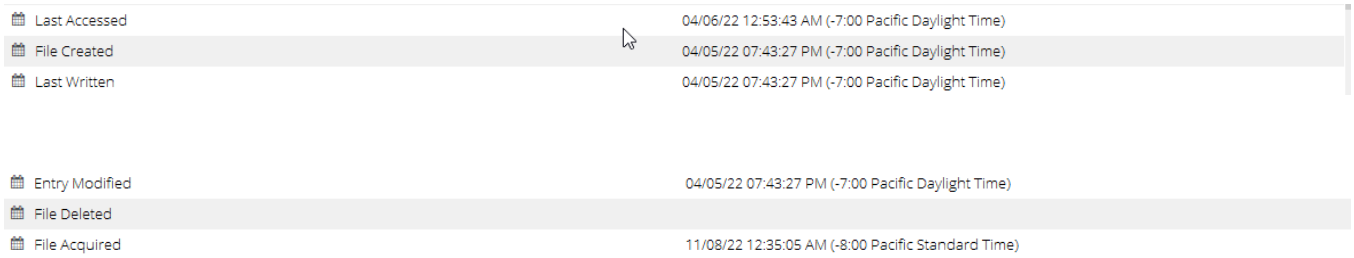
File Path: D:\Users\Thales\Documents\board_presentation.pptx



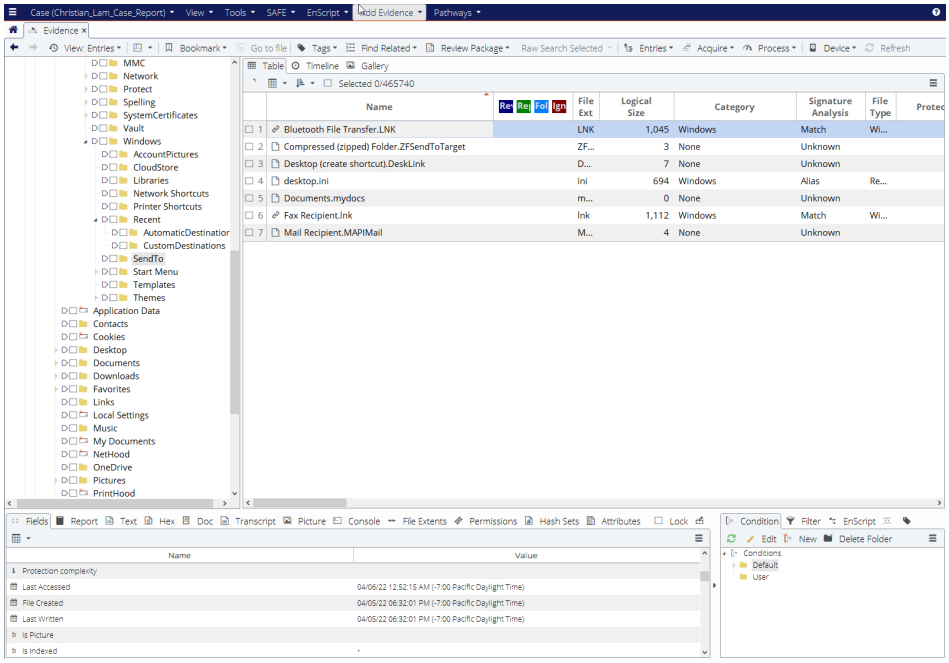
File Path: D:\Users\Thales\Documents\Quizzes\Quiz4.docx

