

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.**

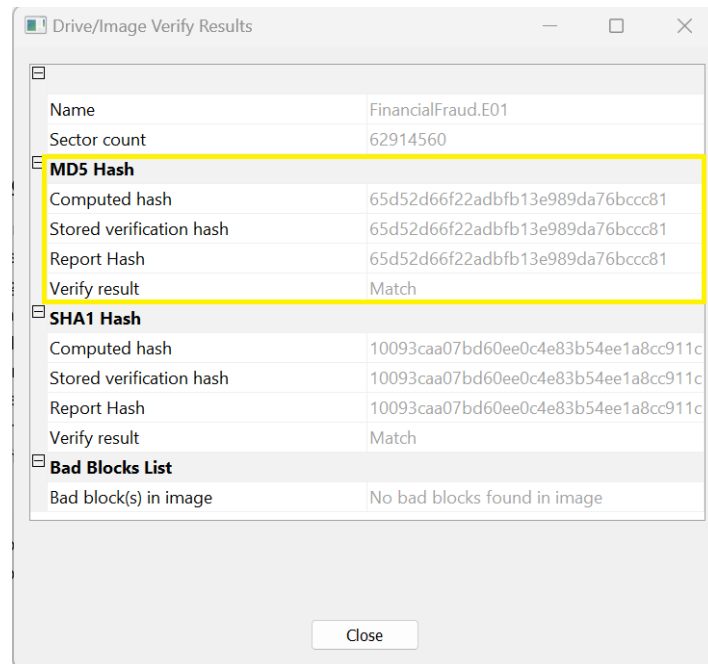


Figure 1 Hash Verification of the image FinancialFraud.E01

- 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.

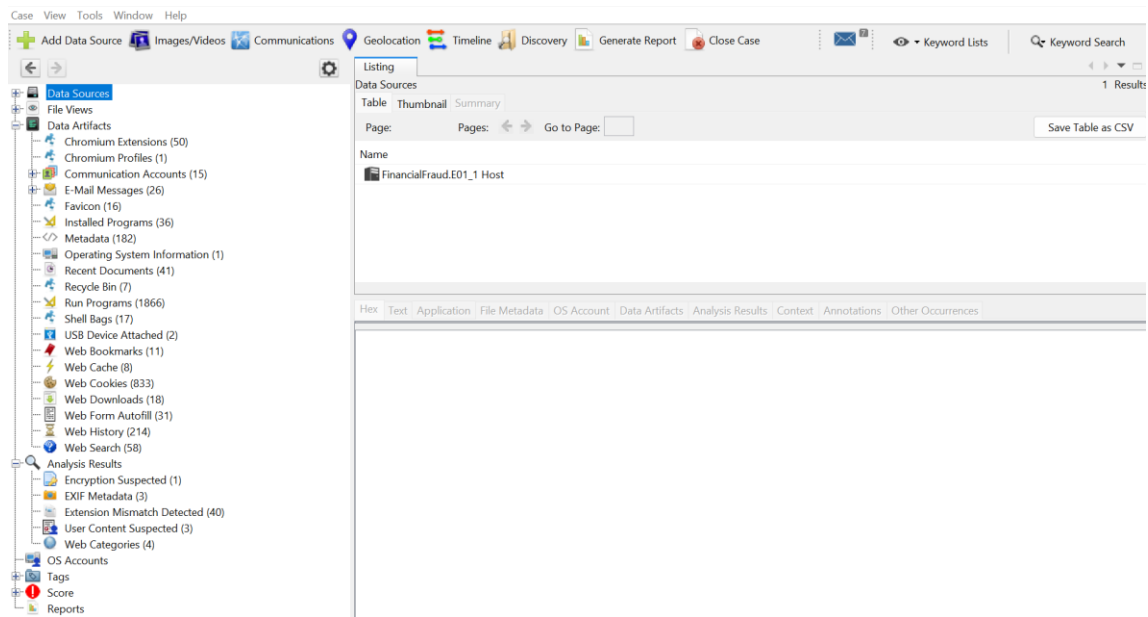


Figure 2 Autopsy File Path

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.

The screenshot shows a forensic analysis tool interface. On the left, a file tree is visible with categories like 'By Extension', 'By MIME Type', 'Deleted Files', 'Data Artifacts', and 'Installed Programs'. The 'Operating System Information (1)' item is highlighted. The main pane displays a table of operating system information for the file 'FinancialFraud.E01'.

| Source Name | S | C | O | Name | Program Name | Processor Architecture | Temporary Files Directory | Path |
|--------------------|---|---|---|-----------------|-----------------|------------------------|---------------------------|------------|
| FinancialFraud.E01 | | | | DESKTOP-TQA6OF2 | Windows 10 Home | AMD64 | %SystemRoot%\TEMP | C:\Windows |

Below the table, there is a section titled 'Operating System Information' with a table of key-value pairs:

| Type | Value | Source(s) |
|-----------------|-------------------------|-----------------|
| Name | DESKTOP-TQA6OF2 | Recent Activity |
| Program Name | Windows 10 Home | Recent Activity |
| Processor Archi | AMD64 | Recent Activity |
| Temporary File | %SystemRoot%\TEMP | Recent Activity |
| Path | C:\Windows | Recent Activity |
| Product ID | 00326-10000-00000-AA194 | Recent Activity |
| Owner | linkmate01@outlook.com | Recent Activity |
| Source File Pat | /img_FinancialFraud.E01 | |
| Artifact ID | -9223372036854775670 | |

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.

