



Cybersecurity

## 21.3 The Final Report

# Case Report

## Pure Gold Credit Union

# Table of Contents

---

[Case Report](#)

[Pure Gold CU](#)

[Peter's iPhone](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Peter's iPhone](#)

[Evidence to Establish Personas](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: GPS Location Information](#)

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist Pure Gold Credit Union (PGCU) case involving the conspiracy associated with the theft of funds.

- Peter is a suspect in the aforementioned conspiracy.
- As part of the investigation, Peter's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

### Executive Summary

On January 21, 2016, Digitech Inc. was engaged to assist Pure Gold Credit Union (PGCU) in investigating a conspiracy related to the theft of funds. The primary suspect in this case was Peter Barnes, the Lead Teller at PGCU. As part of the investigation, Peter's iPhone was confiscated for evidence examination. Digitech Inc. was tasked with analyzing the data to uncover evidence tied to the theft and fraud.

Further investigation revealed that Peter Barnes, along with Rosie Lloyd, the Financial Advisor, and Oliver Bell, the District Manager, were involved in the conspiracy. Oliver Bell, who was referred to as "Mr. X" in email communications, was identified as the ringleader behind the fraudulent activities. The collaboration among these individuals led to a significant breach of trust and financial misconduct within PGCU. Digitech Inc.'s role was crucial in uncovering the key evidence necessary to resolve this case and hold those responsible accountable.

## Equipment and Tools

To gather and analyze evidence in the investigation, several tools and equipment were used:

1. **Autopsy:** A digital forensics platform used to conduct a thorough analysis of the suspect's devices, including extracting and examining data from the iPhones of Peter Barnes and Rosie Lloyd (serial numbers: [Peter's iPhone Serial Number], [Rosie's iPhone Serial Number]).
2. **Kali Linux:** A powerful operating system with specialized security tools for digital forensics, utilized to conduct deep system scans, data recovery, and identify any hidden or encrypted files.
3. **SQLite Browser:** Used for viewing and analyzing SQLite database files, helping to examine data stored on mobile devices and other electronic evidence.
4. **iPhones:** The confiscated iPhones of Peter Barnes sr.no. FFNHHK2RPLJM and Rosie Lloyd sr. no. FFPHG1LYPLJM were critical for examining communications, app data, and files that could provide evidence of their involvement in the conspiracy.
5. **Firefox:** Employed to access and investigate online accounts, communications, and other web-based evidence such as email logs or browsing history.

6. **VLC:** Used for reviewing voicemail recordings, ensuring any voice messages related to the case were accurately analyzed.
7. **Gmail:** Investigated to uncover email communications and potential evidence linking the suspects, particularly messages involving "Mr. X," the ringleader.

These tools, along with the detailed analysis of the confiscated iPhones, allowed for a comprehensive investigation, uncovering crucial evidence tied to the conspiracy.

## Details of Peter's iPhone

### Details of Peter's iPhone

Name	Findings	Location/File in iPhone image file
Model	Iphone12,8 or just iphone12 SE	activation_record.plist
Host Name	Peter's iphone	data_ark.plist
OS Version	V16.5.1	data_ark.plist
User Email	Peterbarnes12792@icloud.com	Protected Index and also from SMS and from partial.emlx of any message
Phone Number	+16155719608	CellularUsage.db and confirmed from SMS etc.
Serial Number	FFNHHK2RPLJM	activation_record.plist
ICCID	89148000009489719791	activation_record.plist
IMEI	311480010283519	activation_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Run on the zip file PeteriphoneImage.zip in kali
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb	Run on the zip file

	534ca0d1e83ffd27683e621607	PeteriohoneImage.zip in kali
--	----------------------------	---------------------------------

## Details of Rosie's iPhone

### Details of Rosie's iPhone

Name	Findings	Location/File in iPhone image file
Model	Iphone12,8 or just iphone12 SE	activation_record.plist
Host Name	Rosie's iphone	data_ark.plist
OS Version	T16.5	data_ark.plist
User Email	Rosielloyd071292@icloud.com	Protected Index and also from SMS and from partial.emlx of any message
Phone Number	+16154278267	CellularUsage.db and confirmed from SMS etc.
Serial Number	FFPHG1LYPLJM	activation_record.plist
ICCID	89148000009489732844	activation_record.plist
IMEI	311480010308141	activation_record.plist
MD5 Hash	e666cd1232ead8f76c0a42910f54b7d5	Run on the zip file RosieiphonelImage.zip in kali
SHA256 Hash	0aa14fa06a416fd59c1e6586c888dd3511b1a98c7a01915233181866bedd7671	Run on the zip file RosieiphonelImage.zip in kali

## Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Peter:

Phone Number: +16155719608

Email: Peterbarnes12792@icloud.com

Relationship: Accused (Lead Teller)

Rosie:

Phone Number: +16154278267

Email: Rosielloyd071292@icloud.com

Relationship: Accomplice (Financial Advisor)

Oliver Bell District Manager – Ring Leader (clearly established from emails and voice mail files obtained from the phones of Peter and Rosie both, VM was from Oliver). Oliver is Mr. X.

Phone Number: +16158070242 (obtained from voicemail.db in the sqlitebrowser)

Others named in the emails of Peter and Rosie were Michael Rokas, Catarina Mona and Lanzo Agneza but no direct link can be established between, to or from them from the provided image files PeteriphonelImage.zip and RosieiphonelImage.zip.

The investigation revealed clear involvement of Peter Barnes, Rosie Lloyd, and Oliver Bell in the financial theft conspiracy. Peter, the Lead Teller, and Rosie, the Financial Advisor, were directly implicated, with evidence showing their participation in the fraudulent activities. Oliver Bell, the District Manager, was identified as the ringleader, based on email communications and a voicemail retrieved from both Peter and Rosie's phones.

Oliver's voicemail, retrieved from the PeteriphonelImage.zip and RosieiphonelImage.zip, explicitly referenced the stolen funds and his involvement in covering up the fraud. He stated, "hi peter it's your buddy Oliver, from my math you and Rosie have queered over 125k. remember though I get 20% and i keep clearing the audit record so that Evelyn can never catch you. Give me my cash though put it in an envelope and put it at my backdoor. Pleasure doing business with you." This statement directly ties Oliver to the scheme, offering clear evidence of his role as the mastermind.

Despite mentions of other individuals like Michael Rokas, Catarina Mona, and Lanzo Agneza in emails, no direct link or evidence of participation was found w.r.t. these individuals from the provided image files.

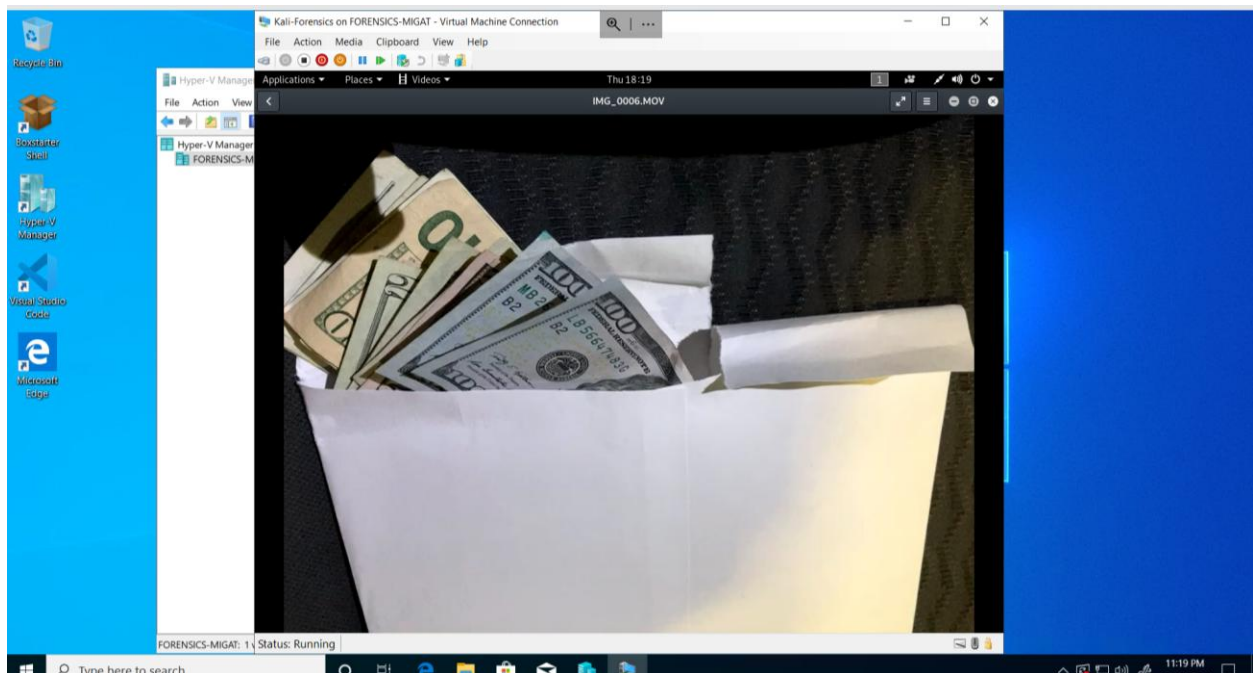
## Evidence relating to theft of PGCU funds

This sub-section provides details regarding the evidence found as it relates to the theft of funds

Extracted IMG-0006.mov file from Peter's phone shows currency some have bill serials visible

File was run in Kali >>xdg-open IMG-0006.MOV

Serial numbers of certain bills are visible and can be checked against the currency database for theft validation.



