Cybersecurity

21.3 The Final Report

Case Report
Pure Gold Credit Union

Table of Contents

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.

Upon investigating Rosie Lloyd and Peter Barnes' email and SMS message communication, our team found extensive communication between the two parties, meeting in person and discussing plans to commit the crime both over text message and through email correspondence. In these messages, both parties indicated that they were angry that they weren't being compensated fairly by Pure Gold Credit Union. Peter Barnes also had been in contact with a mysterious person, known only by the alias "X". "X" had established email correspondence with Mr. Barnes, and had sent him a voicemail. Upon listening to the voicemail, we determined that the identity of "X" was in fact District Manager, Oliver Bell.

Equipment and Tools

This investigation was conducted on a Kali Linux machine using an open source digital forensics tool called Autopsy. We were also able to analyze email and SMS messages using SQLite Browser, a graphical user interface that helps our team visualize this data. Voicemails were extracted and listened to on our local machines using Windows Media Player. We converted Apple Timecodes using a free online converter tool online (https://www.epochconverter.com/coredata).

Details of Peter's iPhone

Details of Peter's iPhone

Name	Findings	Location/File in iPhone image file
Model	Iphone 12/8	activation_record.plist
Host Name	Peter's iPhone	data_ark.plist
OS Version	16.5.1	data_ark.plist
User Email	peterbarnes12792@icloud.com	Accounts3.sqlite
Phone Number	6155719608	cellularusage.db
Serial Number	FFNHHK2RPLJM	activation_record.plist
ICCID	89148000009489719791	activation_record.plist
IMEI	352853889135063	activation_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Provided
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	Provided

Details of Rosie's iPhone

Details of Rosie's iPhone

Name	Findings	Location/File in iPhone image file
Model	iPhone 12/8	activation_record.plist
Host Name	Rosie's iPhone	data_ark.plist
OS Version	16.5	data_ark.plist
User Email	rosielloyd071292@icloud.com	Accounts3.sqlite
Phone Number	6154278267	cellularusage.db
Serial Number	FFPHG1LYPLJM	activation_record.plist
ICCID	89148000009489732844	activation_record.plist
IMEI	311480010308141	activation_record.plist
MD5 Hash	e666cd1232ead8f76c0a42910f54b7d5	Provided
SHA256 Hash	0aa14fa06a416fd59c1e6586c888dd3511b1a98c7a01915233181866bedd767152d6577ccb534ca0d1e83ffd27683e621607	Provided

Evidence to Establish Personas

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

Peter Barnes:

Phone Number:	6155719608
Email:	peterbarnes12792@icloud.com
Relationship:	Conspirator

Rosie Lloyd:

Phone Number:	6154278267
Email:	rosielloyd071282@icloud.com
Relationship:	Conspirator

Oliver Bell - aka “Mr. X”

Phone Number:	6158070242 (from voicemail records)
Email:	hockeyfan4747@proton.me
Relation:	Conspirator

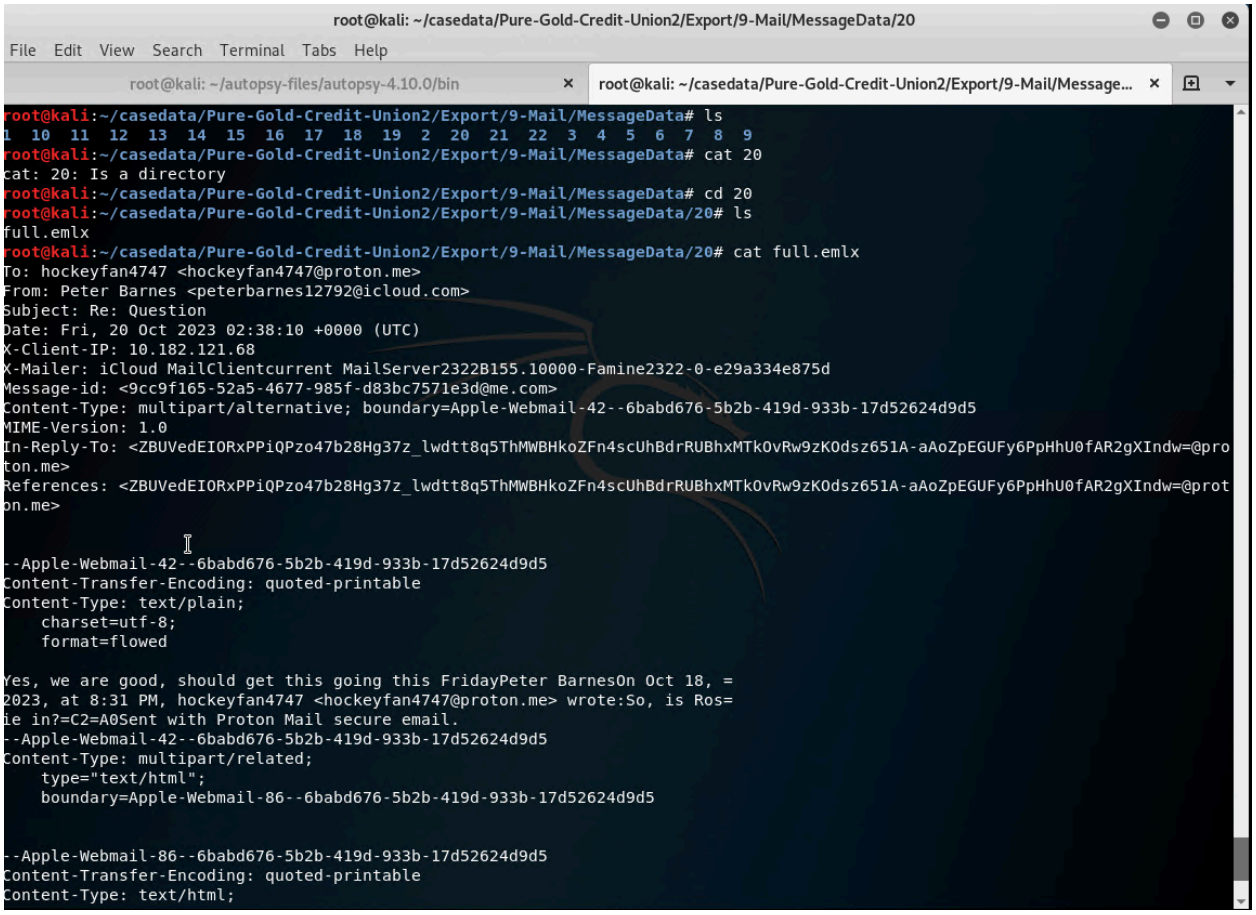
After reviewing the SMS message data and email data between Rosie Lloyd and Peter Barnes, it is clear that Peter is using the email peterbarnes12792@icloud.com and Rosie is using rosielloyd071282@icloud.com. Their email messages to each other also regularly conclude with a signature of their name further proving to us it is them using these emails. Analyzing the SMS message data, we can clearly see text messages being sent back and forth between Rosie and Peter. Our team was able to identify which person was sending emails by paying close attention to the timestamps of the messages sent.
Mr. Barnes had also communicated with District Manager, Mr. Oliver Bell through email, SMS and voicemail communications. We were able to determine that Mr. Bell was using the email hockyfan4747@proton.me because we were able to triangulate the timestamps associated with his text messages he sent corresponding to the time the voicemail came in as well.