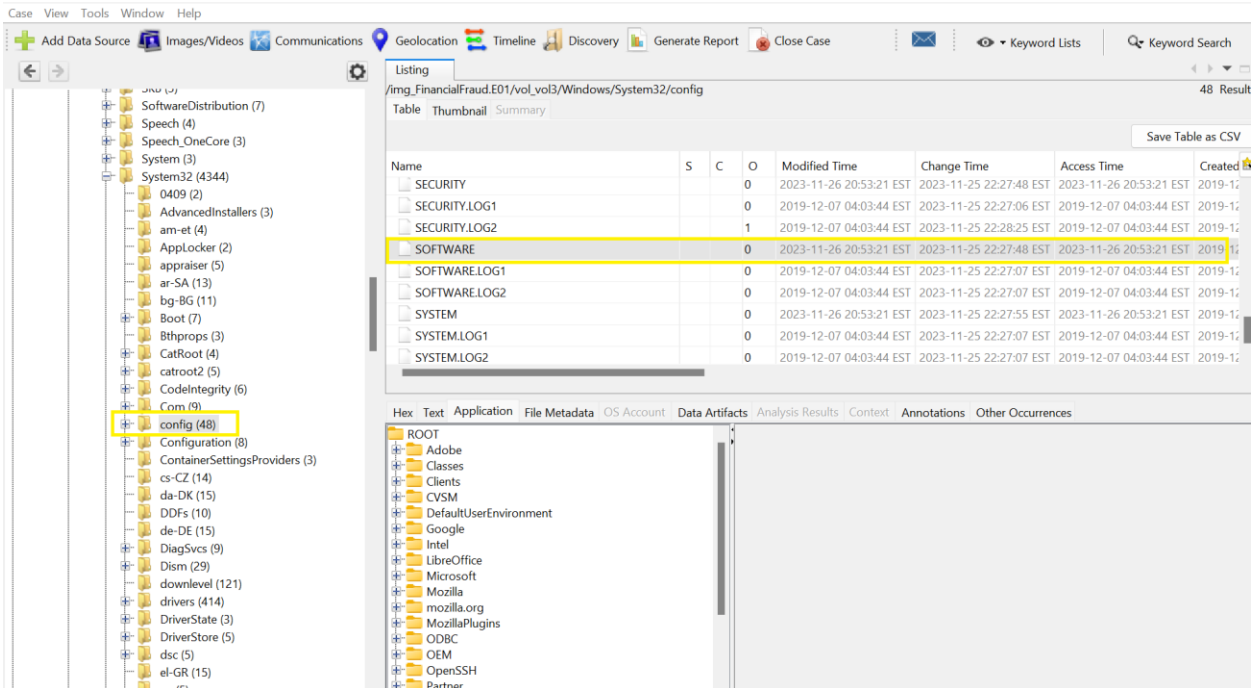


Figure 4 The Software file

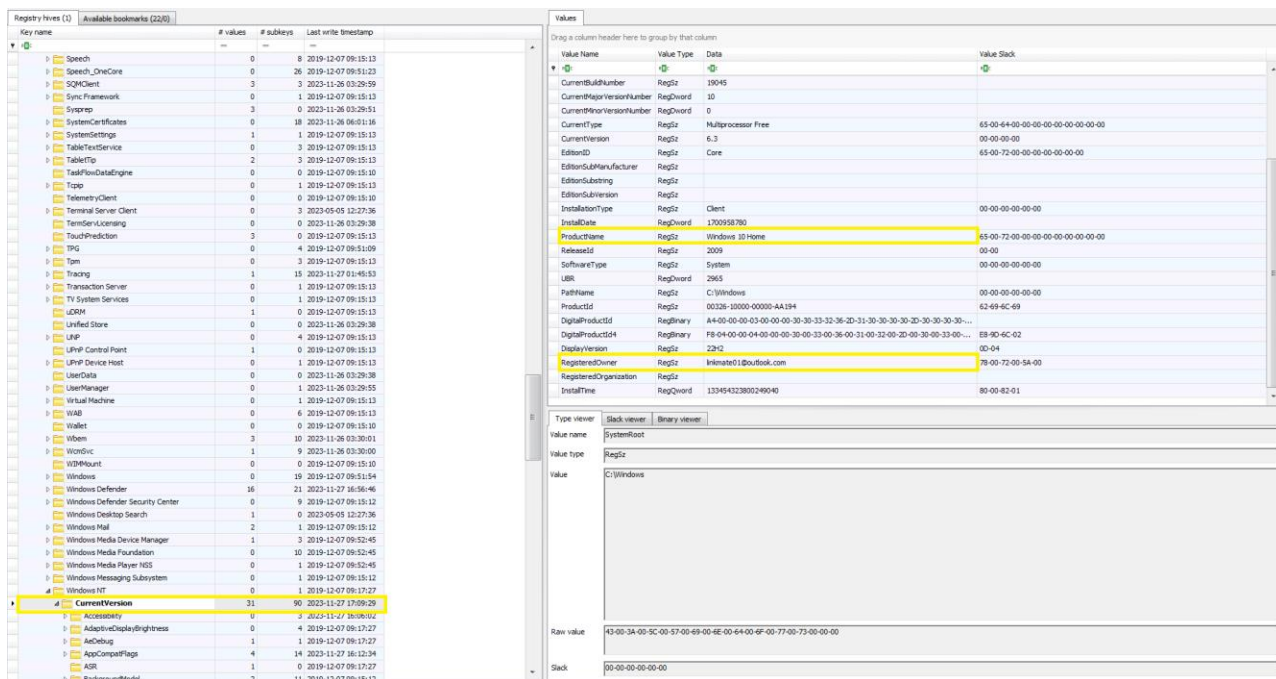


Figure 5 OS Version of the System

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.

Listing

Default 26 Res

Table Thumbnail Summary

Page: Pages: Go to Page: Save Table as CSV

| Source Name | S | C | O | E-Mail From | E-Mail To | Date Received | Message ID | Pat |
|-------------|---|---|---|-----------------------|----------------------|-------------------------|---------------|-----|
| Sent | | | | linkmate76@gmail.com; | mbuffet01@gmail.com; | 2023-11-26 00:33:08 EST | Not available | /po |

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 8 of 9 Result E-Mail Message

From: linkmate76@gmail.com; 2023-11-26 00:33:08 E

To: mbuffet01@gmail.com;

CC:

Subject: Request of Approval : Purchase of new Plotter for the Museum

Headers Text HTML RTF Attachments (1) Accounts

Original Text

Dear Mad,

I trust this email finds you well. I am writing to seek your approval for the purchase of three new plotter for the museum. The current plotters have been in use for the several years and are no longer meeting our operational needs. After , Careful consideration it has been determined that investing in a new plotter is essential .

We have obtained quotes from reputable vendors , and after careful consideration we recommend proceeding with HP , the quote is 2500 dollars for each plotter. PFA the attached quote from the vendor

I kindly request your approval for the purchase of the new plotter.

Figure 6 An email for approval of plotter purchase

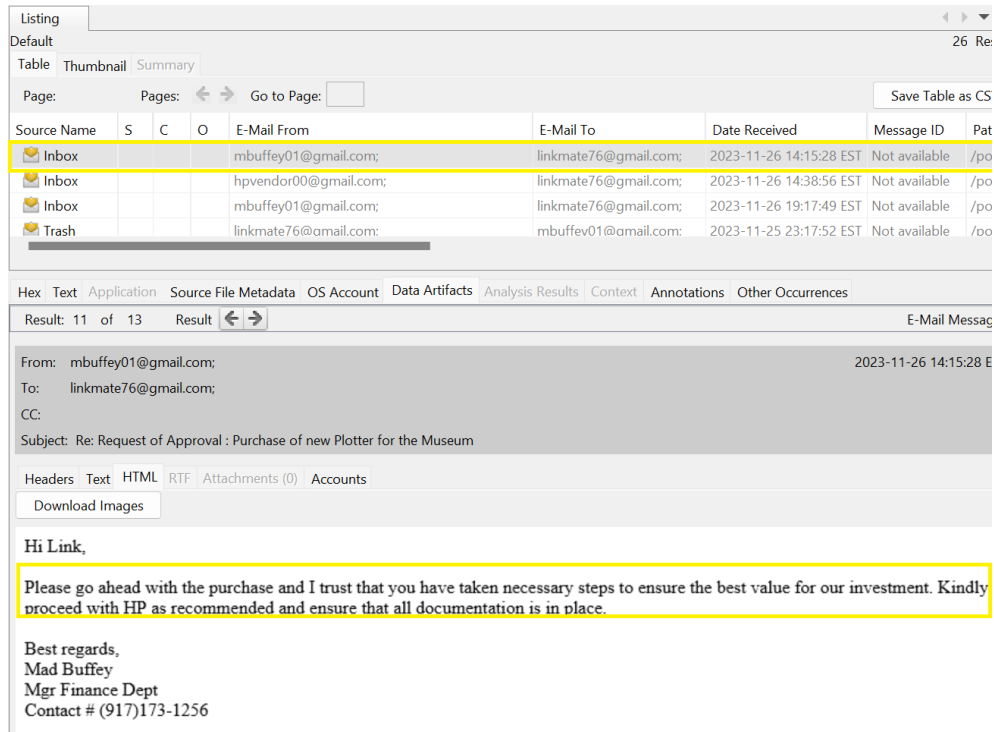


Figure 7 Approval email from mbuffey01@gmail.com

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 hvpvendor00@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.