## Plot Timeline

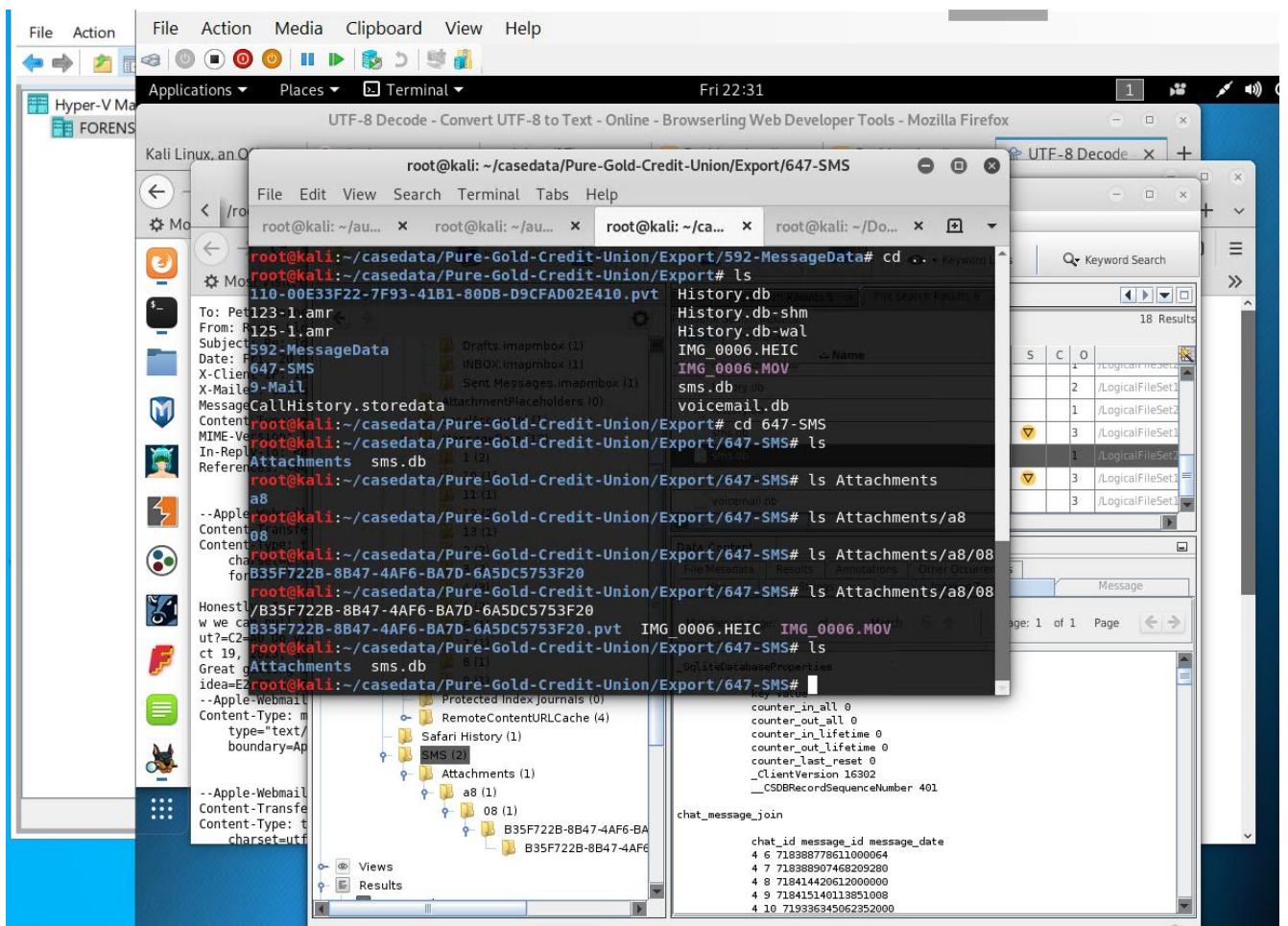
### [Correspondence Evidence

Group members:

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1		Video	Stolen currency picture	IMG-0006.MOV obtained from SMS attachments. See pic below
2	Saturday Oct 21, 2023 12:57:04 AM	GPS data	GPS data indicating Location	IMG-0006.HEIC obtained from SMS attachments, see pic below for exact location
3	Sunday Oct 25, 2023 6:36:50 PM	Voice Mail	This voicemail found on both Peter and Rosie's phones reveals Oliver Bell in the background of this fraud and indicates his ties to Peter and Rosie, it also reveals him possibly being the mastermind. More than 125k stolen.	123-1.amr 125-1.amr
4	Oct 20, 2023 02:11:14 (UTC)	Email, header in pic below	This email shows both Peter and Rosie plan and	9-Mail extracted from Peter's phone. Email



			talk about hidden Mr. X later found to be Oliver. It also indicates that Mr. X (Oliver) is the mastermind.	location in pic under this artifact and remaining are similar. Only this shown
5	oct 20, 2023 02:33:47 (UTC) Rosie to Peter email	Email, header in pic below	This email shows Rosie's intent to commit money fraud in association with Peter and Mr. X (Oliver Bell). Email obtained from Rosie's phone via extraction 592-MessageData	extraction 592-MessageData see pic below for artifacts 1 thru 4 above.
6	Various	SMS	SMS messages indicating meeting between Peter and Rosie. but nothing significant other than meeting but VM by Oliver and other attachments such as currency video and GPS information were significant	647-SMS and sms.db, see pic below
7	Oct 12, 2023 22:59:41 (UTC)	2 Emails, back and forth Peter and Rosie, header can be seen in picture below.	Peter and Rosie Met	9-Mail extracted from Peter's phone.

Artifacts 1 thru 4 shown as files and directories above, below pics in sequence, pls note only those artifacts are being included which represent a clear cut milestone.

## Artifact1

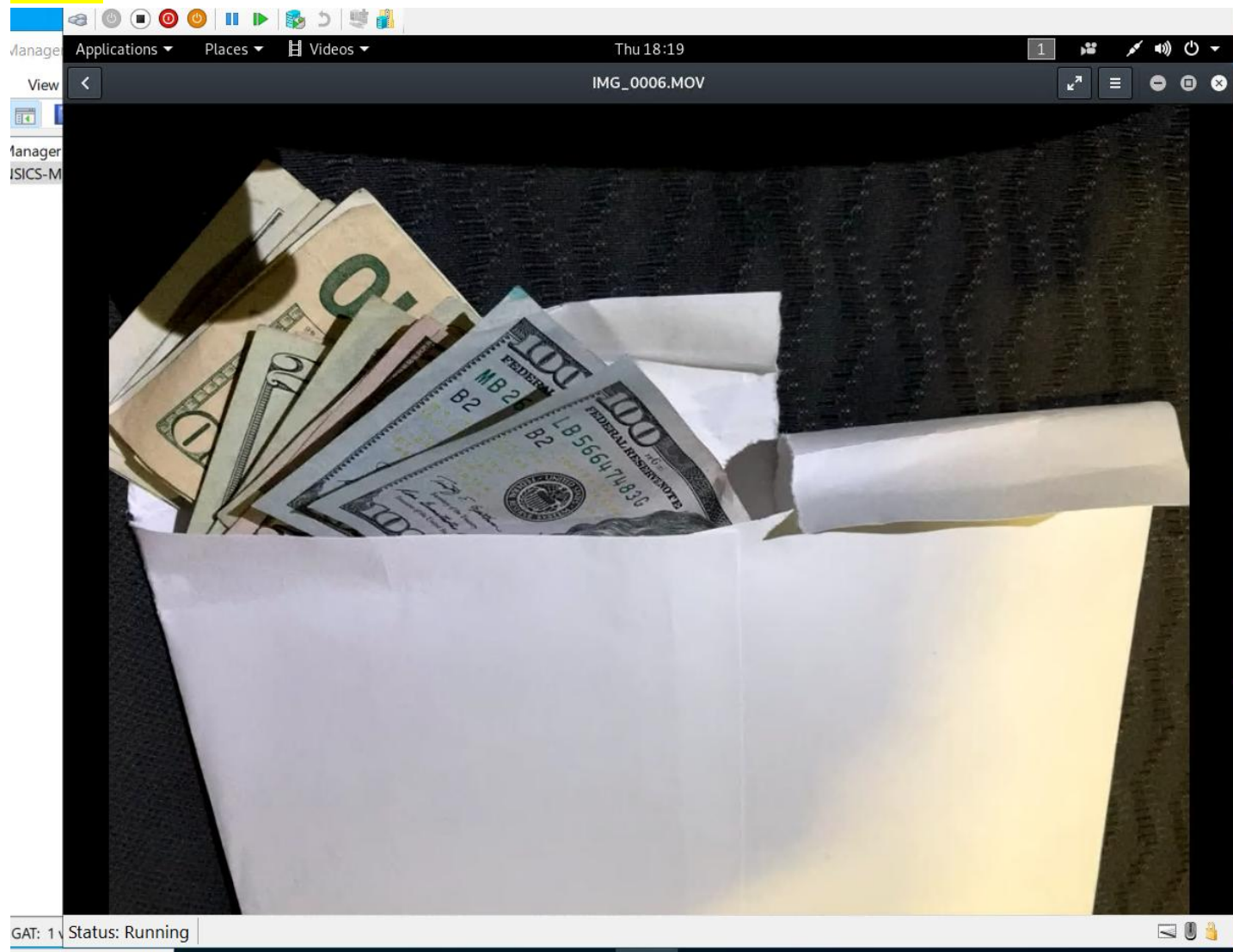


Table: message

Filter	Filter
+16155719...	0
+16155719...	0
+16155719...	0
+16155719...	0
+16155719...	0
+16155719...	0
+16155719...	0
+16155719...	0

