11/30/2023

Case Summary

An art museum in New York City has discovered irregularities in their financial records. The audit revealed discrepancies in bank statements, unexplained approvals, missing funds . The internal audit team compiled a report on the fraud. This report was then presented to the museum's Board of Directors, who, upon reviewing it, reported the matter to the local police department. Following an initial investigation, the police department has raised suspicions that an employee within the museum's finance department may be linked to those activities , with proper warranty they have seized the employee's laptop suspecting its involvement. In line with this, they have requested me to examine the seized laptop to uncover any information related to its usage.

Forensic Acquisition & Exam Preparation

- The environment used for the examination is Dell Inspiron 14 , 12th Gen Intel Core i-7 processor, Windows 11, 64-bit OS with 16.0 GB RAM(15.7 GB Usable).
- The image FinancialFraud.E01 and its files are required for the examination and are saved in the folder Research project.
- The FTK Imager 4.7.1.2 is downloaded from canvas. After downloading , the tool is opened and using the green '+' icon , the image FinancialFraud.E01 is loaded by choosing the image file option. The Properties such as geometry ,hash are observed.
- After right clicking the image , I selected the verify drive/image option and verified hash is shown.
- The verified hash of FinancialFraud.E01 image is **65d52d66f22adbfb13e989da76bccc81.**

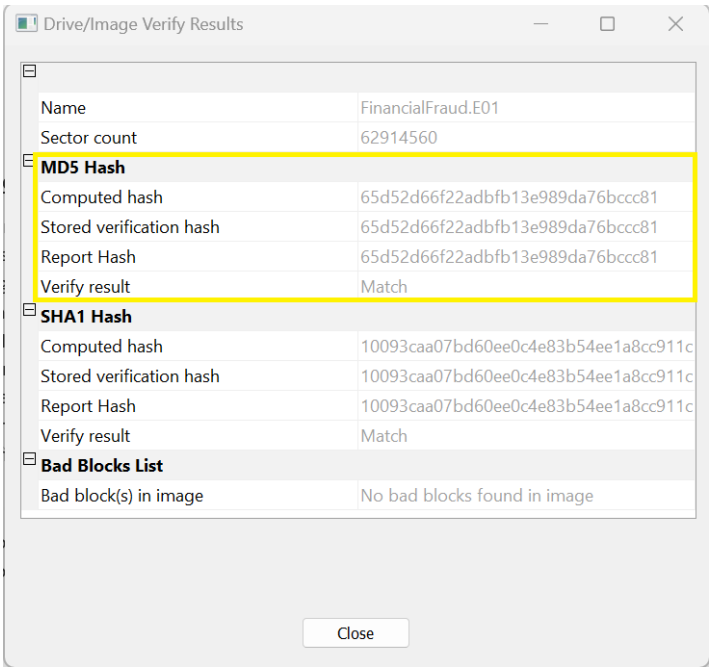

Figure 1 Hash Verification of the image FinancialFraud.E01

- I have downloaded Registry Explorer v1.1.0.6 from Canvas , unzipped, and installed it .
- The Autopsy 4.21.0 tool is downloaded and the image FinancialFraud.E01 is loaded into it for further analysis.

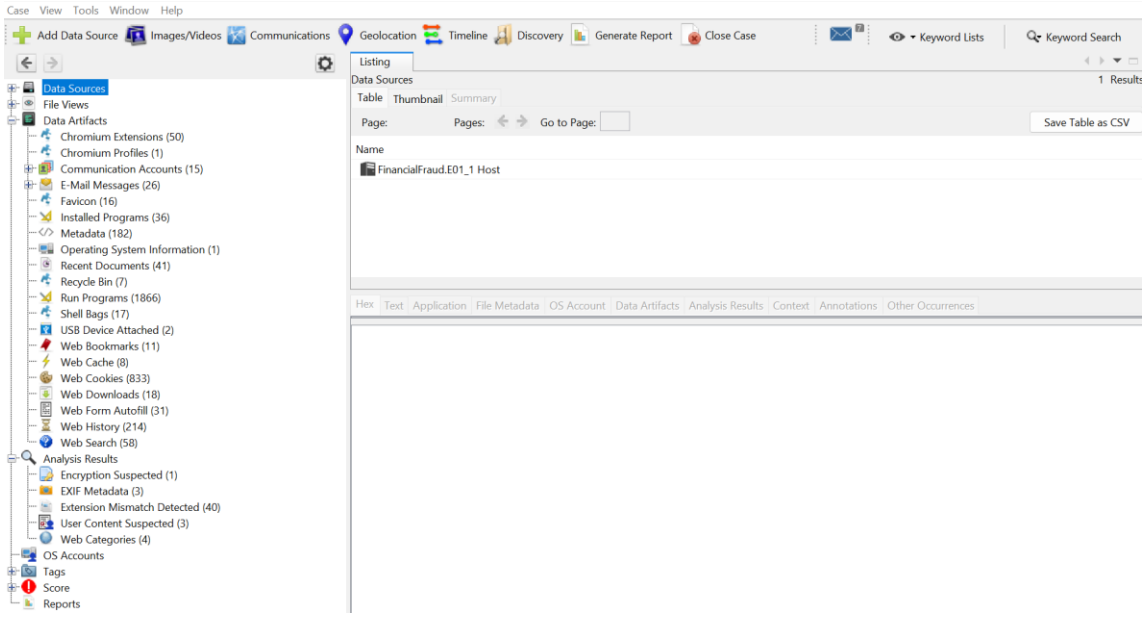

Figure 2 Autopsy File Path

Findings and Report

1) Who is the owner of the computer?

I have found the owner of the computer by navigating to data artifacts >Operating system information. The owner of the computer is found to be linkmate01@outlook.com.

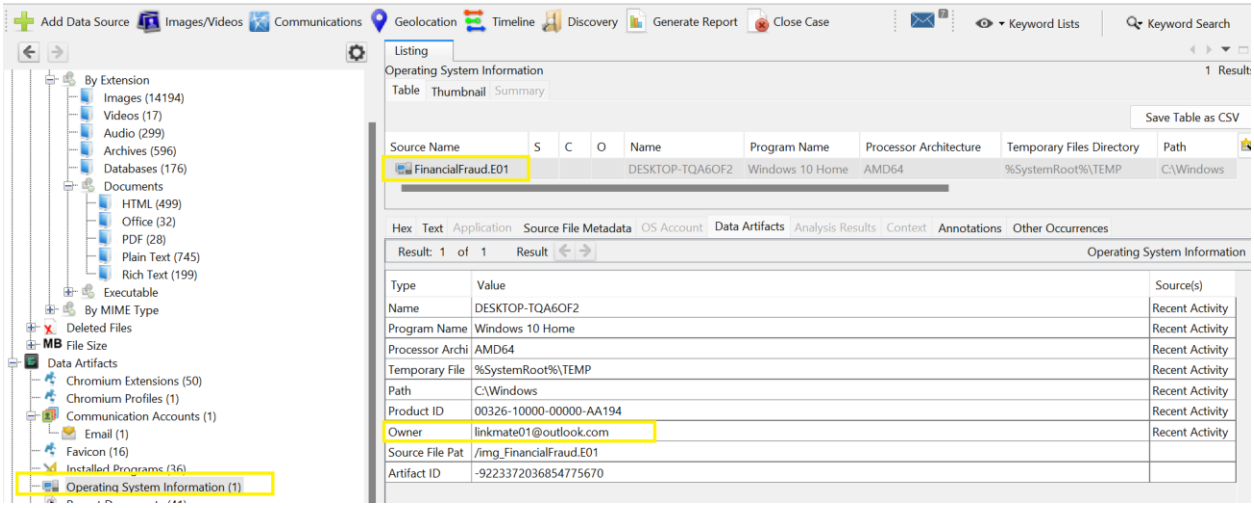

Figure 3 Owner of the computer

2) What version OS was running on the computer in use?

To obtain this data, the Software file is retrieved from the autopsy process by following the path: vol_3 > windows > system32 > config. Once located, the software file is extracted. Subsequently, I loaded it into Registry Explorer and navigated through root > windows_NT > current version, where I identified the operating system version as Windows 10 Home.