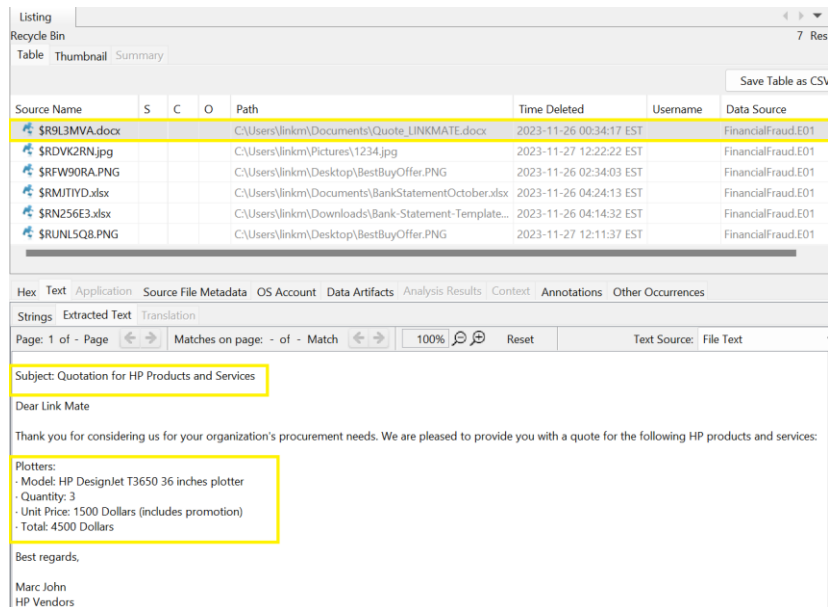


Figure 8 Quote of HP Plotter

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

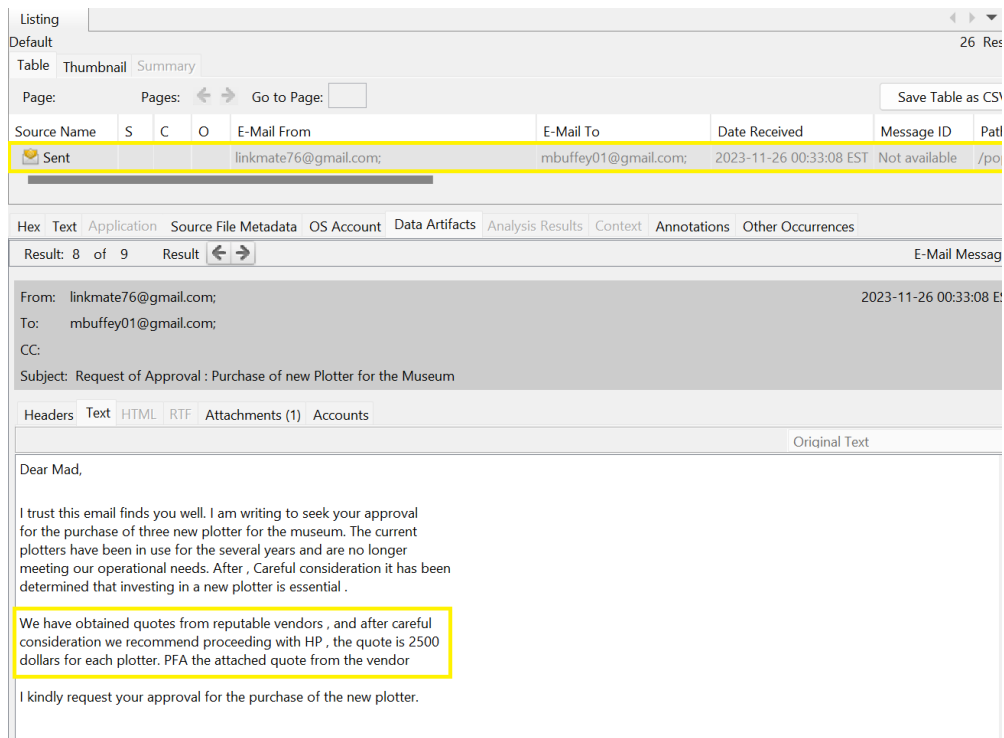


Figure 9 Email conversation between linkmate76@gmail.com and mbuffey01@gmail.com

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

The screenshot shows a file explorer window titled 'Recycle Bin' with 7 results. The file '\$RMJTIYD.xlsx' is highlighted. The file's path is 'C:\Users\linkm\Documents\BankStatementOctober.xlsx' and it was deleted on '2023-11-26 04:24:13 EST'. The file's source is 'FinancialFraud.E01'.

The file content is a bank statement for the NYC Museum for the month of October. The statement includes the following information:

| Date | Description | Credit | Debit | Balance |
|-----------------------------|--------------------------|----------|-----------|-----------|
| 10/01/23 | Purchase Office Supplies | | 5,400.00 | 44,600.00 |
| 10/05/23 | Donation Received | 3,000.00 | | 47,600.00 |
| 10/10/23 | Utilities Payment | | 1,000.00 | 46,600.00 |
| 10/11/23 | Membership Dues | | 800.00 | 45,800.00 |
| 10/12/23 | Payment - Electricity | | 500.00 | 45,300.00 |
| 10/13/23 | Payment - Water Utility | | 50.00 | 45,250.00 |
| 10/20/23 | Exhibition Tickets Sale | 3,000.00 | | 48,250.00 |
| 10/28/23 | Account Transfer Out | | 10,000.00 | 38,250.00 |
| --- End of Transactions --- | | | | |

The statement also includes a summary of the account balance:

| Opening Balance: | 50,000.00 |
|----------------------|-----------|
| Total Credit Amount: | 6,000.00 |
| Total Debit Amount: | 17,750.00 |
| Closing Balance: | 38,250.00 |

The account type is 'Current Account' and the number of transactions is 8.

Figure 10 A Bank statement of Museum

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

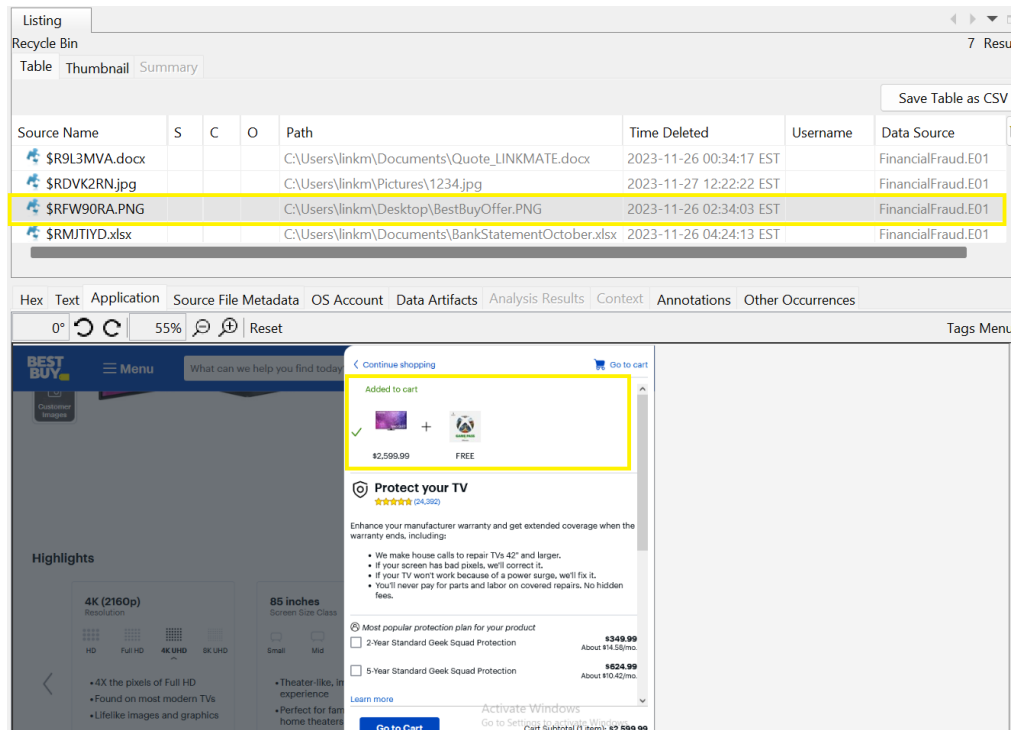


Figure 11 An image of a TV on Best Buy website found in the recycle bin

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.