Pure-Gold-Credit-Union - Autopsy 4.10.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Keyword Lists Keyword Search

Directory Tree

- Data Sources
  - LogicalFileSet1 (1)
  - PeteriPhoneImage (7)
  - LogicalFileSet2 (1)
- Views
- Results
  - Extracted Content
  - Keyword Hits
    - Single Literal Keyword Search (1)
    - Single Regular Expression Search (0)

File Search Results 2

Name	S	C	O	Location
MG_0006.MOV			3	/LogicalFileSet1/PeteriPhoneImage/SMS/Attachments/33/0...
MG_0006.MOV			3	/LogicalFileSet1/PeteriPhoneImage/SMS/Attachments/33/0...
MG_0006.MOV			1	/LogicalFileSet2/RosiePhoneImage/SMS/Attachments/a8/0...
MG_0006.MOV			1	/LogicalFileSet2/RosiePhoneImage/SMS/Attachments/a8/0...

## Artifact2

Online EXIF Viewer - View EXIF Data Online - Mozilla Firefox


https://onlineexifviewer.com

Camera Make and Model

Apple - iPhone SE (2nd generation)

Camera Location Details

Photo GPS Location: [35.97045,-86.8073888888888](#)



All Photo EXIF Data

Save & Share EXIF

Hide Serial Numbers

Make	Apple
Model	iPhone SE (2nd generation)
Orientation	bottom-right
XResolution	72
YResolution	72
ResolutionUnit	inches
Software	16.5
DateTime	2023:10:20 19:53:39
HostComputer	iPhone SE (2nd generation)
TileWidth	512
TileLength	512
Exif IFD Pointer	274

Online EXIF Viewer - View EXIF Data Online - Mozilla Firefox

https://onlineexifviewer.com

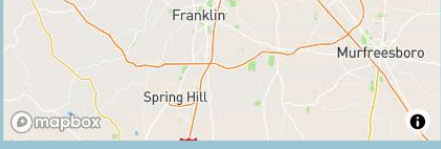
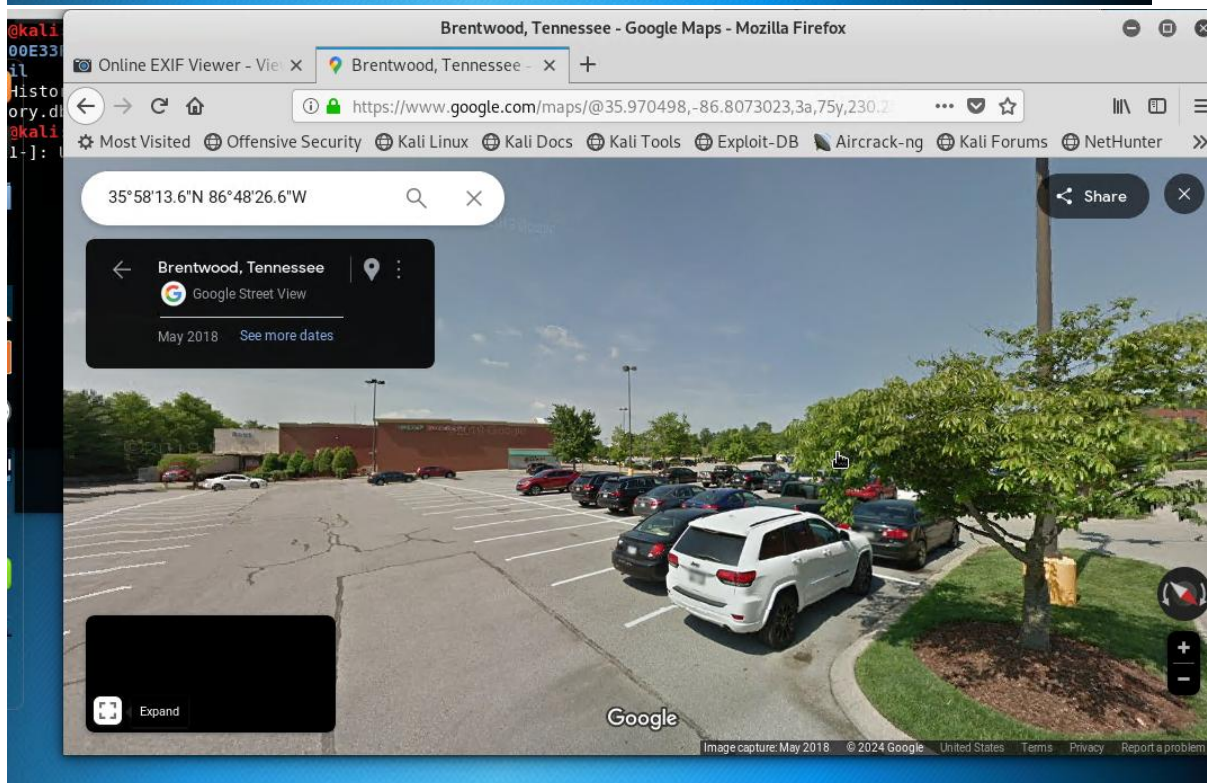
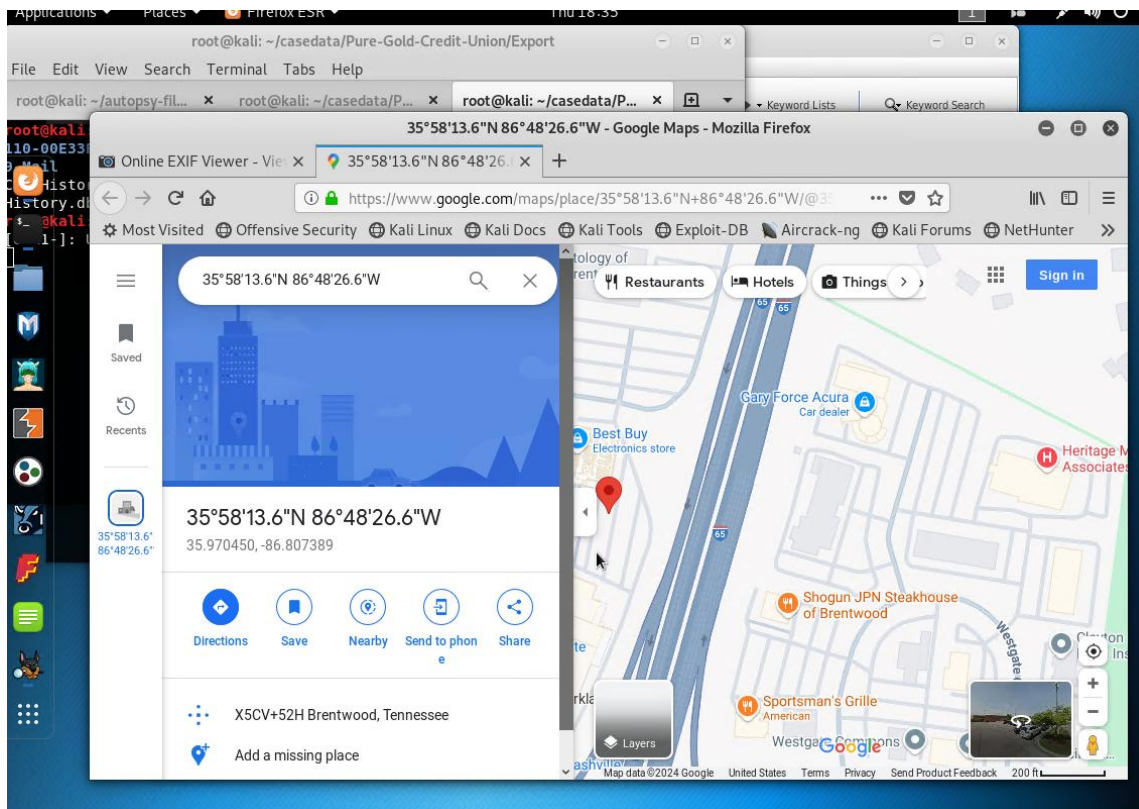