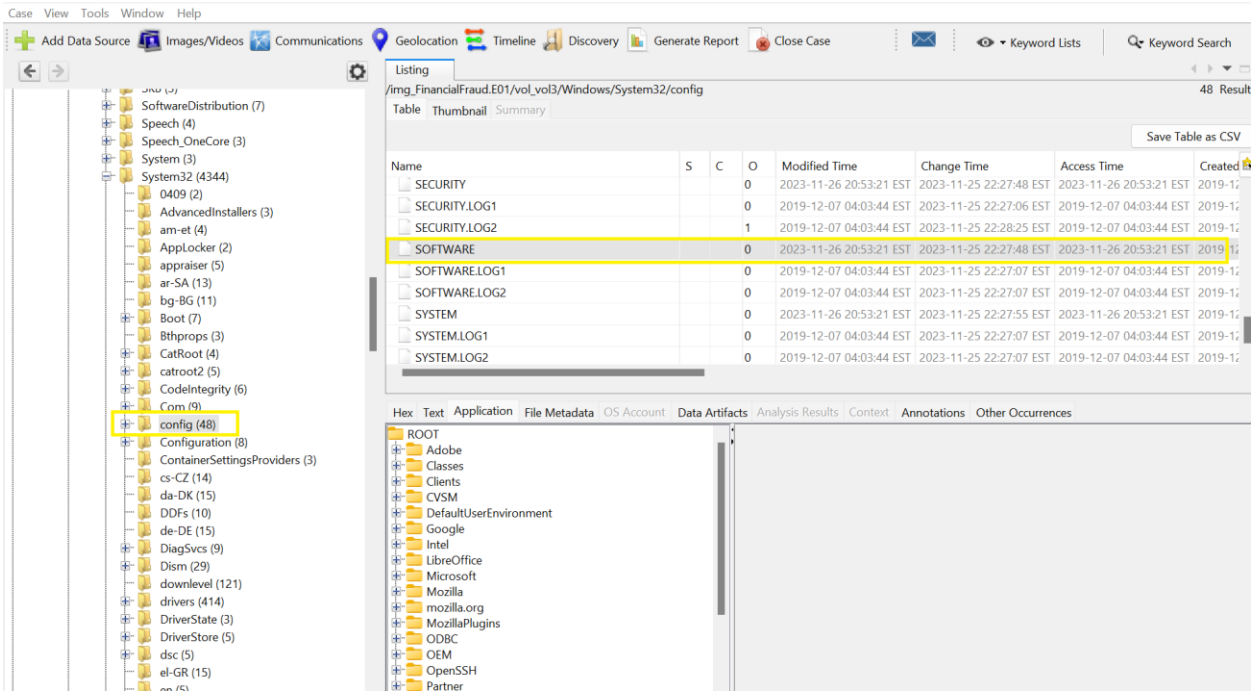

Figure 4 The Software file

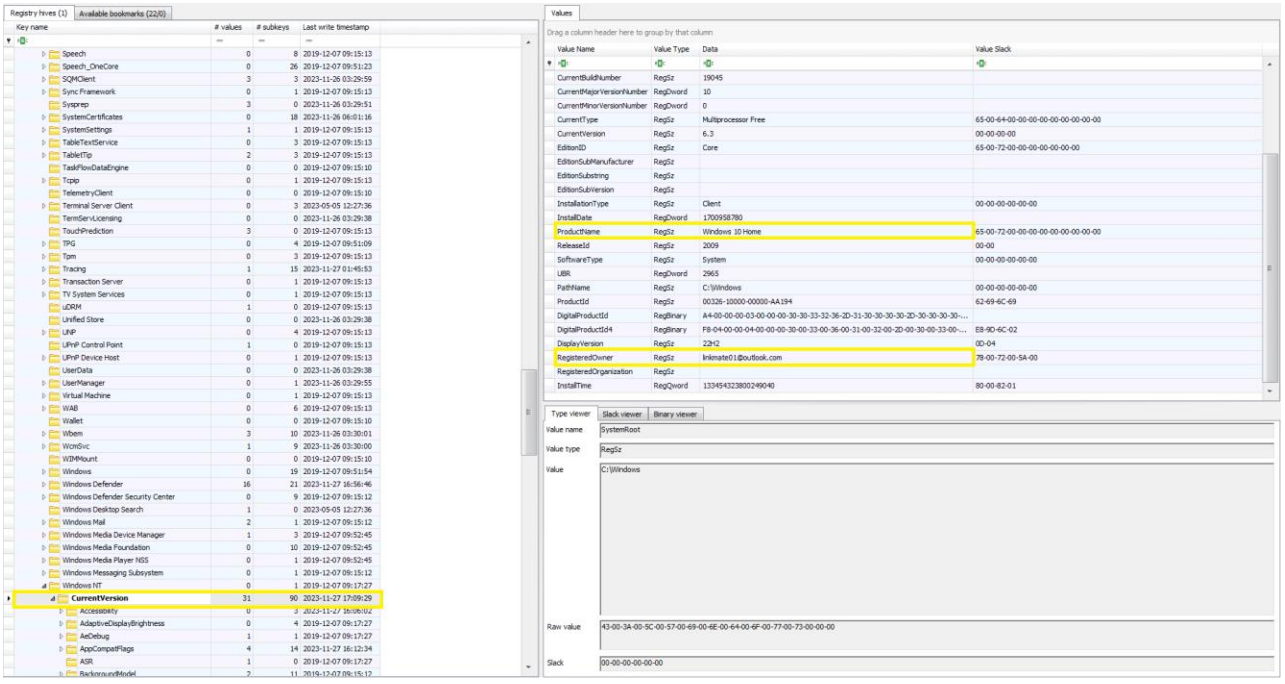

Figure 5 OS Version of the System

3) Are there any e-mail conversations to get approvals to use the funds.

- This information is obtained by navigating to data artifacts and then to E-mail messages .

- There is an email conversation between linkmate76@gmail.com and mbuffet01@gmail.com.
- The email says that linkmate76@gmail.com received a quote from a vendor for $2500 per unit, and mbuffet01@gmail.com approves the purchase and requests that all documents be in place.

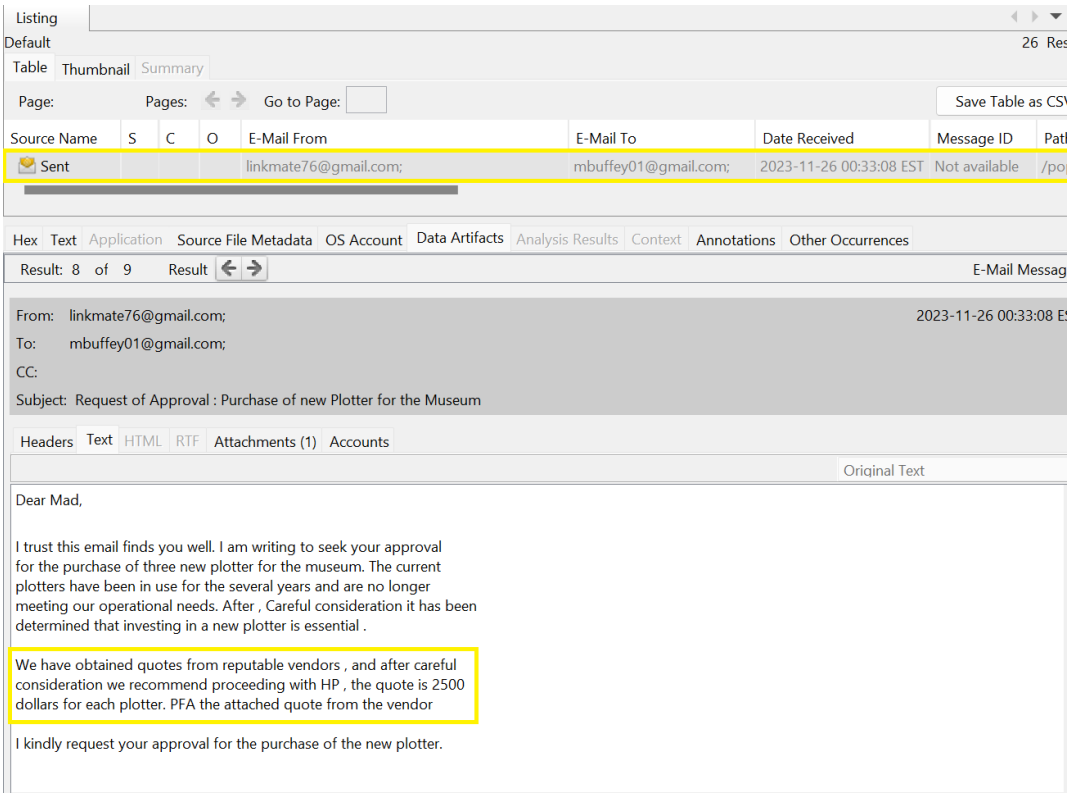

Figure 6 An email for approval of plotter purchase

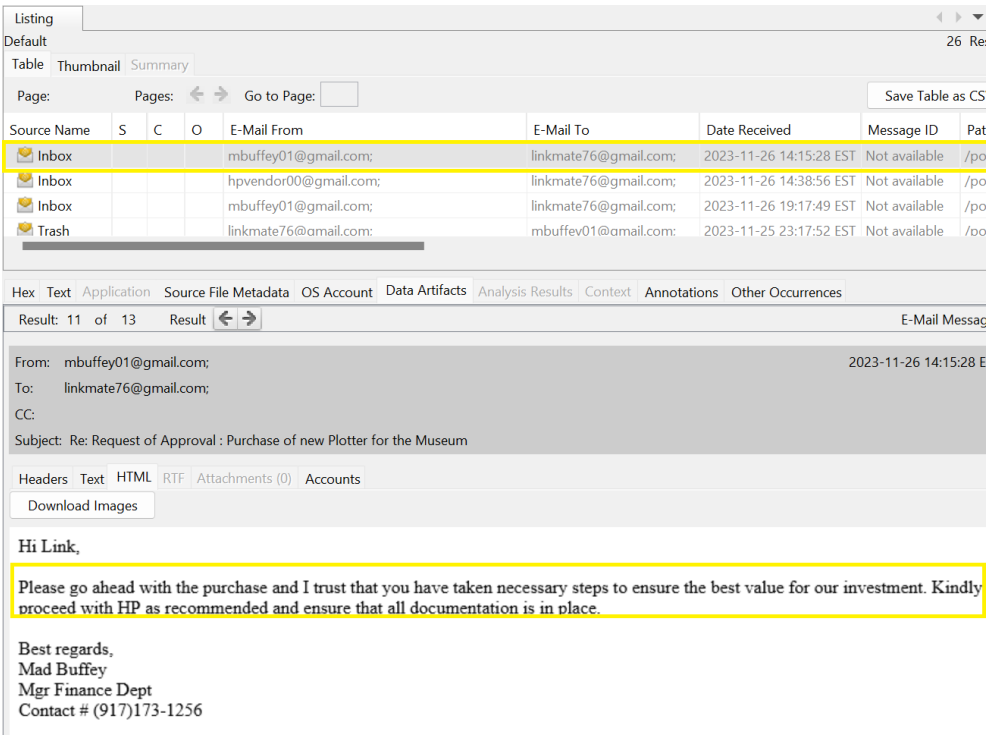

Figure 7 Approval email from mbuffey01@gmail.com

4) Are there any deleted files ? If so , what are they ?

- I have found this information by navigating to data artifacts > Recycle bin.
- A Quote document from hpvendor00@gmail.com as seen in the screenshot below was discovered in the recycle bin. In which the quote for each unit is 1500 dollars as seen in the below screenshot.