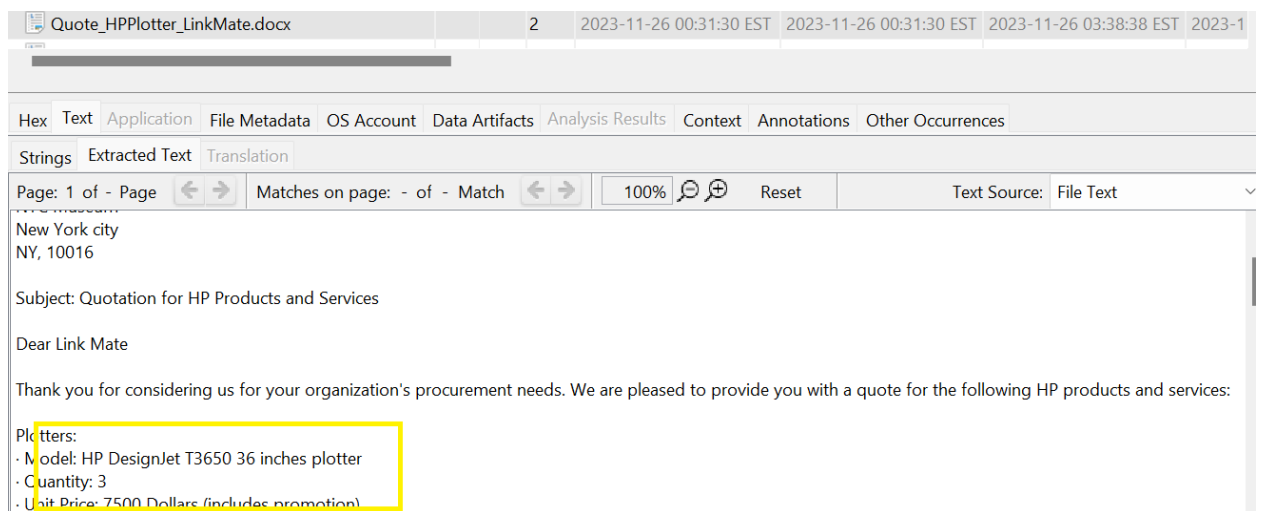


Figure 12 HP Plotter Quote document

| | | | | | |
|-------------------------------|---|-------------------------|-------------------------|-------------------------|--------|
| BankStatementOctober2023.xlsx | 2 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-0 |
| Quote_LINKMATE.docx | 2 | 2023-11-26 00:28:26 EST | 2023-11-26 00:28:26 EST | 2023-11-26 00:28:46 EST | 2023-1 |
| Quote_HPPlotter_LinkMate.docx | 2 | 2023-11-26 00:31:30 EST | 2023-11-26 00:31:30 EST | 2023-11-26 03:38:38 EST | 2023-1 |

| | | | | | | | | | |
|-----|------|-------------|---------------|------------|----------------|------------------|---------|-------------|-------------------|
| Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences |
|-----|------|-------------|---------------|------------|----------------|------------------|---------|-------------|-------------------|

| | | |
|---------|----------------|-------------|
| Strings | Extracted Text | Translation |
|---------|----------------|-------------|

Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text

Marc John
HP Vendors

-----METADATA-----

Application-Name: LibreOffice/7.6.3.2\$Windows_X86_64 LibreOffice_project/29d686fea9f6705b262d369fede658f824154cc0

Application-Version: 15.0000

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.

| | | | | | | |
|--------------------|-----------|-------------|---|-------------------------------------------|-------------------------|--------------------|
| Listing | | | | | | 36 Results |
| Installed Programs | | | | | | |
| Table | Thumbnail | Summary | | | | |
| Page: 1 of 1 | Pages: | Go to Page: | | | Save Table as CSV | |
| Source Name | S | C | O | Program Name | Date/Time | Data Source |
| SOFTWARE | | | 0 | Microsoft Update Health Tools v.3.74.0.0 | 2023-11-27 18:49:21 EST | FinancialFraud.E01 |
| SOFTWARE | | | 1 | Adobe Acrobat (64-bit) v.23.006.20380 | 2023-11-26 06:05:27 EST | FinancialFraud.E01 |
| SOFTWARE | | | 1 | LibreOffice 7.6.3.2 v.7.6.3.2 | 2023-11-26 02:07:00 EST | FinancialFraud.E01 |
| SOFTWARE | | | 1 | Mozilla Maintenance Service v.115.5.0 | 2023-11-26 01:11:42 EST | FinancialFraud.E01 |
| SOFTWARE | | | 1 | Mozilla Thunderbird (x64 en-US) v.115.5.0 | 2023-11-26 01:11:41 EST | FinancialFraud.E01 |

| | | | | | | | | | |
|-----|------|-------------|----------------------|------------|----------------|------------------|---------|-------------|-------------------|
| Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences |
|-----|------|-------------|----------------------|------------|----------------|------------------|---------|-------------|-------------------|

Result: 3 of 36 Result Installed Programs

| | | |
|-----------------|-------------------------------------------------------------------|-----------------|
| Type | Value | Source(s) |
| Program Name | LibreOffice 7.6.3.2 v.7.6.3.2 | Recent Activity |
| Date/Time | 2023-11-26 02:07:00 EST | Recent Activity |
| Source File Pat | /img_FinancialFraud.E01/vol_vol3/Windows/System32/config/SOFTWARE | |
| Artifact ID | -9223372036854775704 | |

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 shows a screenshot of a file explorer interface. The left sidebar displays a tree view of file types, with 'Recycle Bin (7)' highlighted. The main pane shows a list of files in the Recycle Bin. The file 'SRMJTYD.xlsx' is highlighted, showing its path as 'C:\Users\linkm\Documents\BankStatementOctober.xlsx' and its deletion time as '2023-11-26 04:24:13 EST'. Below the file list, the 'Extracted Text' tab is active, displaying a summary of the file's content. The summary includes a closing balance of 38,250.00 and a list of transactions for October 2023.

| Source Name | S | C | O | Path | Time Deleted | Username | Data Source |
|---------------|---|---|---|-----------------------------------------------------|-------------------------|----------|--------------------|
| SR9L3MVA.docx | | | | C:\Users\linkm\Documents\Quote_LINKMATE.docx | 2023-11-26 00:34:17 EST | | FinancialFraud.E01 |
| SRDVK2RN.jpg | | | | C:\Users\linkm\Pictures\1234.jpg | 2023-11-27 12:22:22 EST | | FinancialFraud.E01 |
| SRFW90RA.PNG | | | | C:\Users\linkm\Desktop\BestBuyOffer.PNG | 2023-11-26 02:34:03 EST | | FinancialFraud.E01 |
| SRMJTYD.xlsx | | | | C:\Users\linkm\Documents\BankStatementOctober.xlsx | 2023-11-26 04:24:13 EST | | FinancialFraud.E01 |
| SRNZ56E3.xlsx | | | | C:\Users\linkm\Downloads\Bank-Statement-Template... | 2023-11-26 04:14:32 EST | | FinancialFraud.E01 |
| SRUNLSQ8.PNG | | | | C:\Users\linkm\Desktop\BestBuyOffer.PNG | 2023-11-27 12:11:37 EST | | FinancialFraud.E01 |
| SRXWUUVZ.gif | | | | C:\Users\linkm\Downloads\HyundaiLogoStacked_4cbl... | 2023-11-26 04:14:32 EST | | FinancialFraud.E01 |

| Strings | Extracted Text | Translation |
|-------------------|-------------------------------|-----------------|
| Page: 1 of - Page | Matches on page: - of - Match | 100% Reset |
| NYC | Total Credit Amount: | 6,000.00 |
| NY 10016 | Total Debit Amount: | 17,750.00 |
| | Closing Balance: | 38,250.00 |
| | Account Type: | Current Account |
| | Number of Transactions: | 8 |

| Transactions | Date | Description | Credit | Debit | Balance |
|--------------|----------|--------------------------|----------|-----------|-----------|
| | 10/01/23 | Purchase Office Supplies | | 5,400.00 | 44,600.00 |
| | 10/05/23 | Donation Received | 3,000.00 | | 47,600.00 |
| | 10/10/23 | Utilities Payment | | 1,000.00 | 46,600.00 |
| | 10/11/23 | Membership Dues | | 800.00 | 45,800.00 |
| | 10/12/23 | Payment - Electricity | | 500.00 | 45,300.00 |
| | 10/13/23 | Payment - Water Utility | | 50.00 | 45,250.00 |
| | 10/20/23 | Exhibition Tickets Sale | 3,000.00 | | 48,250.00 |
| | 10/28/23 | Account Transfer Out | | 10,000.00 | 38,250.00 |