Image Preview

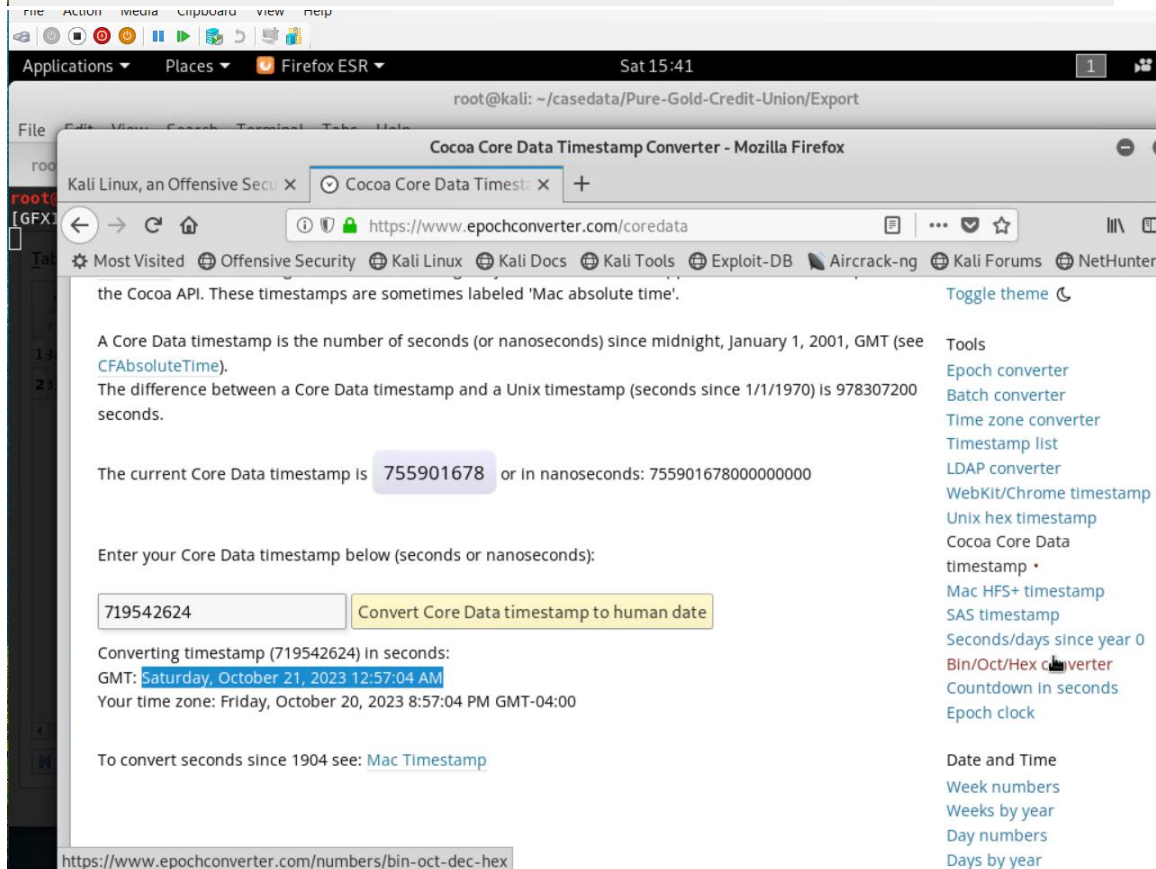
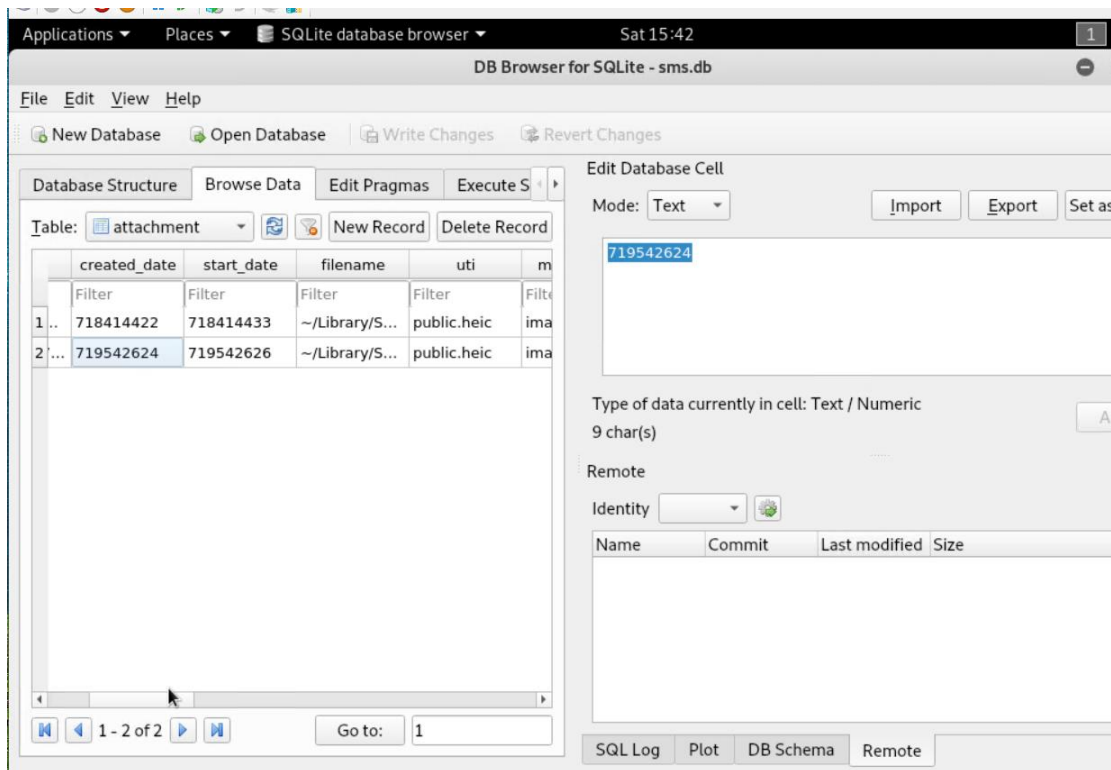
Preview not available

HostComputer	iPhone SE (2nd generation)
TileWidth	512
TileLength	512
Exif IFD Pointer	274
GPS Info IFD Pointer	2148
ExposureTime	1/46
FNumber	f/1.8
ExposureProgram	Normal program
ISOSpeedRatings	320
ExifVersion	0232
DateTimeOriginal	2023:10:20 19:53:39
DateTimeDigitized	2023:10:20 19:53:39
OffsetTime	-05:00
OffsetTimeOriginal	-05:00
OffsetTimeDigitized	-05:00
ShutterSpeedValue	1/46





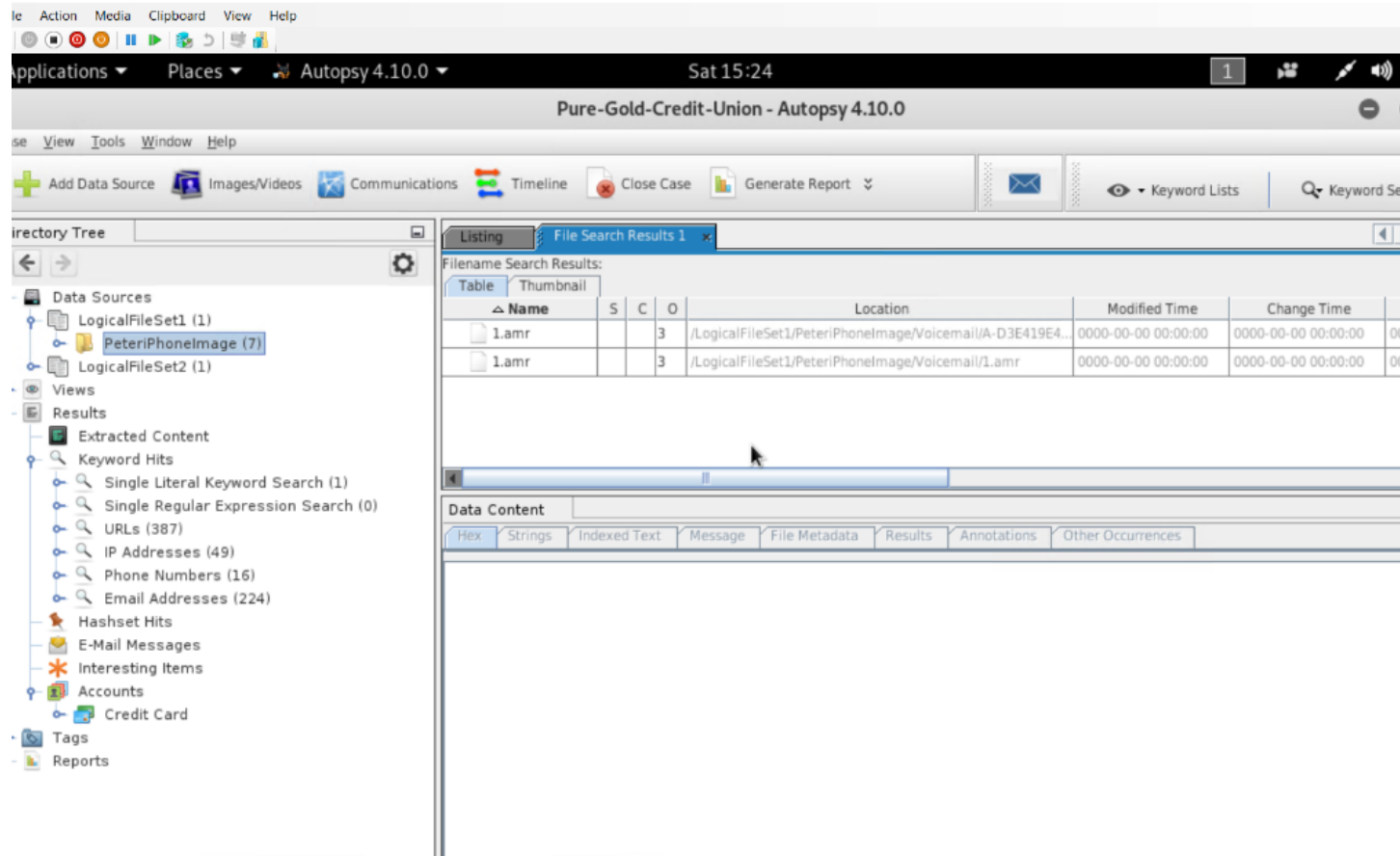
Artifact2 time conversion below Saturday Oct 21, 2023 12:57:04 AM