Investigative Leads

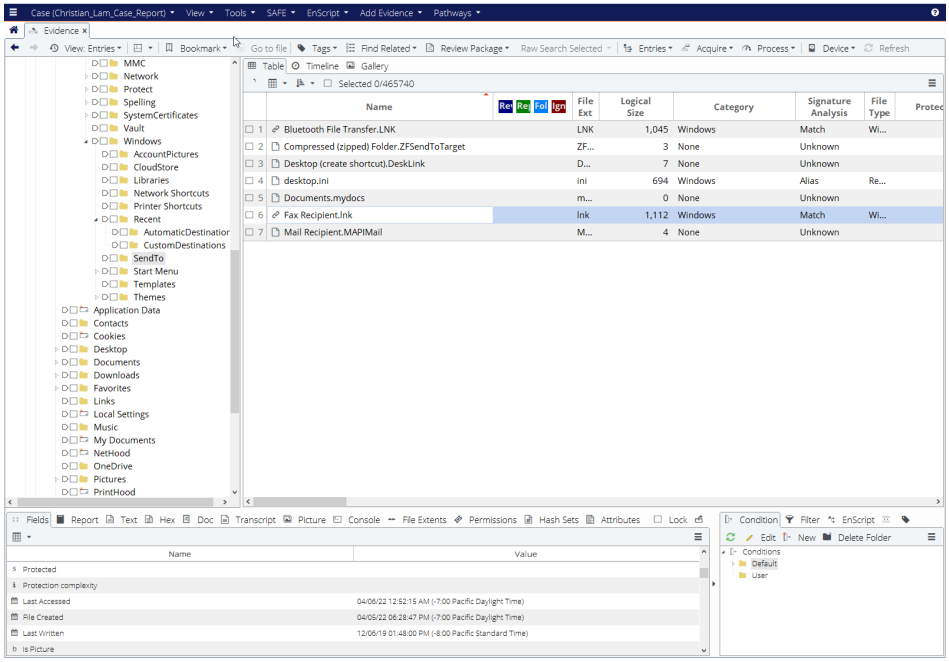
While analyzing Mr.Atherton's hard drive, in this case, I found some possible cases in which the images had a connection through fax or Bluetooth. By locating the LNK files for the corresponding files that contained the images of the stolen artwork I analyzed the relevant timestamps for the files in order to compare with the timestamps I found for files under the methods of fax and Bluetooth



Relevant Timestamps for each Image File



Timestamps for Bluetooth LNK File



Timestamps for Fax LNK File

Recommendations

Ms.Dove's unique artwork was found located on Mr.Atherton's hard drive.

In Mr. Atherton's hard drive, there was a connection with Bluetooth. There is a possibility that the images could have been stolen through a Bluetooth device. There is a possibility that when Ms.Dove was walking around the room or out of the room Mr. Atherton could have used a Bluetooth device to steal the images. It is recommended for Ms. Dove to never leave her computer unattended. I would advise that if you have to step away from your laptop then simply close the laptop so that it locks the laptop. If it was a desktop then simply sign out of the computer so that nobody can access the device easily.

The college/community should definitely improve their security awareness knowledge so that Ms.Dove understands the methods that can be used to steal her artwork. Informing both the faculty and the students can teach Ms.Dove in this case how to secure her personal data and prevent data breaches. In the case of Mr.Atherton, with the knowledge of security awareness, he can understand the serious consequences that he will be faced

Conclusion

While analyzing Mr. Atherton's computer hard drive it was obvious that his computer contained the unique artwork belonging to Ms. Dove. By using Encase in this analysis, it was easier to locate the images that were stolen. It was discovered that on the hard drives some of the files were hidden using different file extensions. A couple of other images were found using different extensions but misplaced the file signature of the image file to hide its identity of it. Some images Mr.Atherton had decided to hide within PowerPoint and quiz documents. The timestamps of the images are also similar to files that belong to Bluetooth and Fax. This could be an indication that a connection using Bluetooth and Fax was involved during the incident.

References

Duttke, J. (n.d.). *Browser-based online and offline hex editing*. HexEd.it. Retrieved December 9, 2022, from https://hexed.it/

"7-Zip." *Download*, https://www.7-zip.org/download.html.

OpenText encase forensic. OpenText. (n.d.). Retrieved December 9, 2022, from https://www.opentext.com/products/encase-forensic

Appendix

JPG - A file extension for images/photos

LNK - File extension for a shortcut that shows the original file path

EnCase - A executable software that allows evidence to be recovered and analyzed from hard drives

File Extension - The ending of a file name determines the type and format of a file

File Signature - The data values of a file that identifies the contents within the file

Hex Values - Values within the value that are calculated by Hexadecimal that corresponds with the data and information within the file.

Hexed.it - A free online webrowser application that can edit hex values of a specific file

Bluetooth - A wireless technology that uses a radio frequency to share data over a short distance, eliminating the need for wires

Fax - An image of a document made by electronic scanning and transmitted as data by telecommunication links.