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 shows a screenshot of a file explorer interface. The left sidebar displays a tree view of file types, with 'Office' highlighted. The main pane shows a list of files in the Office folder. The file 'BankStatementOctober2023.xlsx' is highlighted, showing its path as 'C:\Users\linkm\Documents\BankStatementOctober.xlsx' and its deletion time as '2023-11-26 03:30:13 EST'. Below the file list, the 'Extracted Text' tab is active, displaying a summary of the file's content. The summary includes a closing balance of 48,250.00 and a list of transactions for October 2023.

| Name | S | C | O | Modified Time | Change Time | Access Time | Created |
|-------------------------------|---|---|---|-------------------------|-------------------------|-------------------------|-----------|
| soffice.odt | | | | 2023-05-05 14:28:46 EDT | 2023-11-25 21:05:55 EST | 2023-11-25 21:07:13 EST | 2023-0... |
| idxexample.odt | | | 0 | 2023-05-05 14:28:46 EDT | 2023-11-25 20:53:12 EST | 2023-11-25 21:07:16 EST | 2023-0... |
| BankStatementOctober2023.xlsx | | | 1 | 2023-11-26 03:30:13 EST | 2023-11-26 03:30:13 EST | 2023-11-26 03:30:13 EST | 2023-1... |
| LINKBankStatementOct2023.xlsx | | | 0 | 2023-11-26 04:39:53 EST | 2023-11-26 04:39:53 EST | 2023-11-26 04:39:53 EST | 2023-1... |

| Strings | Extracted Text | Translation |
|-------------------|-------------------------------|-----------------|
| Page: 1 of - Page | Matches on page: - of - Match | 100% Reset |
| NYC Museum | Opening Balance: | 50,000.00 |
| NYC | Total Credit Amount: | 6,000.00 |
| NY 10016 | Total Debit Amount: | 7,750.00 |
| | Closing Balance: | 48,250.00 |
| | Account Type: | Current Account |
| | Number of Transactions: | 7 |

| Transactions | Date | Description | Credit | Debit | Balance |
|--------------|----------|-----------------------------|----------|----------|-----------|
| | 10/01/23 | Purchase Office Supplies | | 5,400.00 | 44,600.00 |
| | 10/05/23 | Donation Received | 3,000.00 | | 47,600.00 |
| | 10/10/23 | Utilities Payment | | 1,000.00 | 46,600.00 |
| | 10/11/23 | Membership Dues | | 800.00 | 45,800.00 |
| | 10/12/23 | Payment - Electricity | | 500.00 | 45,300.00 |
| | 10/13/23 | Payment - Water Utility | | 50.00 | 45,250.00 |
| | 10/20/23 | Exhibition Tickets Sale | 3,000.00 | | 48,250.00 |
| | | --- End of Transactions --- | | | |

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.

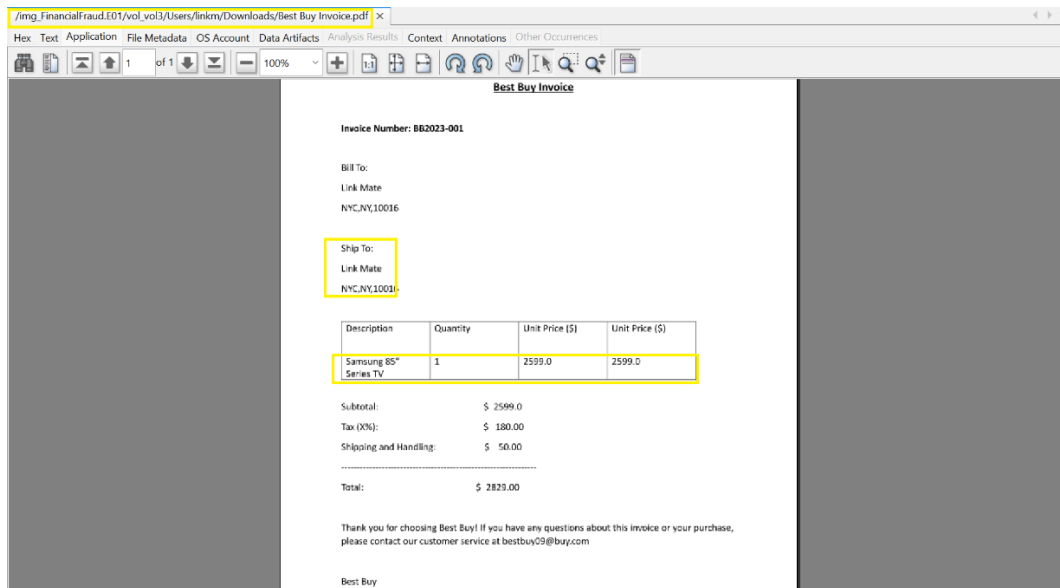


Figure 17 Invoice received from BestBuy

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.