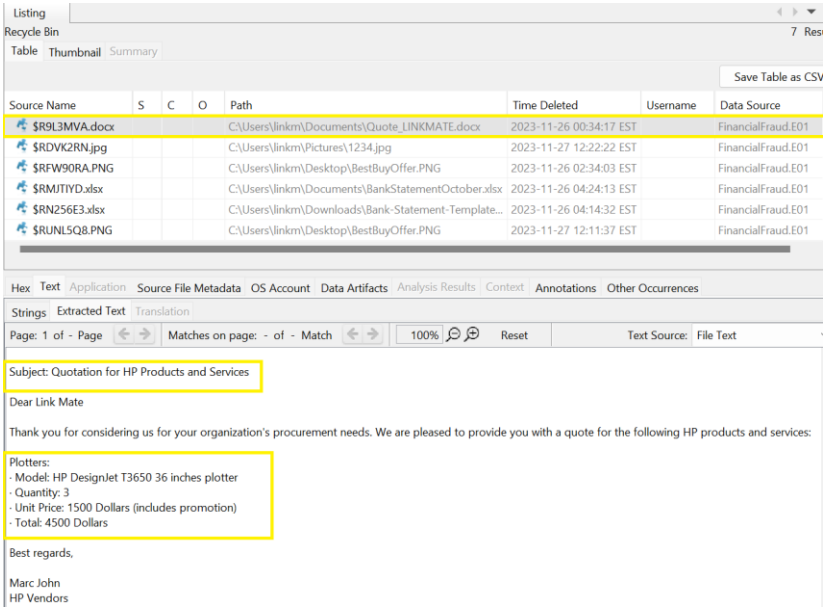

Figure 8 Quote of HP Plotter

- whereas the quote for each unit in the email sent to mbuffey01@gmail.com is 2500 dollars as seen in the below image.

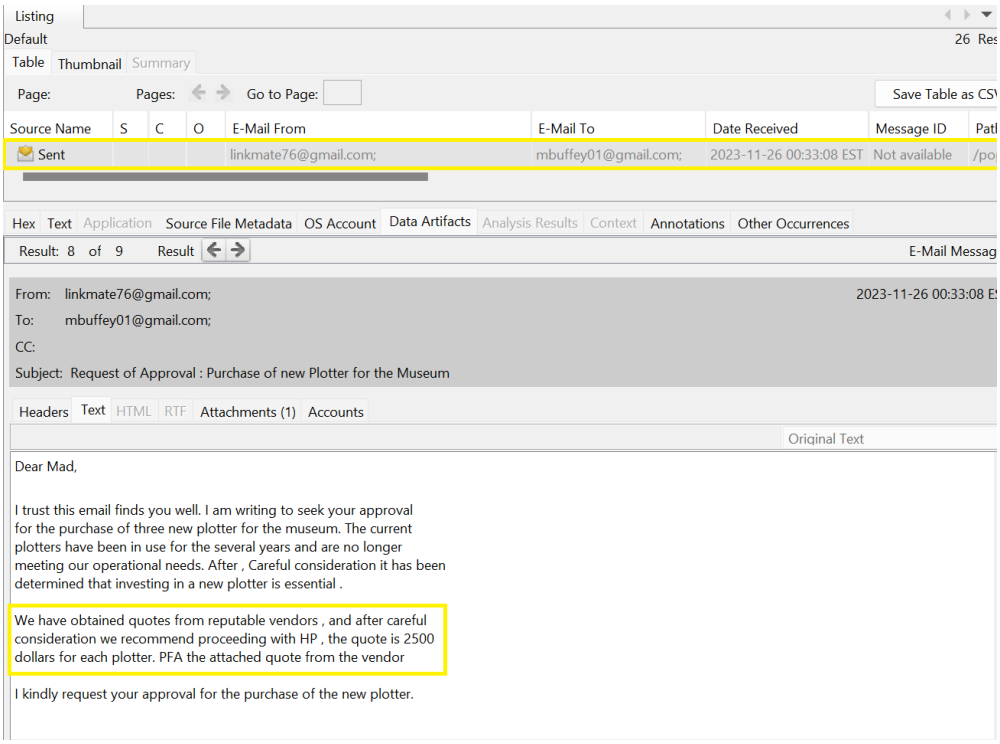

Figure 9 Email conversation between linkmate76@gmail.com and mbuffey01@gmail.com

- A bank statement for the month of October of NYC museum was found in the recycle bin.

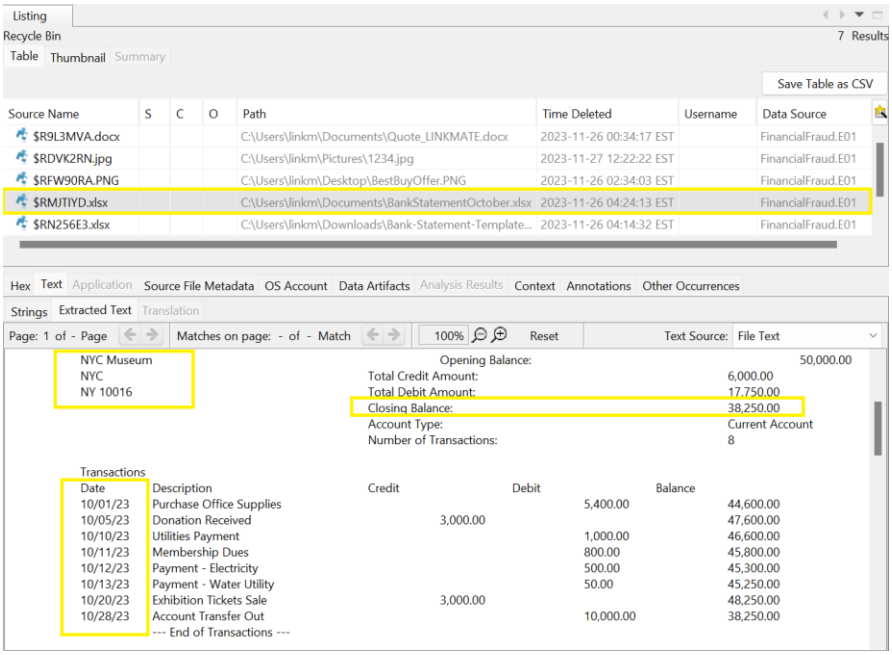

Figure 10 A Bank statement of Museum

- A picture of a Best Buy TV was also found in the recycle bin.

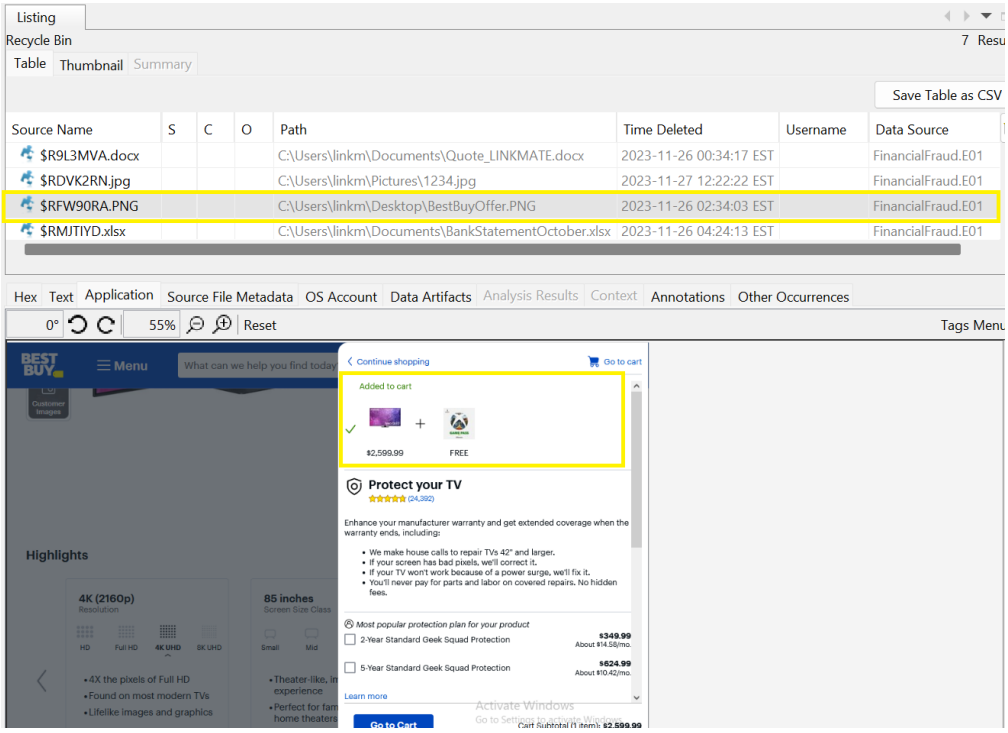

Figure 11 An image of a TV on Best Buy website found in the recycle bin

5) Was the employee using any office program to make documents?

This information is obtained by navigating to file views > File Types > Documents >Office . The document in the screenshot below is a document with a quote price 7500 Dollars and it is created with LibreOffice v7.6.3.2.