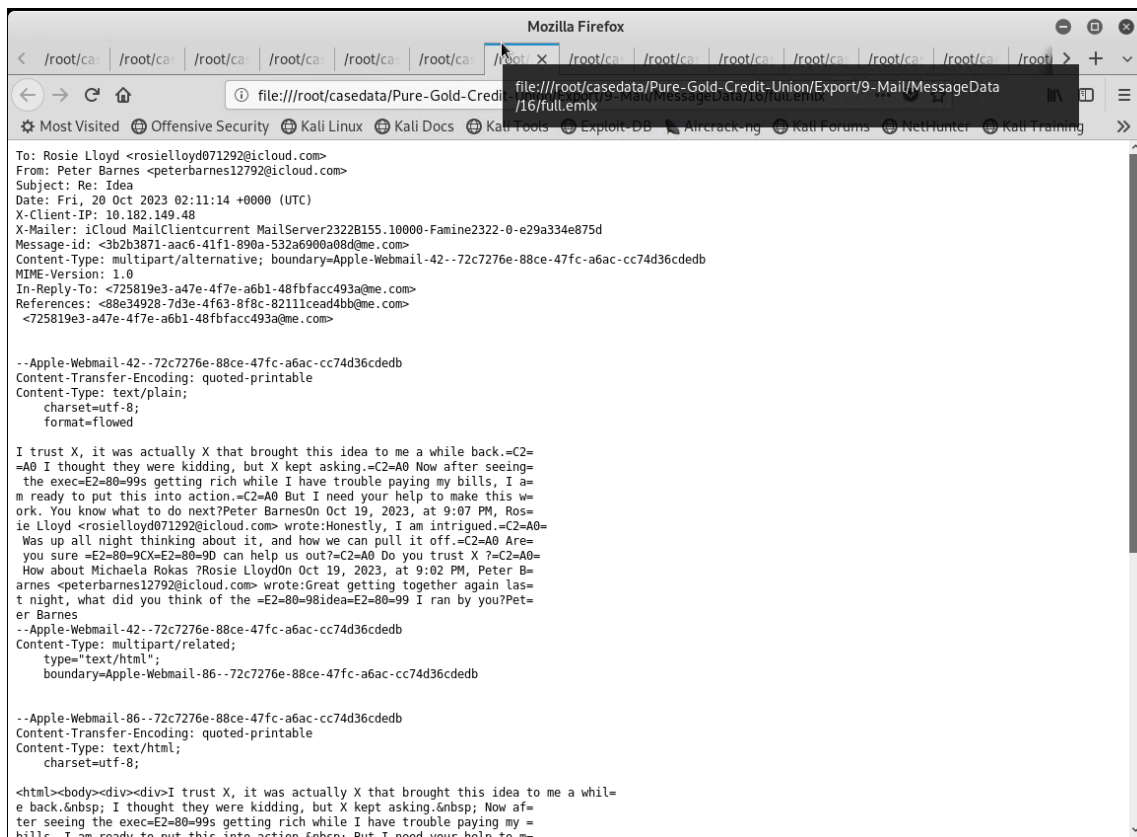
### Artifact3

Oliver's VM left for Peter stated "hi peter it's your buddy Oliver, from my math you and Rosie have queered over 125k. remember though I get 20% and i keep clearing the audit record so that Evelyn can never catch you. Give me my cash though put it in an envelope and put it at my backdoor. Pleasure doing business with you."

Exact location of artifact3 is in below pic



Artifact4 To Rosie from Pater Barnes



Email location for this one shown below



DB Browser for SQLite - sms.db

File Edit View Help

root@kali: ~/casedata/Pure-Gold-Credit-Union/Export/9-Mail/MessageData

File Edit View Search Terminal Tabs Help

root@kali:~/casedata/Pure-Gold-Credit-Union/Export/9-Mail/MessageData# ls

```
4E6A2774-1647-484D-8321-E8379D7AAE70  MessageData
AttachmentPlaceholders                metadata.plist
AutoFetchEnabled                      'Protected Index'
'Envelope Index'                      'Protected Index Journals'
'Envelope Index-shm'                  'Protected Index-shm'
'Envelope Index-wal'                  'Protected Index-wal'
LocalAccountId                        RemoteContentURLCache currently in cell: NULL
MailboxCollections.plist              VIPs.plist 0 byte(s)
```

root@kali:~/casedata/Pure-Gold-Credit-Union/Export/9-Mail/MessageData# cd MessageData

bash: cd: MessageData: No such file or directory

root@kali:~/casedata/Pure-Gold-Credit-Union/Export/9-Mail/MessageData# cd MessageData

bash: cd: MessageData: No such file or directory

root@kali:~/casedata/Pure-Gold-Credit-Union/Export/9-Mail/MessageData# ls

```
1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 3 4 5 6 7 8 9
2.emlxpart partial.emlx
```

root@kali:~/casedata/Pure-Gold-Credit-Union/Export/9-Mail/MessageData#

Database Structure Browse Data Edit Pragma Execute SQL

Table: attachment

user_info	transfer_name	total_bytes	is_stick
Filter	Filter	Filter	Filter

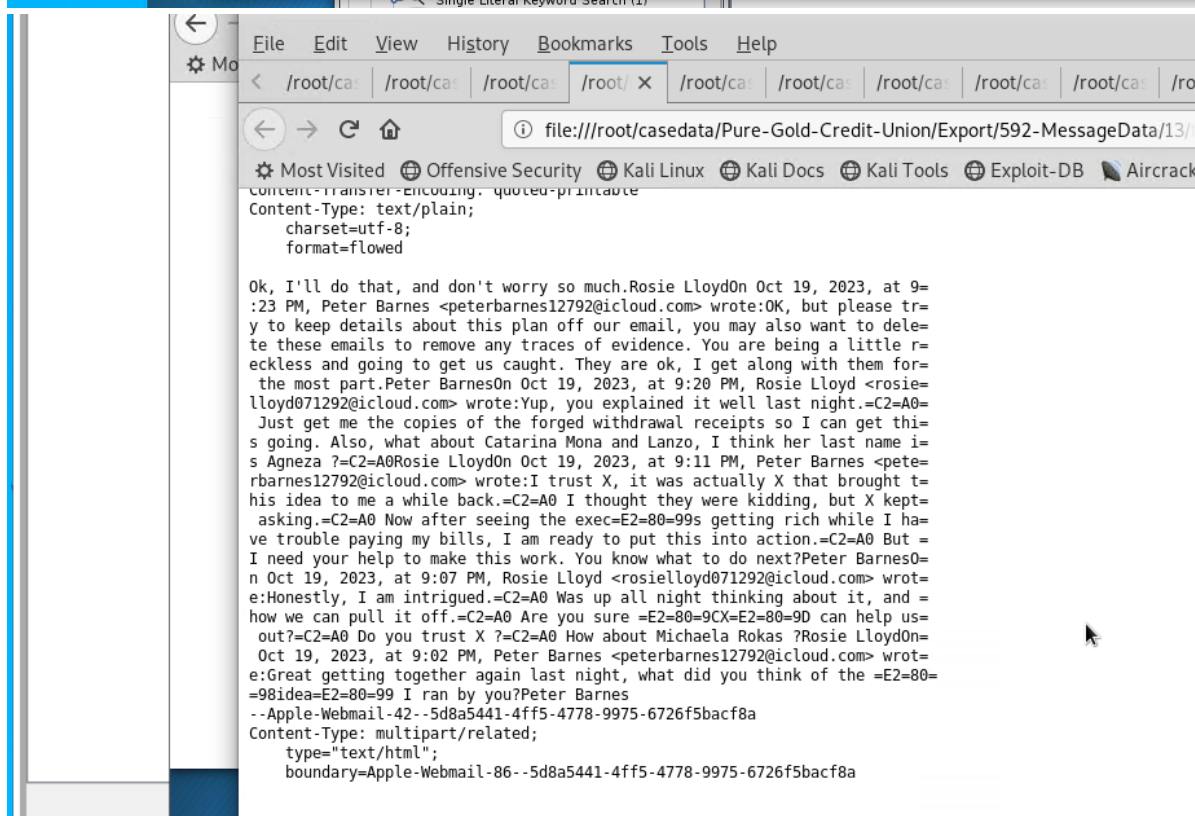
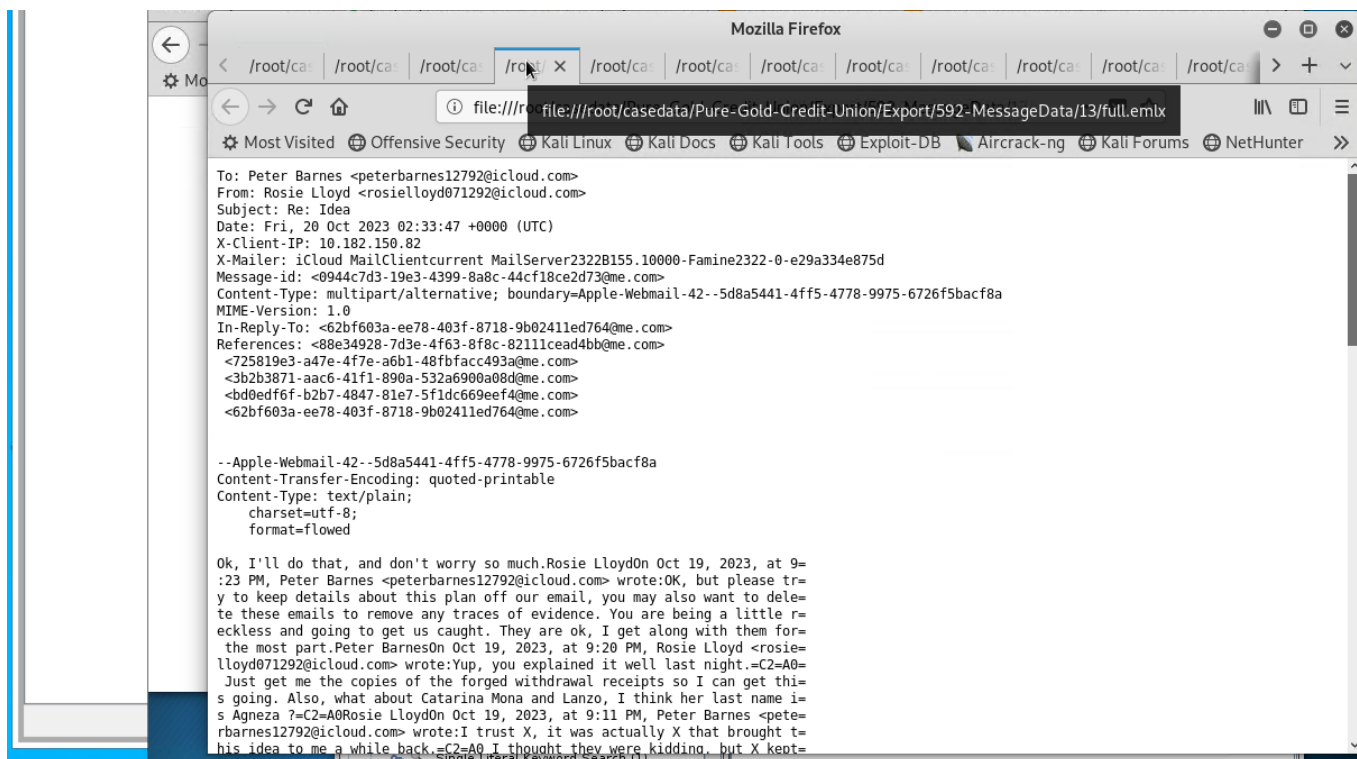
Edit Database Cell