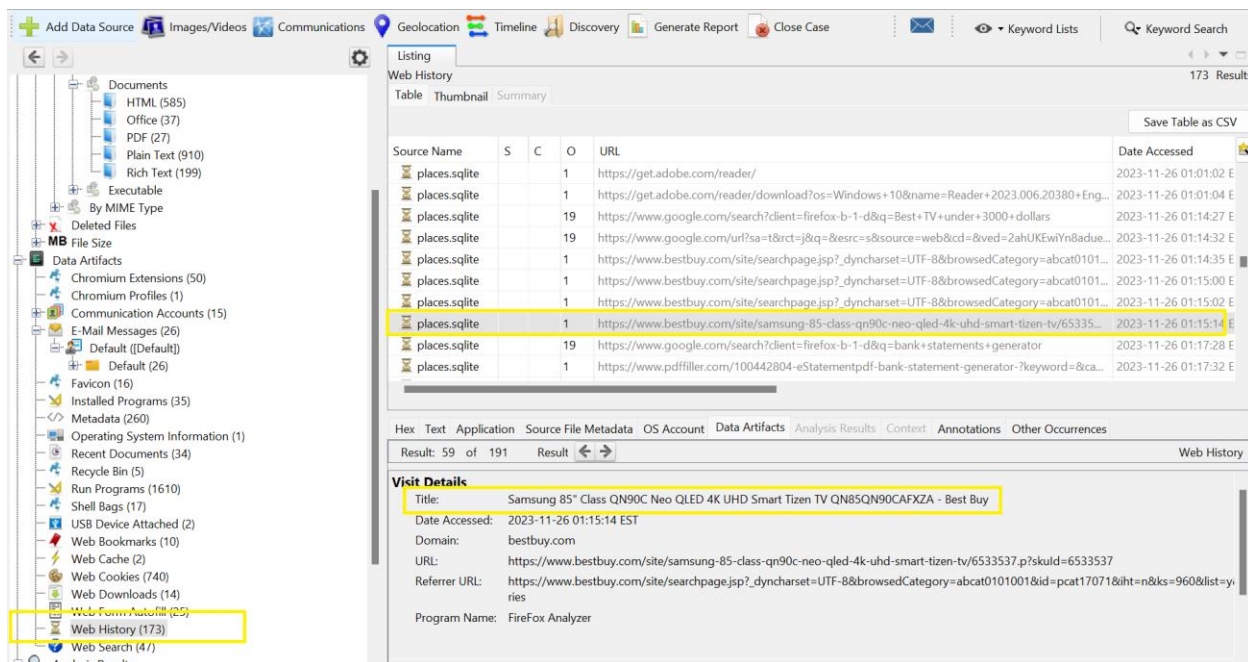


Figure 18 Web history related to best buy

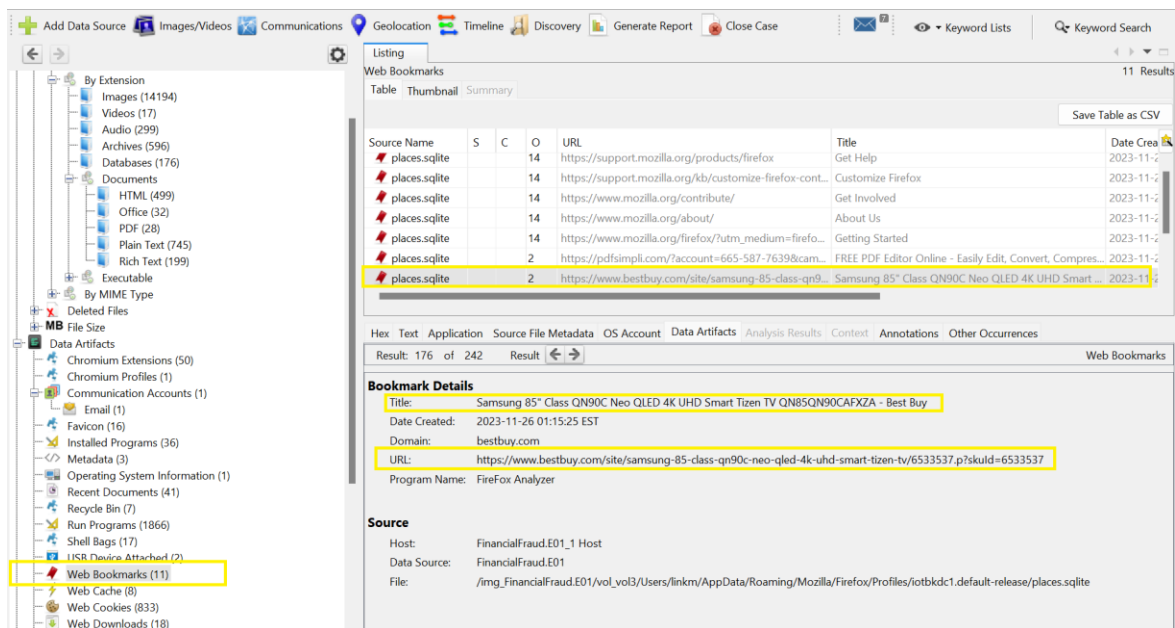


Figure 19 Bookmarks related to best buy

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.

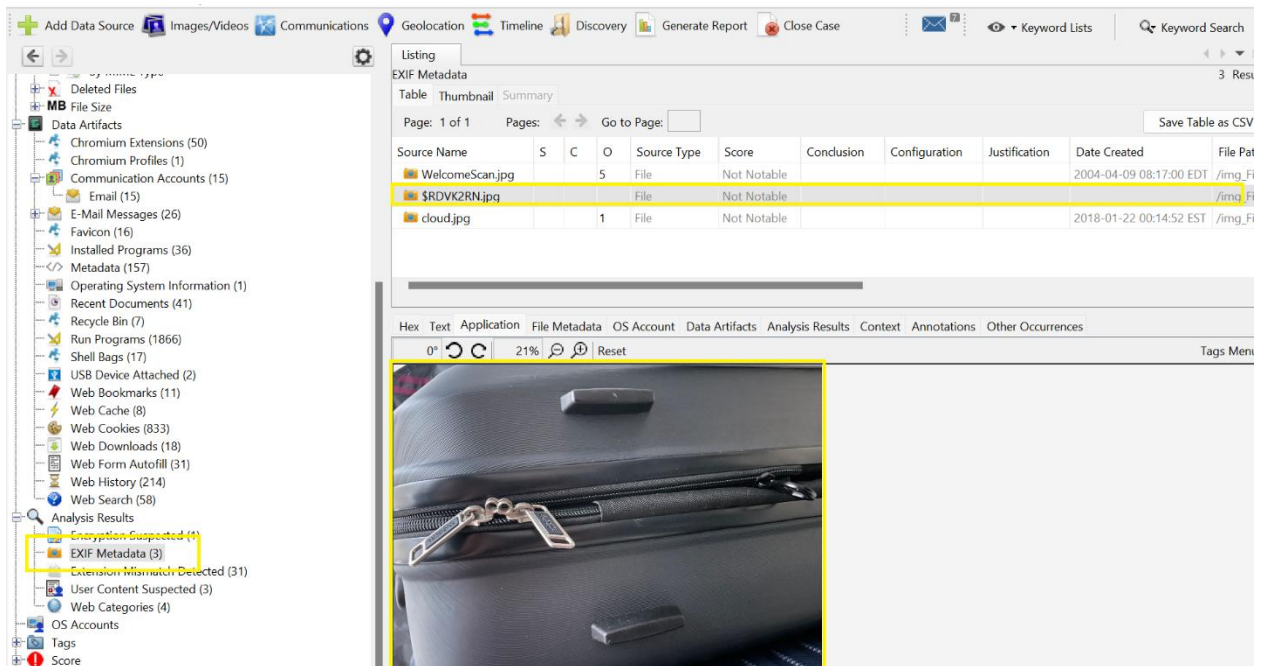


Figure 20 A suitcase picture found in EXIF Metadata

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.dupllichecker.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.

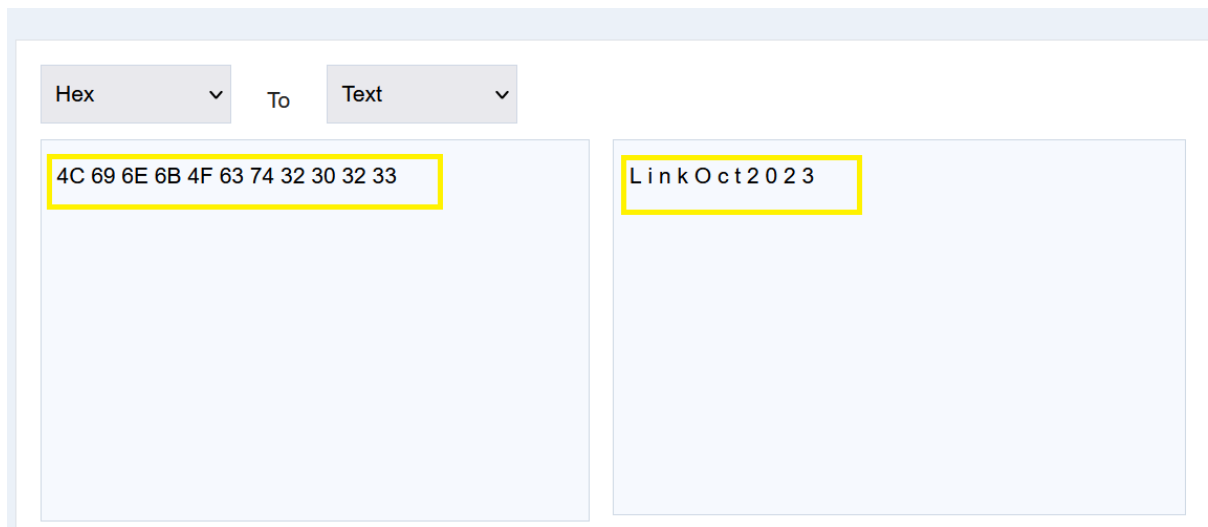


Figure 21 Hex to Text conversion

File Listing:

| Name | S | C | O | Modified Time | Change Time | Access Time | Created |
|---------------------------------------|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|
| 4C 69 6E 6B 4F 63 74 32 30 32 33.xlsx | | | | 2023-11-27 12:28:26 EST | 2023-11-27 14:30:27 EST | 2023-11-27 14:30:37 EST | 2023-11-27 14:30:37 EST |