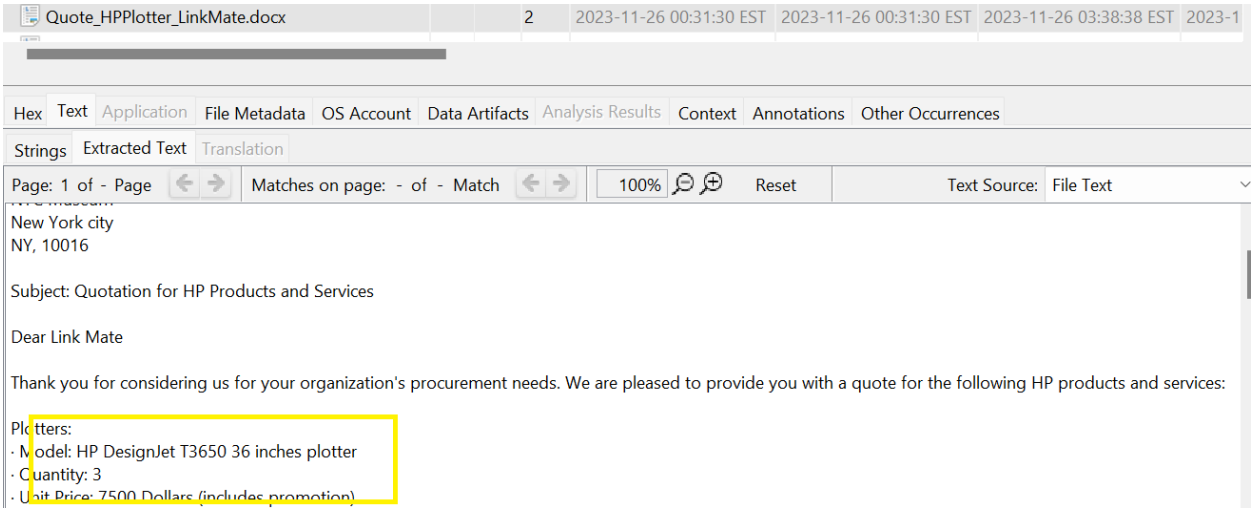

Figure 12 HP Plotter Quote document

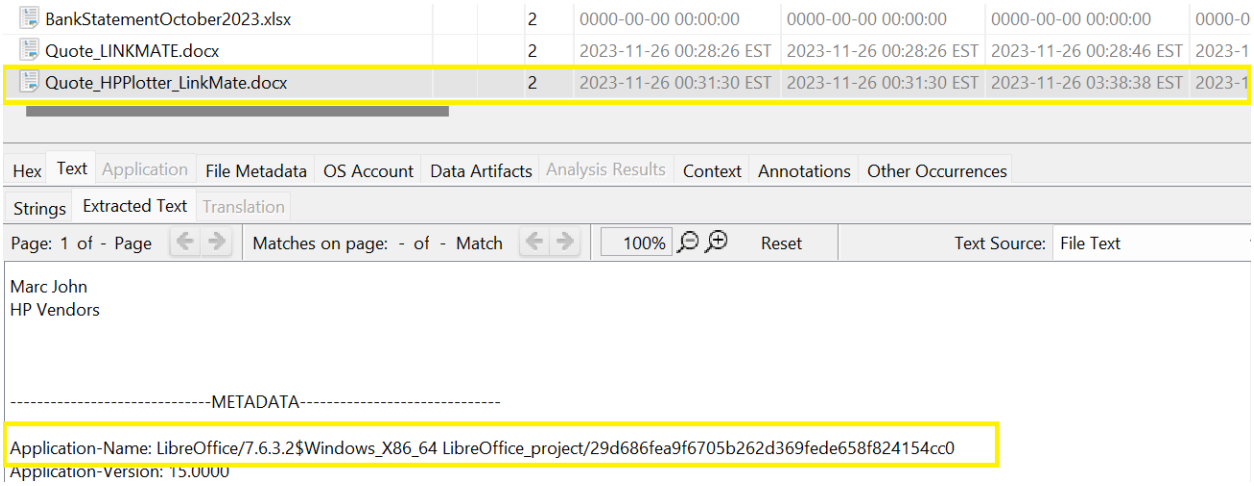

Figure 13 Using LibreOffice to make the document

Installation of LibreOffice v7.6.3.2 is seen in the screenshot below. This information is obtained by navigating to data artifacts , Installed programs.

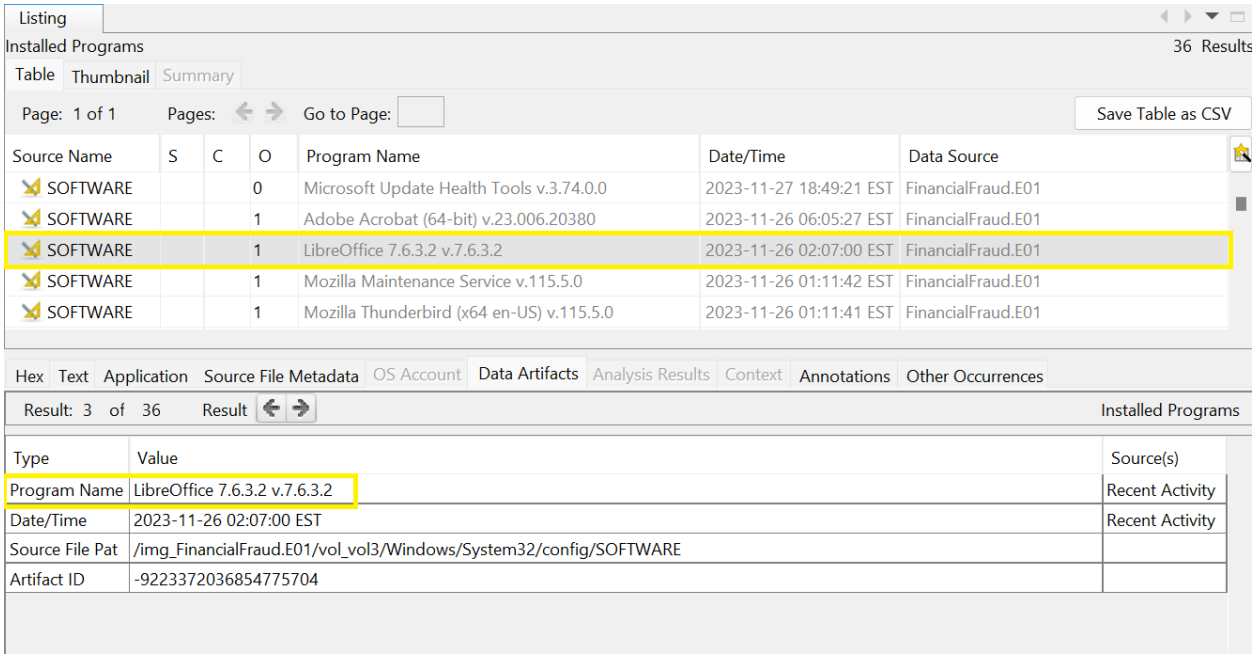

Figure 14 Installation of LibreOffice

6) Are there any same bank statements for a specific period?

- Yes, I have found two different bank statements of the museum for a particular period i.e., October 2023.
- A bank statement of museum for the month October 23 is found in the recycle bin which has a closing balance of 38,250 dollars.

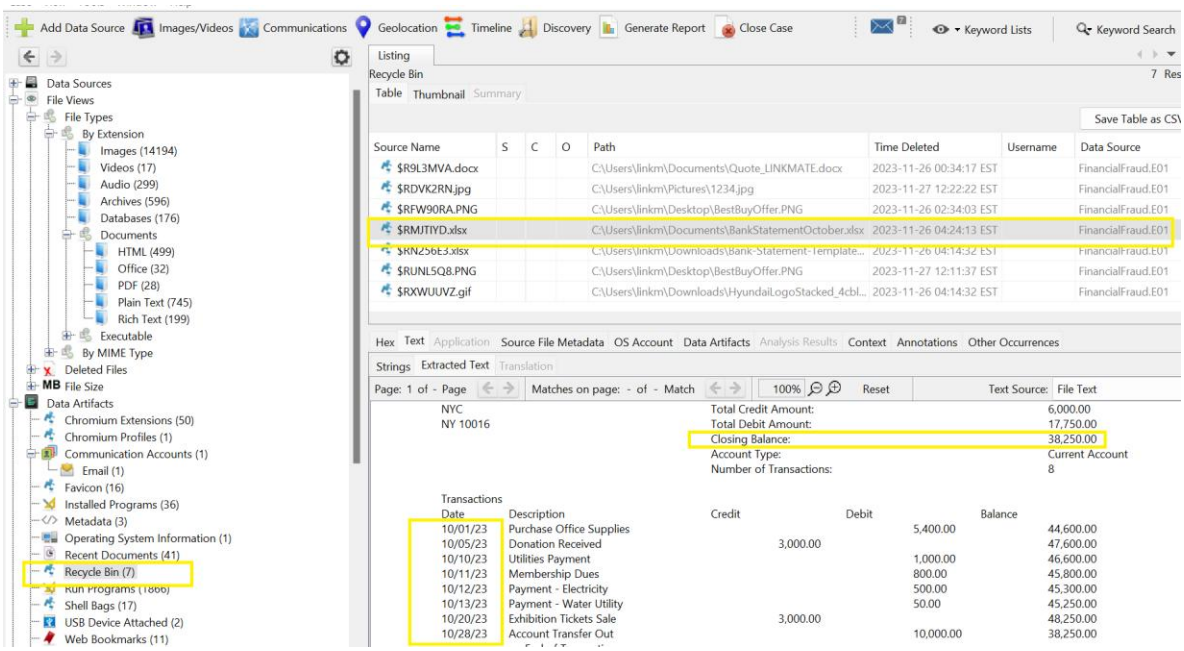

Figure 15 Bank statement found in recycle bin

- Another bank statement for the same period is found by navigating to the file views > File Types > Documents >Office. This statement has a closing balance of 48,250 and it is missing a transaction named Account transfer out for 10,000 dollars.