Mode: Text

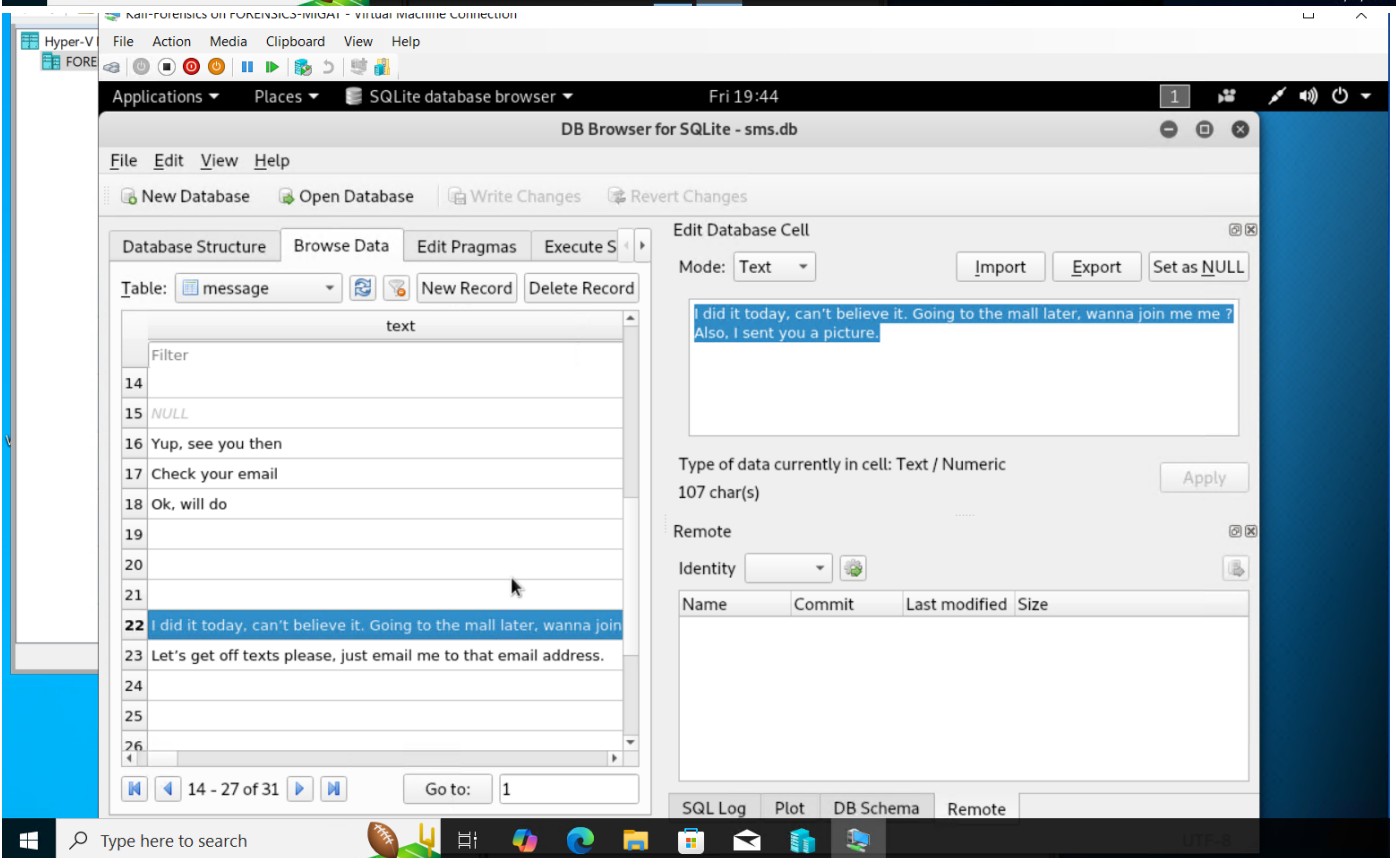
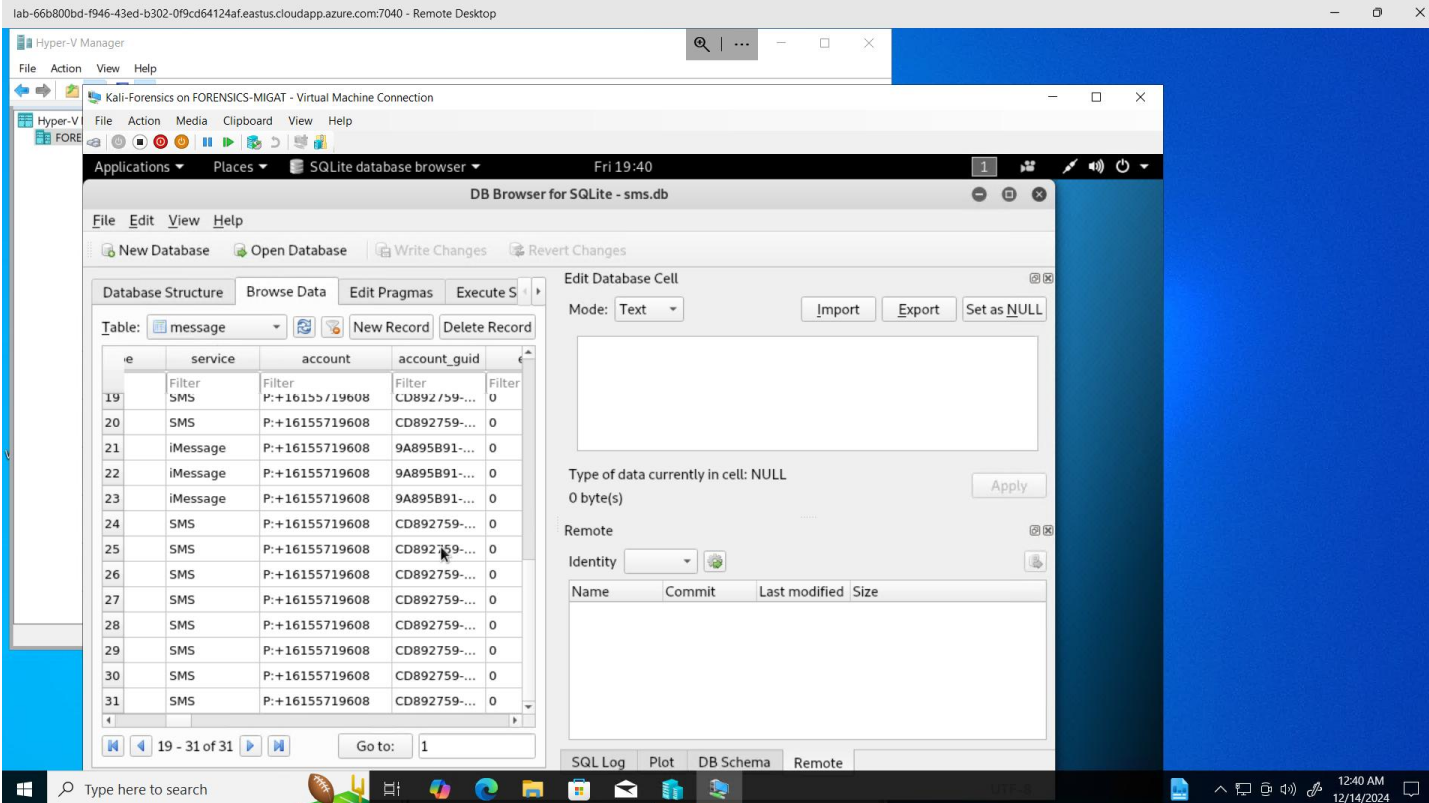
Import Export Set as NULL