File Details: 4C 69 6E 6B 4F 63 74 32 30 32 33.xlsx

Strings: Extracted Text

Page: 1 of 1

Matches on page: - of - Match

Text Source: File Text

Customer Information:

Link Mate
ADDRESS
90 Bedford Street, Corner Groove, NYC, NY, 10014-5304
2547-96574-2541-4004

Branch N

ACCOUNT NUMBER
1234567890

| OPENING BALANCE | PERIOD | PAGE | TOTAL CREDIT | TOTAL DEBIT | CLOSING BALANCE | 10/01/23 | 1 of 1 |
|-----------------|-----------|-------------------------|--------------|-------------|-----------------|-----------|--------|
| 10,895.92 | | 16,430.00 | 7,773.00 | 17,052.00 | | | |
| Date | Reference | Transaction Description | | | Credit | Debit | |
| 10/02/23 | 0302433 | Payroll | | 2,500.00 | | 13,395.00 | |
| 10/13/23 | 0302434 | Payroll | | 2,500.00 | | 15,895.00 | |
| 10/20/23 | 0302435 | Credit Card Payment | | | 1,430.00 | | |
| 17,325.00 | | | | | | | |
| 10/25/23 | 302436 | Deposit | | 10,000.00 | | 27,325.00 | |
| 10/26/23 | 302437 | AWOL Vision | | | 6,898.00 | 17,927.00 | |
| 10/27/23 | 302438 | American Airlines | | | | 575.00 | |
| 17,352.00 | | | | | | | |
| 10/28/23 | 302438 | Hotel | | | 300.00 | 17,052.00 | |

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.

Listing

Web Bookmarks 11 Results

Table Thumbnail Summary

Save Table as CSV

| Source Name | S | C | O | URL | Title | Date Created |
|---------------|---|---|----|---------------------------------------------------------|-----------------------------------------------------------|--------------|
| places.sqlite | | | 14 | https://www.mozilla.org/about/ | About Us | 2023-11-26 |
| places.sqlite | | | 14 | https://www.mozilla.org/firefox/?utm_medium=firefox... | Getting Started | 2023-11-26 |
| places.sqlite | | | 2 | https://pdfsimpli.com/?account=665-587-7639&cam... | FREE PDF Editor Online - Easily Edit, Convert, Compres... | 2023-11-26 |
| places.sqlite | | | 2 | https://www.bestbuy.com/site/samsung-85-class-qn90c... | Samsung 85" Class QN90C Neo QLED 4K UHD Smart ... | 2023-11-26 |
| places.sqlite | | | 2 | https://awolvision.com/products/awol-vision-ltv-3500... | Awol Vision 92"-120" 4K 3D Rollable Triple Laser TV L... | 2023-11-26 |

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 177 of 242 Result

Web Bookmarks

Bookmark Details

Title: Awol Vision 92"-120" 4K 3D Rollable Triple Laser TV LTV-3512R

Date Created: 2023-11-26 04:06:43 EST

Domain: awolvision.com

URL: https://awolvision.com/products/awol-vision-ltv-3500-vividstorm-floor-rising-screens-bundle?variant=40494287585328&gad_source=1&gclid=...

Program Name: Firefox Analyzer

Source

Host: FinancialFraud.E01_1 Host

Data Source: FinancialFraud.E01

File: /img_FinancialFraud.E01/vol_vol3/Users/linkm/AppData/Roaming/Mozilla/Firefox/Profiles/iotbkdc1.default-release/places.sqlite

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.

Listing
Web History
214 Results
Table Thumbnail Summary
Save Table as CSV

| Source Name | S | C | O | URL | Date Accessed | Referrer URL |
|---------------|---|---|----|-------------------------------------------------------|-------------------------|----------------------------------------|
| places.sqlite | | | 2 | https://www.aa.com/booking/choose-flights/1 | 2023-11-26 04:38:45 EST | https://www.aa.com/booking/search?loc |
| places.sqlite | | | 2 | https://www.aa.com/booking/find-flights | 2023-11-26 04:38:30 EST | https://www.aa.com/booking/choose-fli |
| places.sqlite | | | 2 | https://www.aa.com/booking/search?locale=en_US&f... | 2023-11-26 04:38:44 EST | https://www.aa.com/booking/find-flight |
| places.sqlite | | | 20 | https://www.google.com/search?client=firefox-b-1-d... | 2023-11-26 04:41:04 EST | |
| places.sqlite | | | 20 | https://www.google.com/url?sa=t&rct=j&q=&esrc=s&... | 2023-11-26 04:41:07 EST | https://www.google.com/search?client= |

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 134 of 242
Result
Web History

Visit Details

Title: American Airlines - Book flights
Date Accessed: 2023-11-26 04:38:44 EST
Domain: aa.com
URL: https://www.aa.com/booking/search?locale=en_US&fareType=Lowest&pax=1&adult=1&type=RoundTrip&searchType=Revenue&cabin=&carrier=7D%5D
Referrer URL: https://www.aa.com/booking/find-flights
Program Name: FireFox Analyzer

Source

Host: FinancialFraud.E01_1 Host
Data Source: FinancialFraud.E01
File: /img_FinancialFraud.E01/vol_vol3/Users/linkm/AppData/Roaming/Mozilla/Firefox/Profiles/iotbkdc1.default-release/places.sqlite

Figure 24 American Airlines flight Web Search

New York, NY to Orlando, FL
Monday, December 25, 2023
Lowest fare Flexible
Fri, Dec 22 \$596 Sat, Dec 23 \$596 Sun, Dec 24 \$511 Mon, Dec 25 \$575 Tue, Dec 26 \$647 Wed, Dec 27 \$576 Thu, Dec 28 \$507
Filter by: Stops American Airlines Nearby airports 40 results
Depart 6:30 AM Arrive 10:55 AM Duration 4h 25m 1 stop
JFK - CLT - AA 2643 - 738-Boeing 737
Main Cabin First
Round trip \$635
Activate Windows Go to Settings to activate Windows. \$1,081

Ticket Search.JPG (1 of 3 in group)

Ticket Search.JPG
Analyzed: true
Category:
Tags:
Path: /img_FinancialFraud.E01/vol_vol3/Users/linkm/Pictures/
Created Time: 2023-11-26 04:40:4 EST
Modified Time: 2023-11-26 04:40:4 EST
MD5 Hash: 3862b08e0ab987f5a0f0291972f14e8
Hashset:
Camera Make:

Figure 25 Flight search image

- The other transaction found in the bank statement is hotel and a web search related to the hotels in Orlando, Florida is found.

Listing

Web History 214 Results

Table Thumbnail Summary

Save Table as CSV

| Source Name | S | C | O | URL | Date Accessed | Referrer URL |
|---------------|---|---|----|---------------------------------------------------------|-------------------------|-----------------------------------------|
| places.sqlite | | | 15 | https://mail-attachment.googleusercontent.com/attach... | 2023-11-27 11:09:17 EST | https://mail.google.com/mail/u/0/#inbox |
| places.sqlite | | | | file:///C:/Users/linkm/Downloads/Best%20Buy%20Inv... | 2023-11-27 11:09:39 EST | |
| places.sqlite | | | 20 | https://www.google.com/search?client=firefox-b-1-d... | 2023-11-27 11:37:38 EST | |
| places.sqlite | | | 20 | https://www.google.com/search?client=firefox-b-1-d... | 2023-11-27 11:37:43 EST | https://www.google.com/search?client= |
| places.sqlite | | | 20 | https://www.google.com/search?client=firefox-b-1-d... | 2023-11-27 11:37:47 EST | https://www.google.com/search?client= |

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 148 of 242 Result

Web History

Visit Details

Title: hotels in orlando fl - Google Search

Date Accessed: 2023-11-27 11:37:47 EST

Domain: google.com

URL: https://www.google.com/search?client=firefox-b-1-d&sca_esv=585652102&sxsrf=AM9HkKmwgw2Oq5xLs0oGqUt1g8A65MAjpA:170110306025iM

Referrer URL: https://www.google.com/search?client=firefox-b-1-d&sca_esv=585652102&sxsrf=AM9HkKmwgw2Oq5xLs0oGqUt1g8A65MAjpA:170110306025

Program Name: FireFox Analyzer

Source

Host: FinancialFraud.E01_1 Host

Data Source: FinancialFraud.E01

File: /img_FinancialFraud.E01/vol_vol3/Users/linkm/AppData/Roaming/Mozilla/Firefox/Profiles/iotbkdc1.default-release/places.sqlite

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.