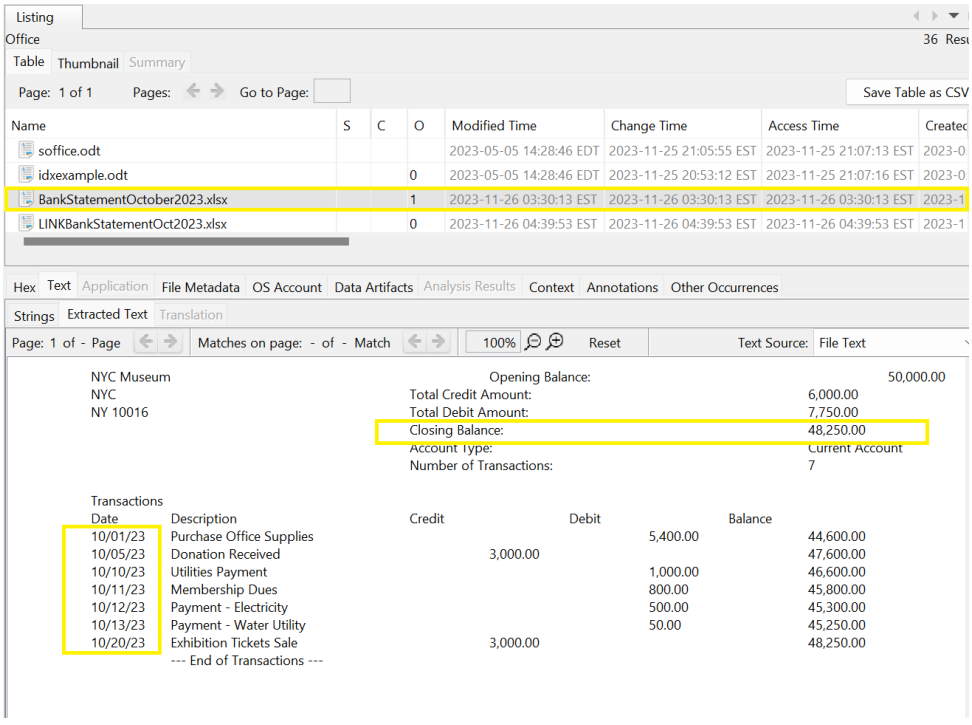

Figure 16 A different bank statement found for same period

7) Is there any invoice from any electronics dealer ?

I have found an invoice from the Best Buy by navigating to vol_vol3>users>linkm> Downloads> Best Buy Invoice . In the document a TV , it's quantity and the price which is 2599 dollars are found . All these details are seen in the screenshot below.

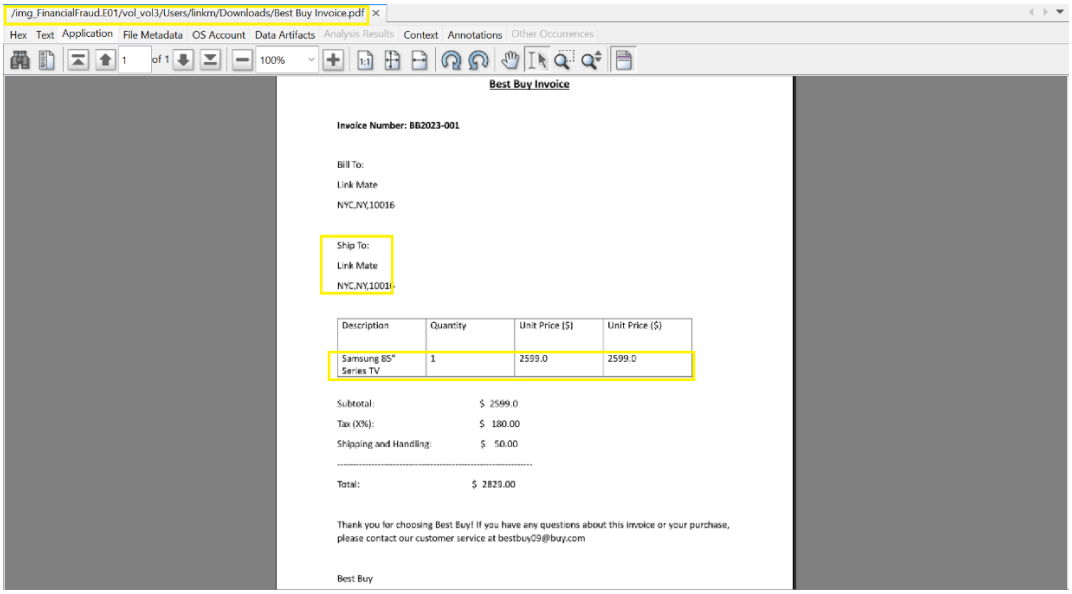

Figure 17 Invoice received from BestBuy

8) Is there any web history/ cache or any information related to the website mentioned in invoice of purchases.

In the invoice , the website mentioned is found to be Best Buy. I have also found the browsing history related to a Samsung 85" 4k UHD Smart TV and a bookmark of a Samsung 85" Best Buy TV saved.

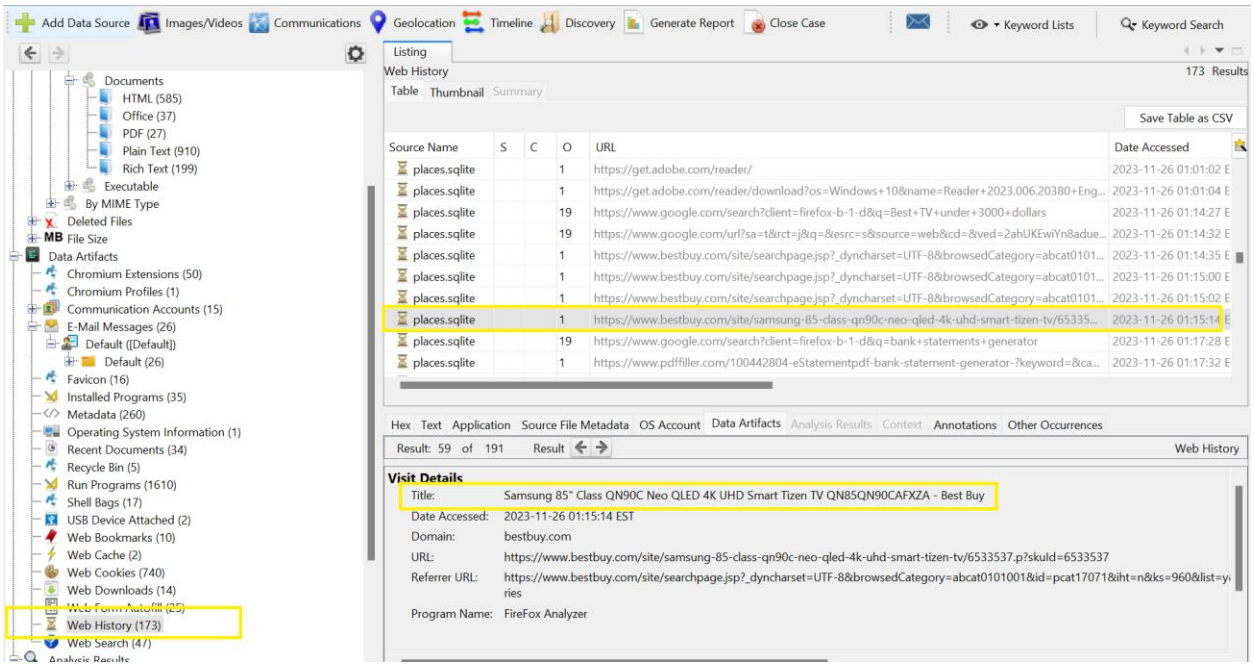

Figure 18 Web history related to best buy

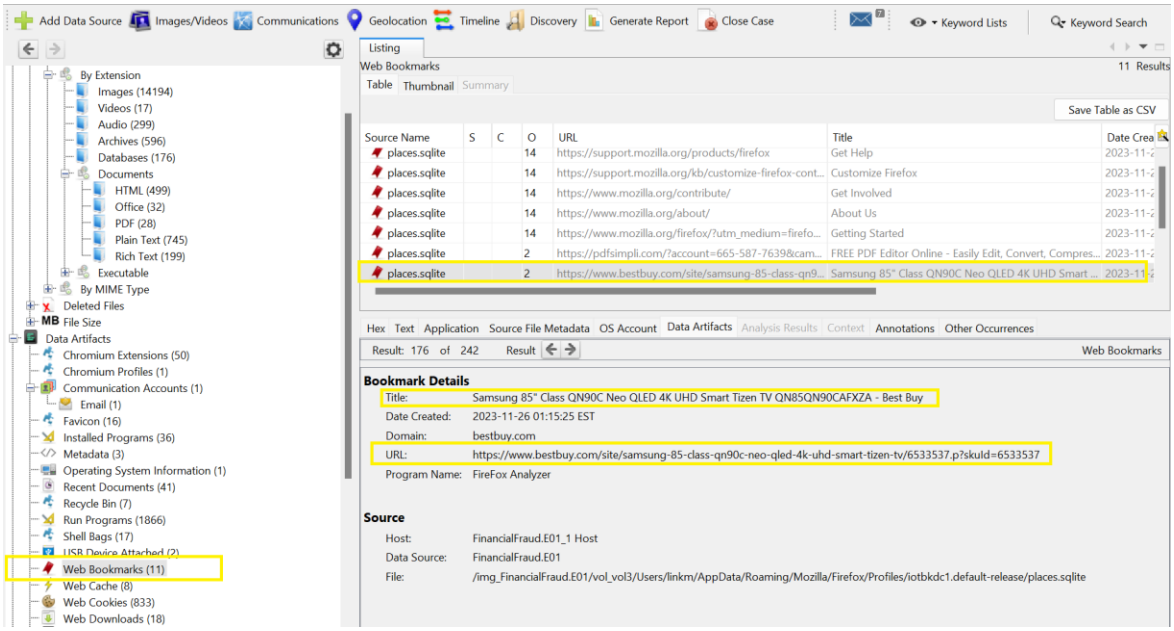

Figure 19 Bookmarks related to best buy

9) Is there any image of any closed container/item ?

A picture of a suitcase is found in the EXIF Metadata. This information is obtained by navigating to Analysis results and to EXIF Metadata.