IMG\_0006.HEIC

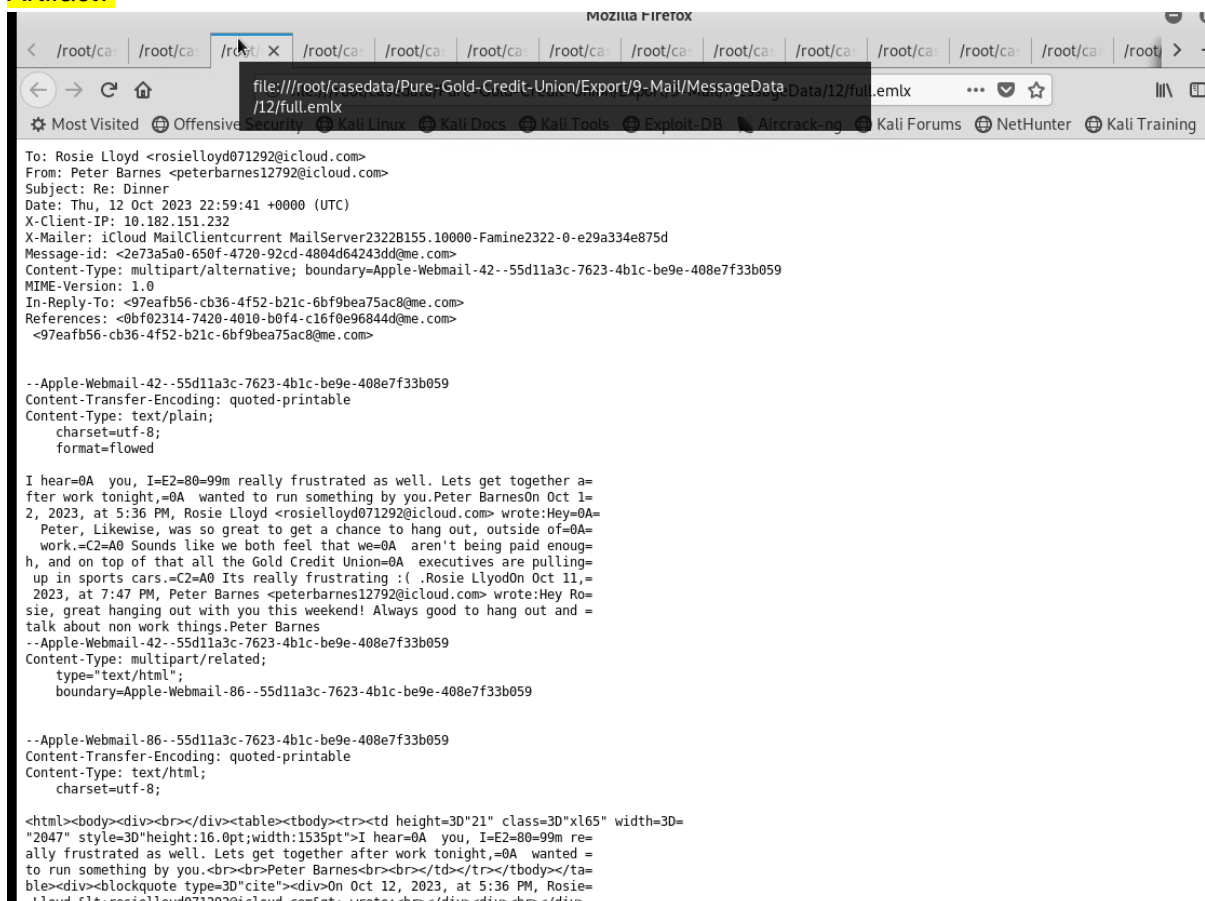
Artifact5



Artifact6



## Artifact7



```

Hey Rosie, great hanging out with you this weekend! Always good to hang out
and talk about non work things. Peter Barnes
--Apple-Webmail-42--af5c1a72-2ad2-4655-8864-13068ebbc066
Content-Type: multipart/related;
    type="text/html";
    boundary=Apple-Webmail-86--af5c1a72-2ad2-4655-8864-13068ebbc066

--Apple-Webmail-86--af5c1a72-2ad2-4655-8864-13068ebbc066
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
    charset=utf-8;

<html><body><div><br></div><table><tbody><tr><td height=3D"21" class=3D"xl65" width=3D=
"2047" style=3D"height:16.0pt;width:1535pt">Hey=0A Peter, <br><br>Likewis=
e, was so great to get a chance to hang out, outside of=0A work.<span sty=
le=3D"mso-spacerun:yes">&nbsp; </span>Sounds like we both feel that we=0A =
aren't being paid enough, and on top of that all the Gold Credit Union=0A=
executives are pulling up in sports cars.<span style=3D"mso-spacerun:yes=
">&nbsp; </span>Its really frustrating :( .<br><br>Rosie Llyod<br><br></td>
</tr></tbody></table><div><blockquote type=3D"cite"><div>On Oct 11, 2023,=
at 7:47 PM, Peter Barnes <mailto:peterbarnes12792@icloud.com> wrote:<br></=
div><div><br></div><div><br></div><div><br></div><div>Hey Rosie, great hanging out w=
ith you this weekend! Always good to hang out and talk about non work thin=
gs.<br></div><div><br></div><div><br></div><div>Peter Barnes<br></div></div></blockquote>=
</div><div><br></div></body></html>
--Apple-Webmail-86--af5c1a72-2ad2-4655-8864-13068ebbc066--

--Apple-Webmail-42--af5c1a72-2ad2-4655-8864-13068ebbc066--

```

## Conclusion

Evidence found on Peter's iPhone indicated the following:

- **Final Conclusions and Evidence from Peter's iPhone:**
- The investigation of Peter Barnes' iPhone provided critical evidence linking him to the conspiracy involving the theft of funds at Pure Gold Credit Union. The email and SMS data retrieved from his phone revealed several key pieces of information:
- **Communication with Oliver Bell:** Emails and voicemail messages directly linked Peter to Oliver Bell, the ringleader. Oliver's voicemail explicitly discussed the stolen funds, the fraudulent actions taken, and the methods used to cover up the crime. The message clearly implicated Peter in the conspiracy, further establishing his role in the theft. Voice mail in files 123-1.amr and 125-1.amr said "hi peter it's your buddy Oliver, from my math you and Rosie have queered over 125k. remember though I get 20% and i keep clearing the audit record so that Evelyne can never catch you. Give me my cash though put it in an envelope and put it at my backdoor. Pleasure doing business with you."
- **Evidence of Fraudulent Transactions:** The phone contained records of communications and activities that corroborated the theft of over \$125,000, as mentioned in Oliver's



voicemail. These records showed Peter's involvement in executing fraudulent transactions and his awareness of the ongoing scheme.

- **Conspiracy with Rosie Lloyd:** Emails and text messages between Peter and Rosie Lloyd highlighted their coordination in executing the fraud. They discussed logistics, financial transactions, and ways to cover their tracks.
- **Attempts to Conceal Evidence:** Peter's phone also revealed attempts to delete or hide incriminating evidence, though these efforts were unsuccessful due to forensic analysis.
- **IMG-006.MOV:** A video file found on Peter's iPhone, labeled IMG-006.MOV, contained footage showing the serial numbers of some of the stolen currency. This video provided direct evidence of the stolen money and linked Peter to the physical handling of the illicit funds.
- **IMG-006.HEIC:** An image file found on the phone, labeled IMG-006.HEIC, displayed the exact geographic coordinates and location where the stolen funds were being stored or exchanged. This image helped confirm the specific location related to the theft and the conspiracy.

Based on the findings from Peter's iPhone, it is evident that he played a significant role in the fraudulent scheme, collaborating with Oliver Bell and Rosie Lloyd. His actions, as captured on the device—including the video and image files—further substantiate the allegations of his involvement in the theft, money laundering, and concealment of the stolen funds.

Evidence found on Rosie's phone and emails clearly showed her participation in this fraud scheme and her intention to commit currency theft. Both Peter and Rosie were found naming Mr. X (Oliver Bell) in the emails.