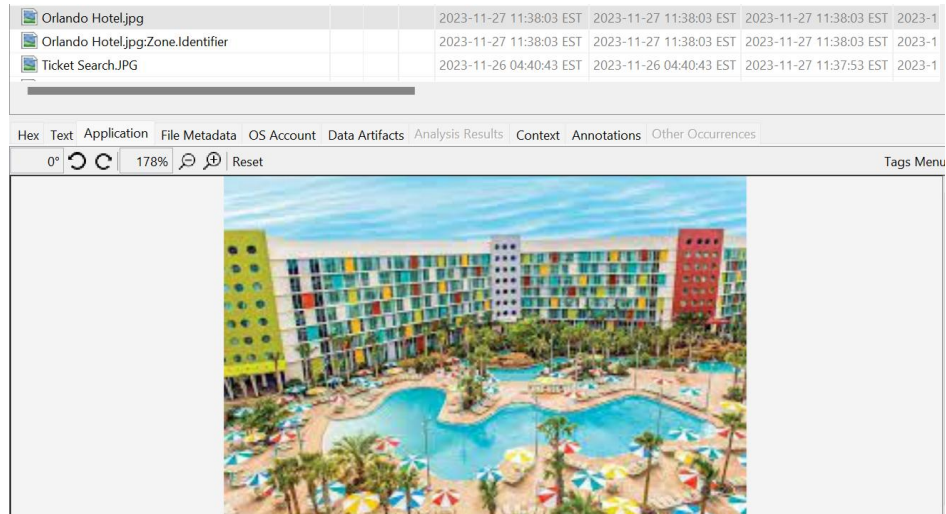


Figure 27 Hotel image 1

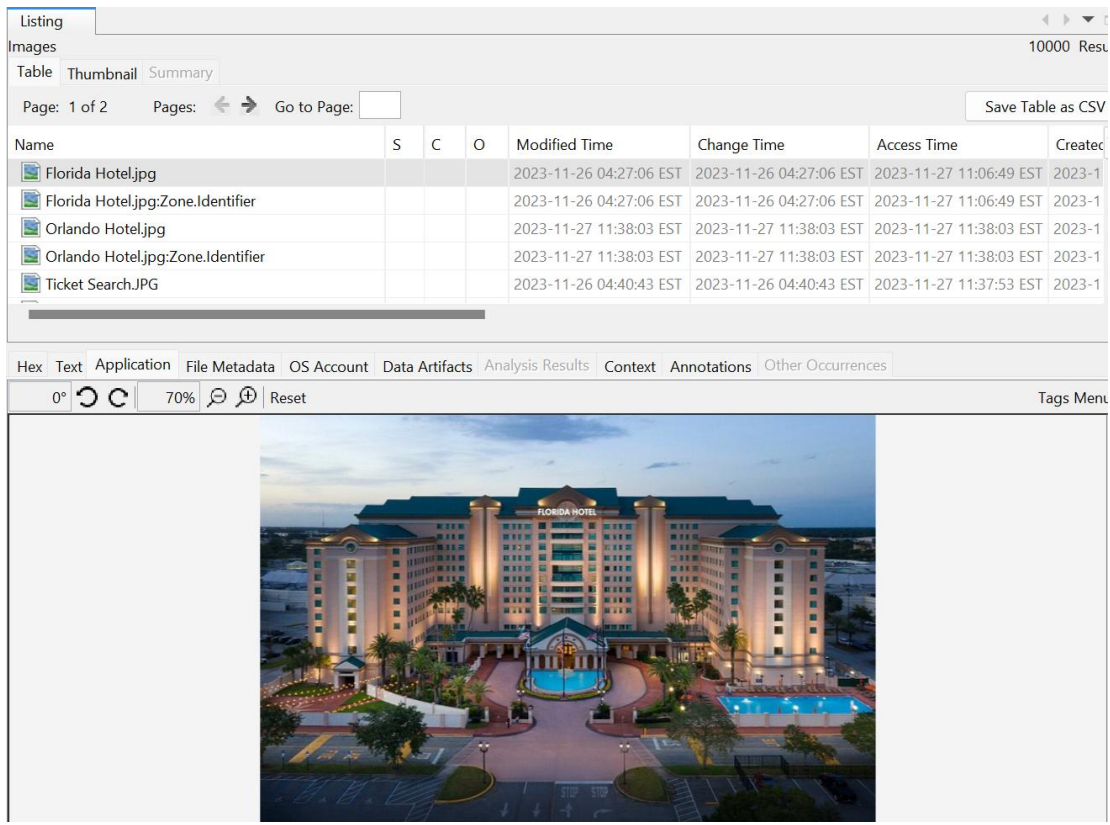


Figure 28 Hotel Image 2

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 **65d52d66f22adbf13e989da76bccc81** . The hash value obtained after completion of exam is same as the hash value obtained before starting the examination.

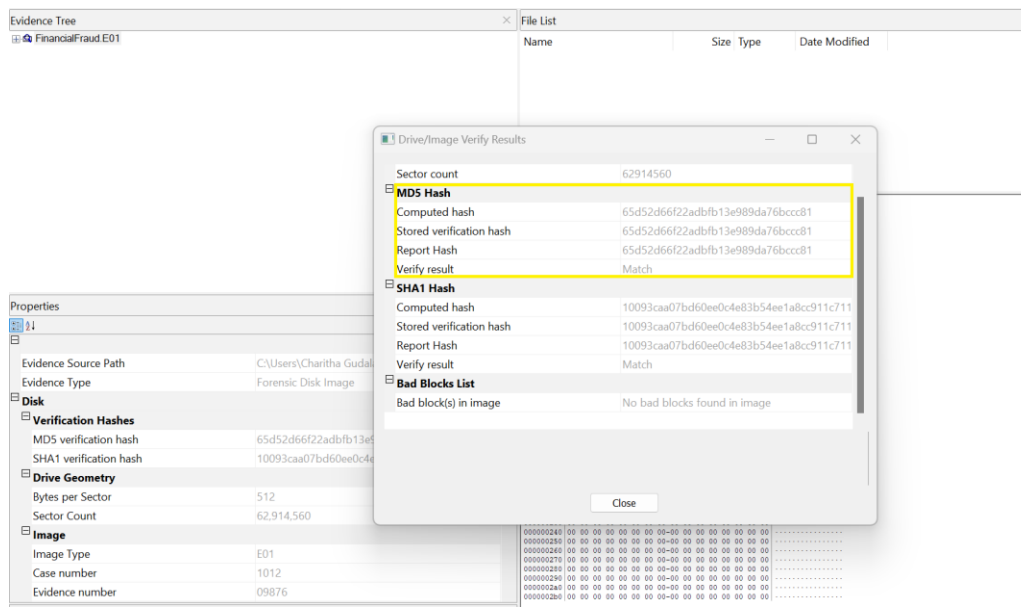


Figure 29 Reverifying the image FinancialFraud.E01 hash

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.