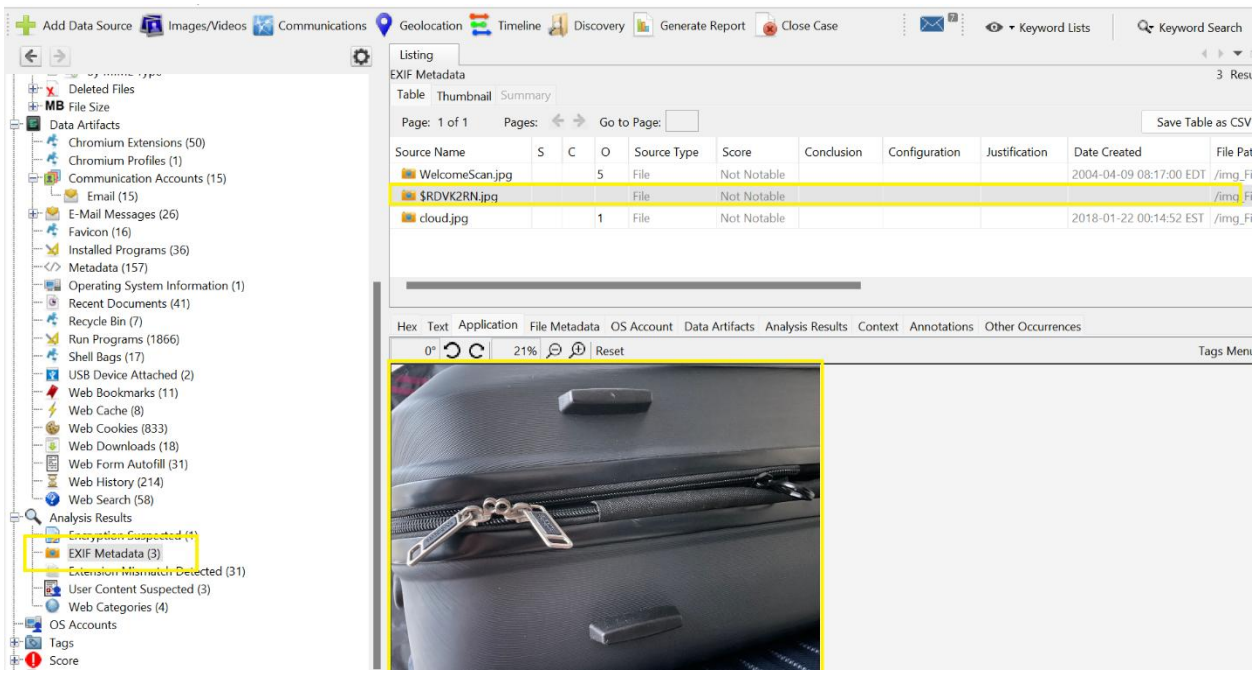

Figure 20 A suitcase picture found in EXIF Metadata

10) Is there any information on missing funds?

- I have found a file with the name 4C 69 6E 6B 4F 63 74 32 30 32 33.xlsx by navigating to file views >File Types >Documents >Office . This hexadecimal file name is converted into plain text using an online editor (https://www.duplichecker.com/hex-to-text.php) and the plain text is found to be **LinkOct2023**.
- The file that is found is identified to be a bank statement of the systems user where a deposit of 10,000 dollars is made . Also, the transactions involving AWOL Vision, American Airlines, and hotel bookings are also found.

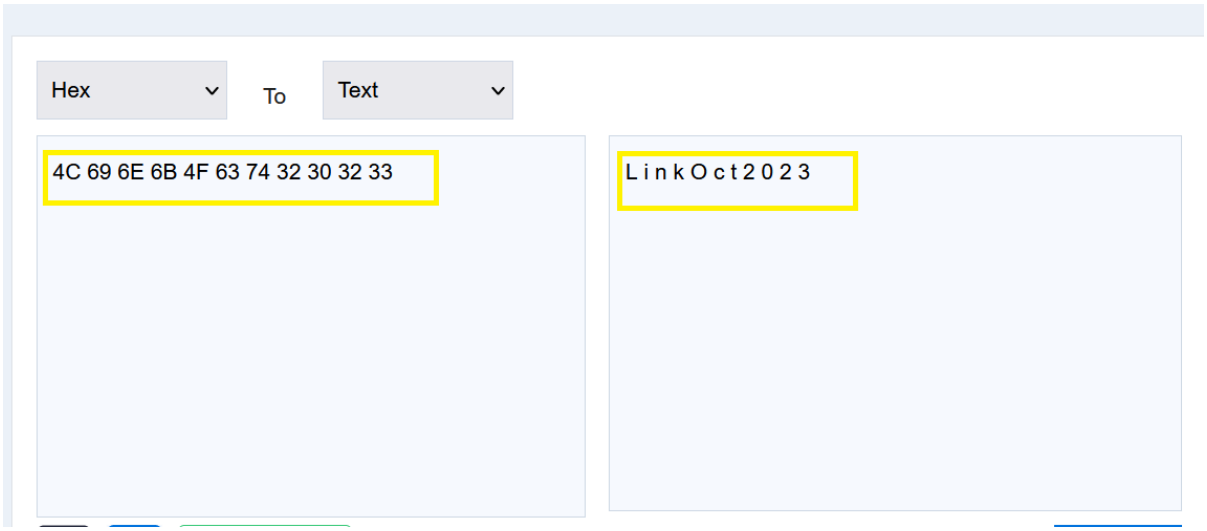

Figure 21 Hex to Text conversion

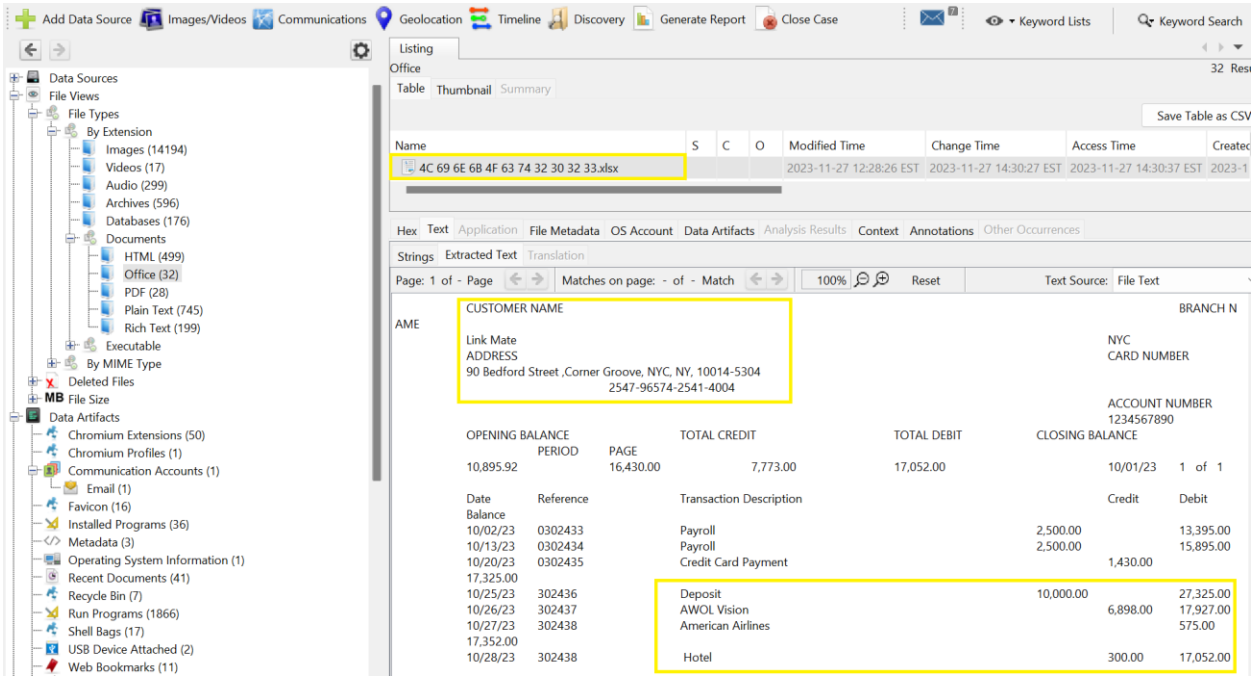

Figure 22 Bank Statement of the system's user - October 2023

- A web bookmark for the one of the transaction AWOL vision is found. The title is 92" Rollable triple laser TV.