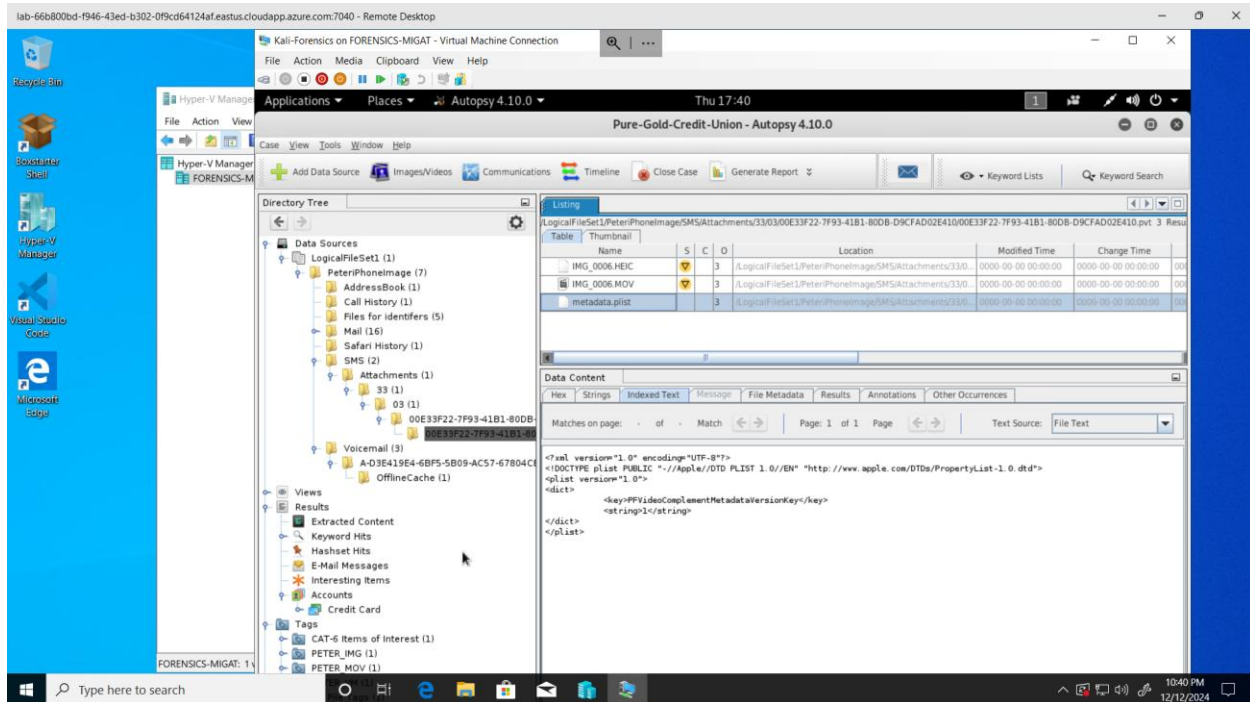
## Bonus Conclusion

Did you determine who is Mr. X? If so, who is it, and how did you figure this out?

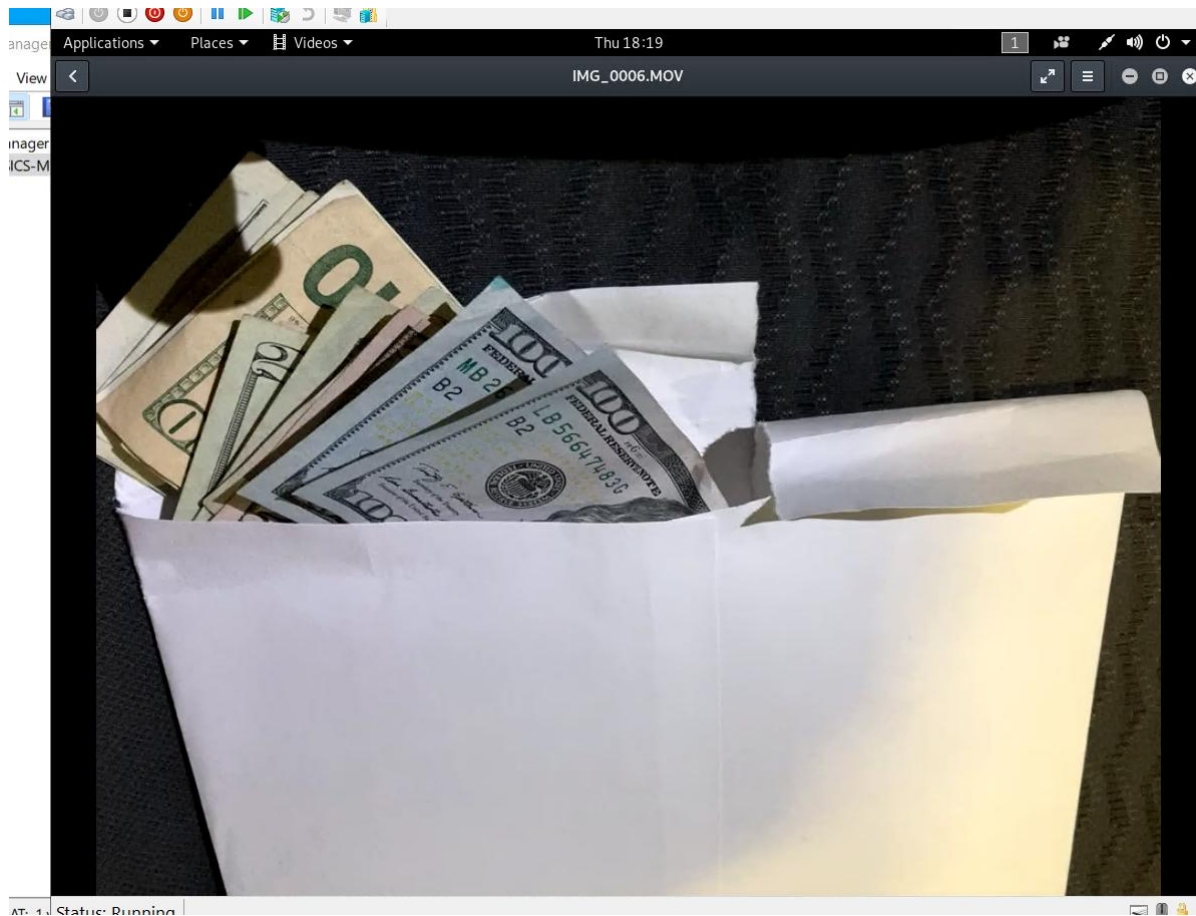
- Oliver Bell's (District Manager) voicemail obtained from files 123-1.amr and 125-1.amr, retrieved from the PeteriphonelImage.zip and RosieiphonelImage.zip, explicitly referenced the stolen funds and his involvement in covering up the fraud. Oliver stated, "hi peter it's your buddy Oliver, from my math you and Rosie have queered over 125k. remember though I get 20% and i keep clearing the audit record so that Evelyne can never catch you. Give me my cash though put it in an envelope and put it at my backdoor. Pleasure doing business with you." This statement directly ties Oliver to the scheme, offering clear evidence of his role as the mastermind.

# Appendix A: Correspondence Evidence

List any sms attachments and pictures found here, see above as well



IMG-0006.MOV



IMG-0006.HEIC is below under Appendix B.

## Appendix B: GPS Location Information



Online EXIF Viewer - View EXIF Data Online - Mozilla Firefox

https://onlineexifviewer.com


Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

### Camera Make and Model

Apple - iPhone SE (2nd generation)

### Camera Location Details

Photo GPS Location: [35.97045,-86.80738888888888](#)



mapbox

### All Photo EXIF Data

[Save & Share EXIF](#)

☒ Hide Serial Numbers

Make	Apple
Model	iPhone SE (2nd generation)
Orientation	bottom-right
XResolution	72
YResolution	72
ResolutionUnit	inches
Software	16.5
DateTime	2023:10:20 19:53:39
HostComputer	iPhone SE (2nd generation)
TileWidth	512
TileLength	512
Exif IFD Pointer	274

root@kali: ~/casedata/Pure-Gold-Credit-Union/Export

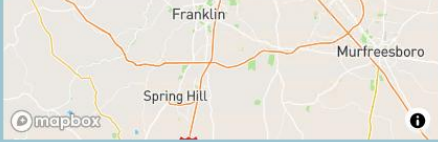
File Edit View Search Terminal Tabs Help

root@kali: ~/autopsy-fil... root@kali: ~/casedata/P... root@kali: ~/casedata/P... Keyword Lists Keyword Search

Online EXIF Viewer - View EXIF Data Online - Mozilla Firefox

https://onlineexifviewer.com

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter



mapbox

### Image Preview

Preview not available

HostComputer	iPhone SE (2nd generation)
TileWidth	512
TileLength	512
Exif IFD Pointer	274
GPS Info IFD Pointer	2148
ExposureTime	1/46
FNumber	f/1.8
ExposureProgram	Normal program
ISOSpeedRatings	320
ExifVersion	0232
DateTimeOriginal	2023:10:20 19:53:39
DateTimeDigitized	2023:10:20 19:53:39
OffsetTime	-05:00
OffsetTimeOriginal	-05:00
OffsetTimeDigitized	-05:00
ShutterSpeedValue	1/46