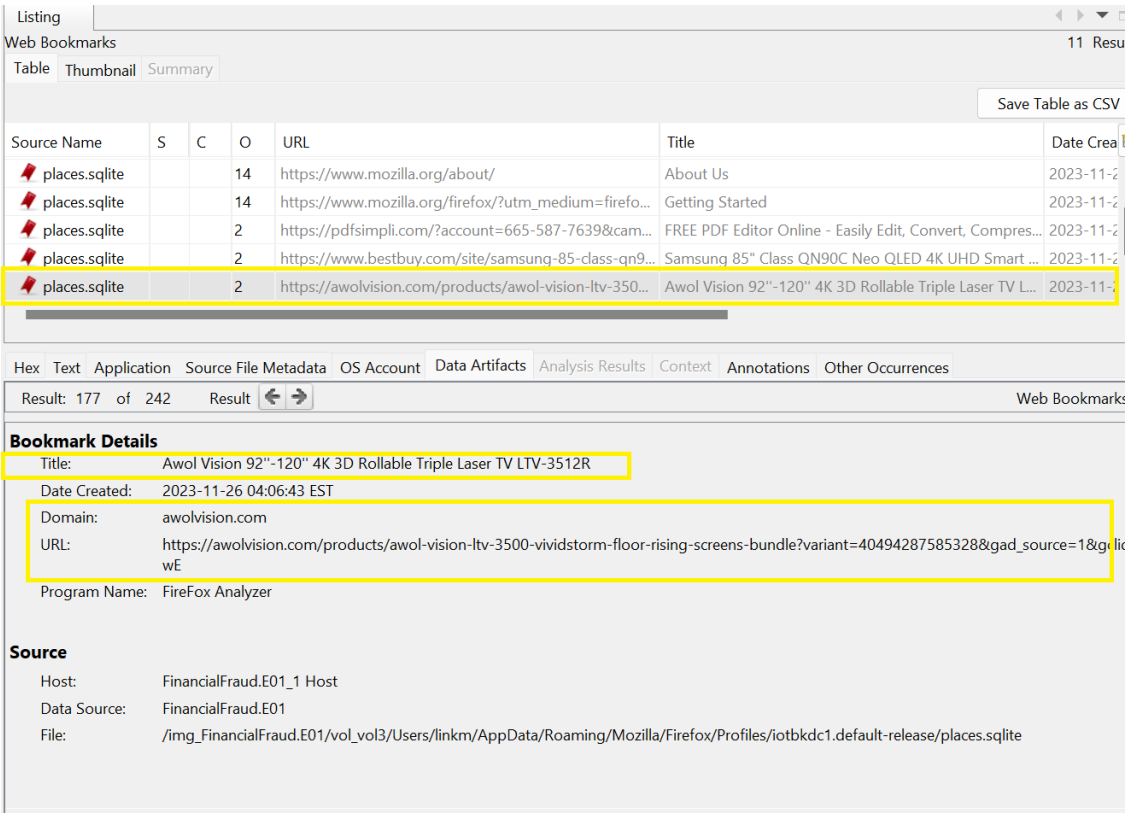

Figure 23 Web bookmark of AWOL Vision

- One of the transaction in the bank statement is American airlines , web search related to it is found. Also , an image of the flight search is also found in images/videos section of Autopsy.

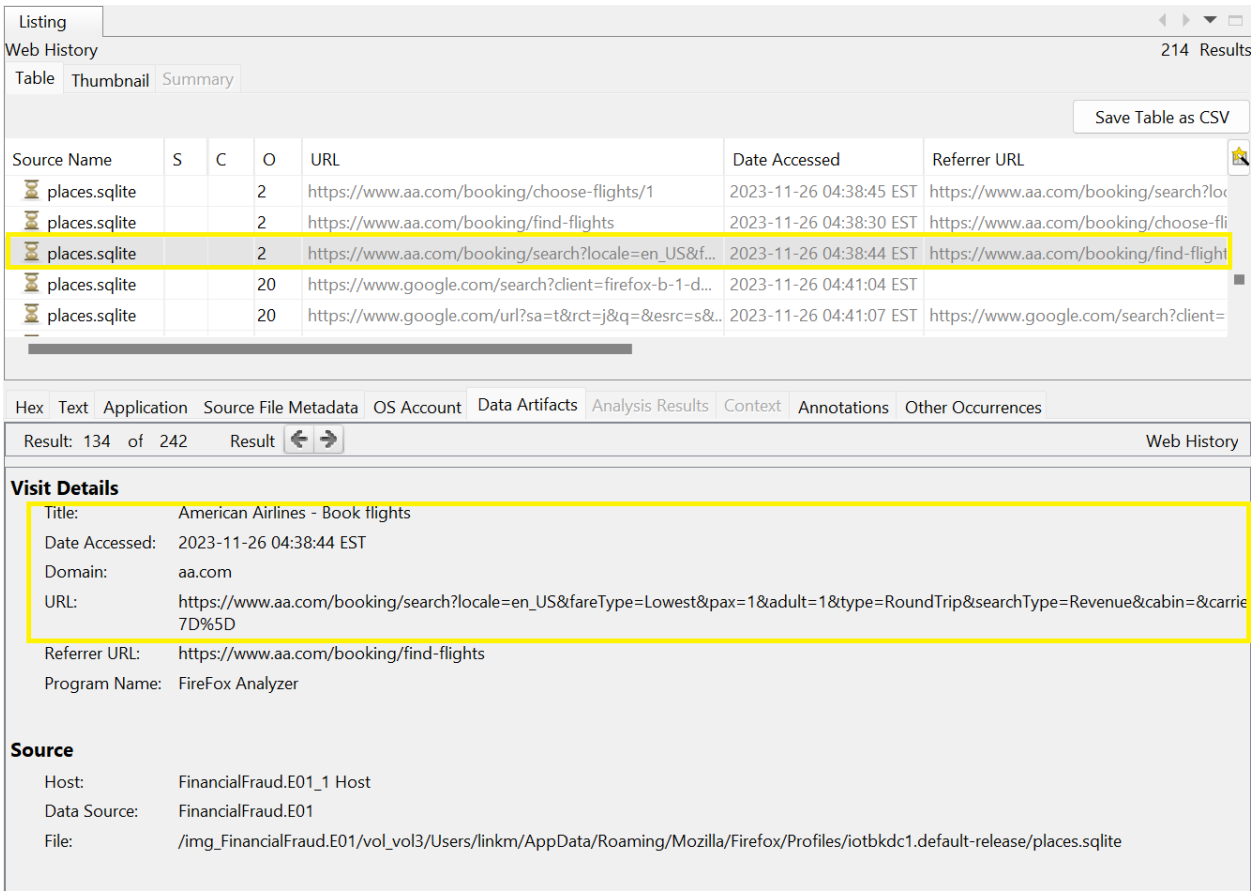

Figure 24 American Airlines flight Web Search

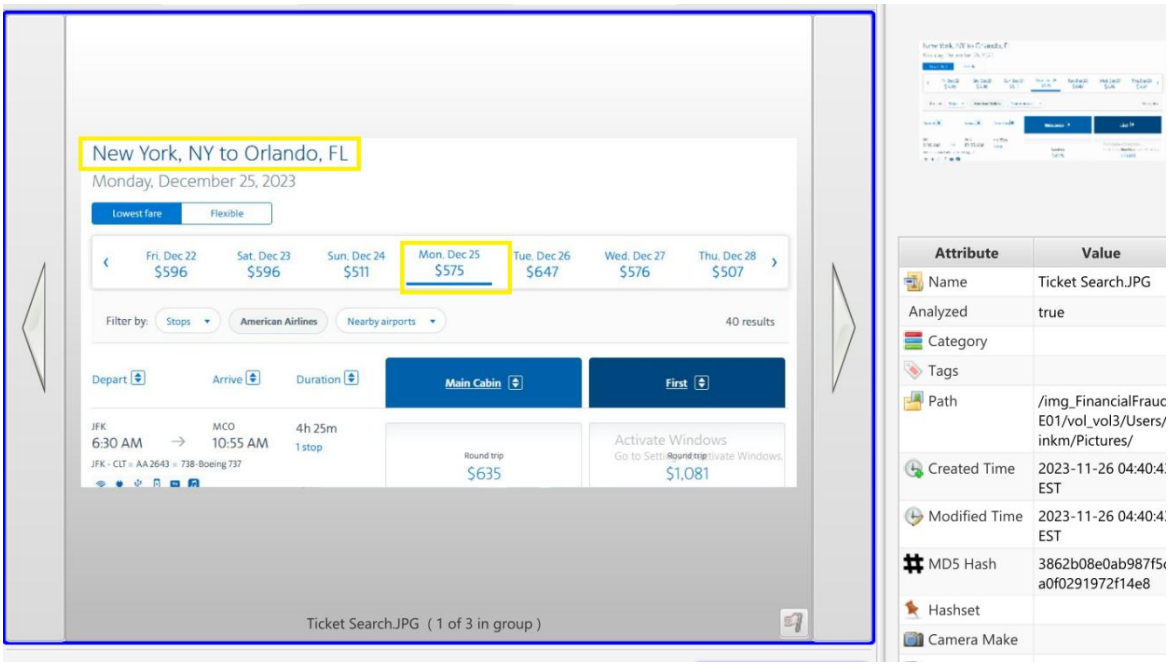

Figure 25 Flight search image

- The other transaction found in the bank statement is hotel and a web serach realted to the hotels in orlando , florida is found .

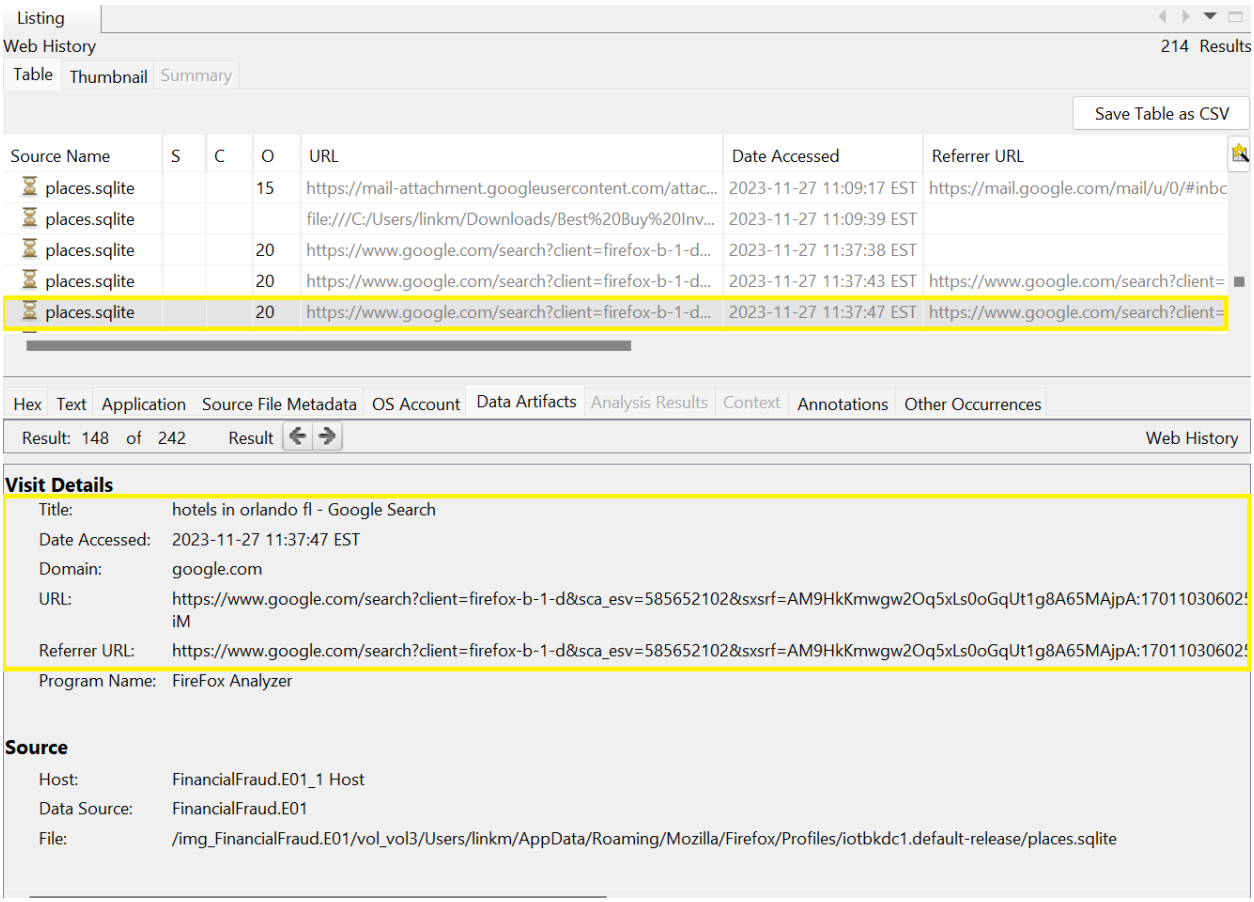

Figure 26 Web History related to the hotel search

11) Are there any hotel images ?

Yes, two images of hotels are found . One of the hotel image is named Orlando Hotel and the other hotel image is named Florida hotel.

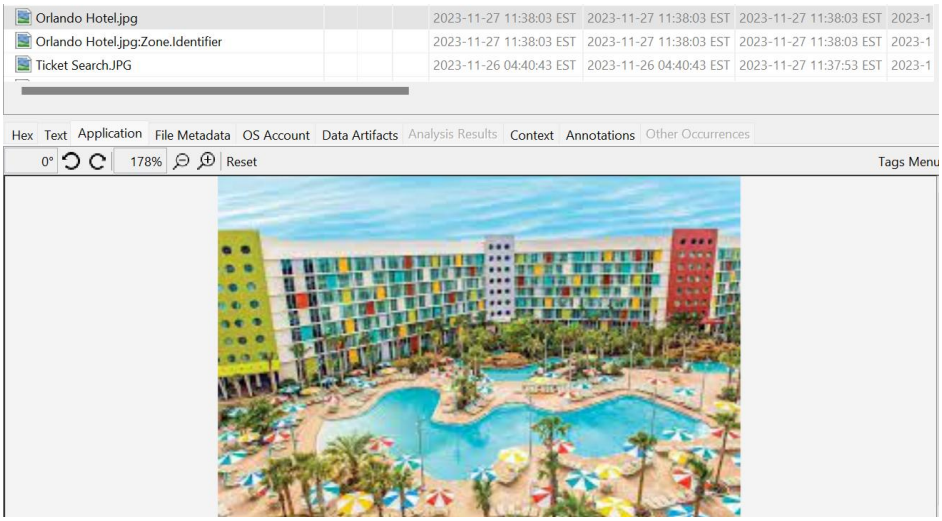

Figure 27 Hotel image 1

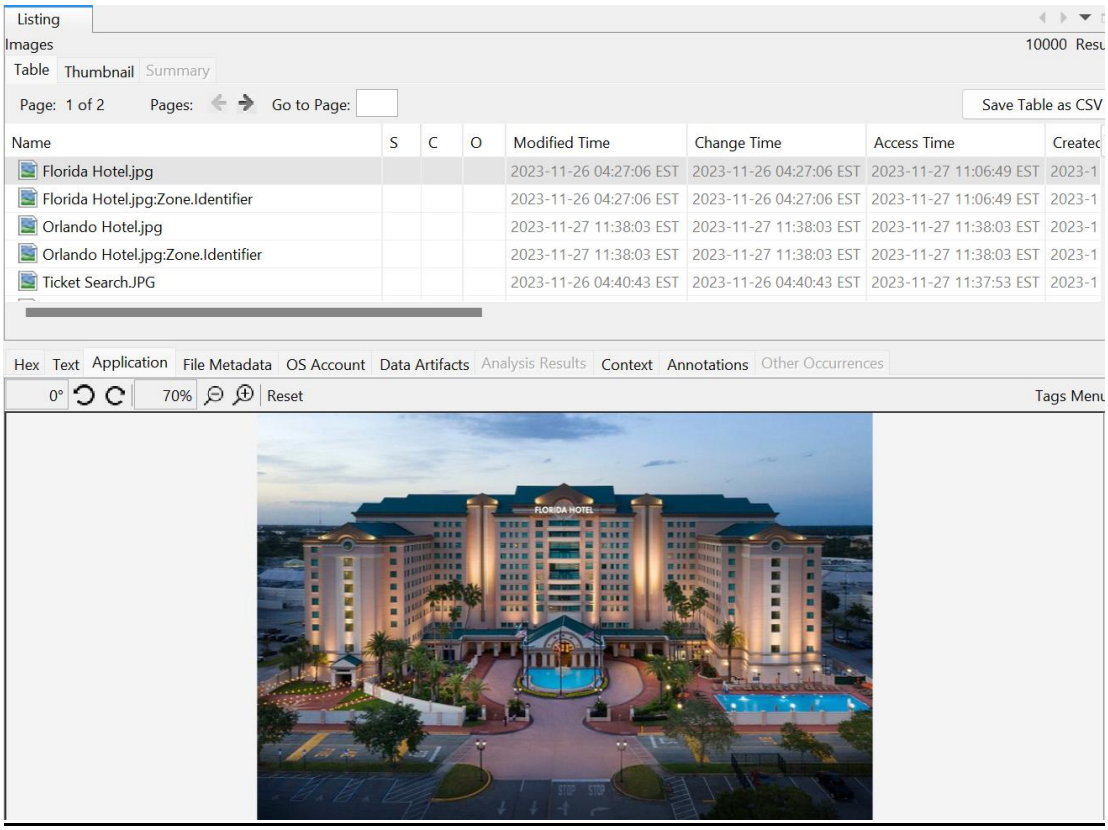

Figure 28 Hotel Image 2

Conclusion :

I Reverified the hash of image FinancialFraud.E01 after completion of examination by right clicking on the image which is loaded into the FTK Imager and then selecting verify image option . The hash value of the image is **65d52d66f22adbfb13e989da76bccc81 .** The hash value obtained after completion of exam is same as the hash value obtained before starting the examination.

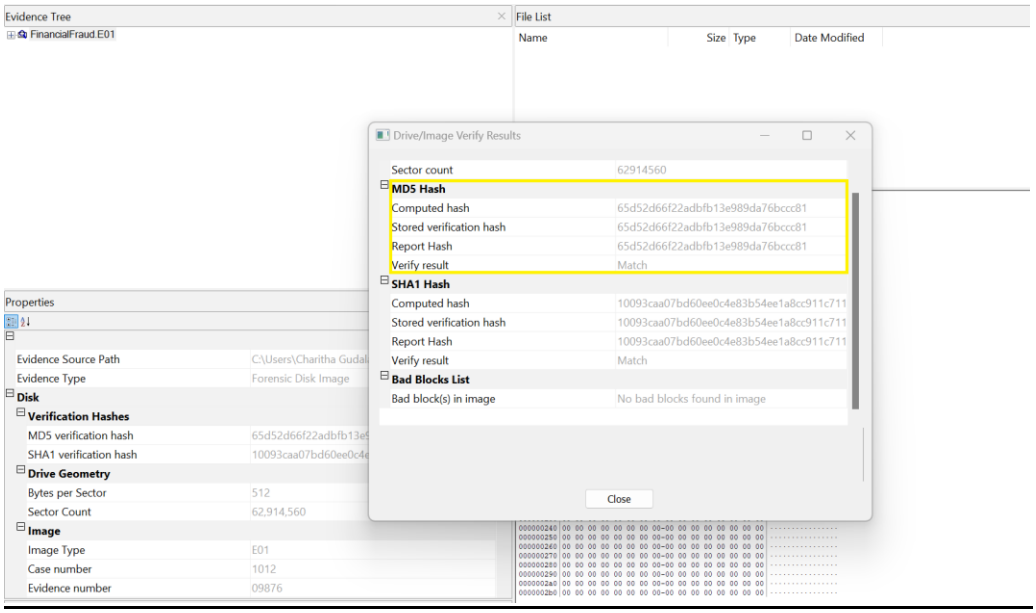

Figure 29 Reverifying the image FinancialFraud.E01 hash

In accordance with the task given by the local police department, I have generated an image file for the seized laptop and conducted a thorough analysis. The examination revealed details about the system's owner and the current version of the operating system. During this analysis, I found an email related to the approval of a plotter purchase. This email originated from linkmate76@gmail.com , to mbuffet01@gmail.com presented a quote different from the quote received from hpvendor00@gmail.com, which was in the recycle bin. Two bank statements for the museum, with two different closing balances during a specific period, were discovered and one of these statements was in the recycle bin. Additionally, an invoice addressed to the system user from Best Buy was found, detailing the purchase of a TV. A related web search about the TV was also found.

A file named 4C 69 6E 6B 4F 63 74 32 30 32 33.xlsx was encountered. Upon converting the filename to plain text, it was found to be "LinkOct2023." This document, identified as a bank statement, has a customer name as the system user's name. The museum's bank statement, which is in the recycle bin, has a $10,000 account transfer and there is a same amount deposit in system users bank statement. There are transactions involving AWOL Vision, American Airlines, and hotel bookings. Web history, bookmarks, and images associated with these transactions were also found. A suitcase was also found in the EXIF data .The final report with all the findings is submitted to the local police department.