Evidence relating to theft of PGCU funds

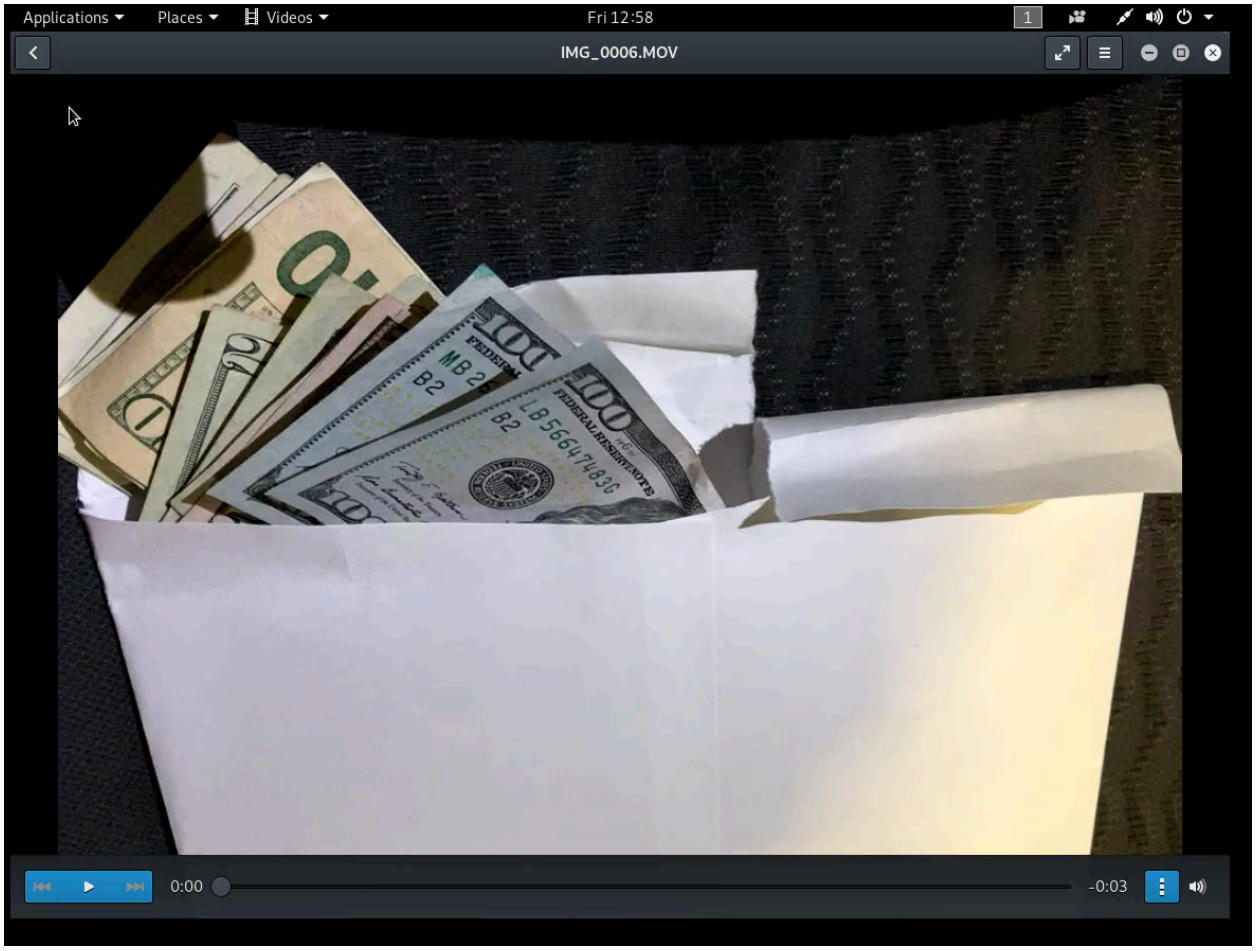
This sub-section provides details regarding the evidence found as it relates to the theft of funds.

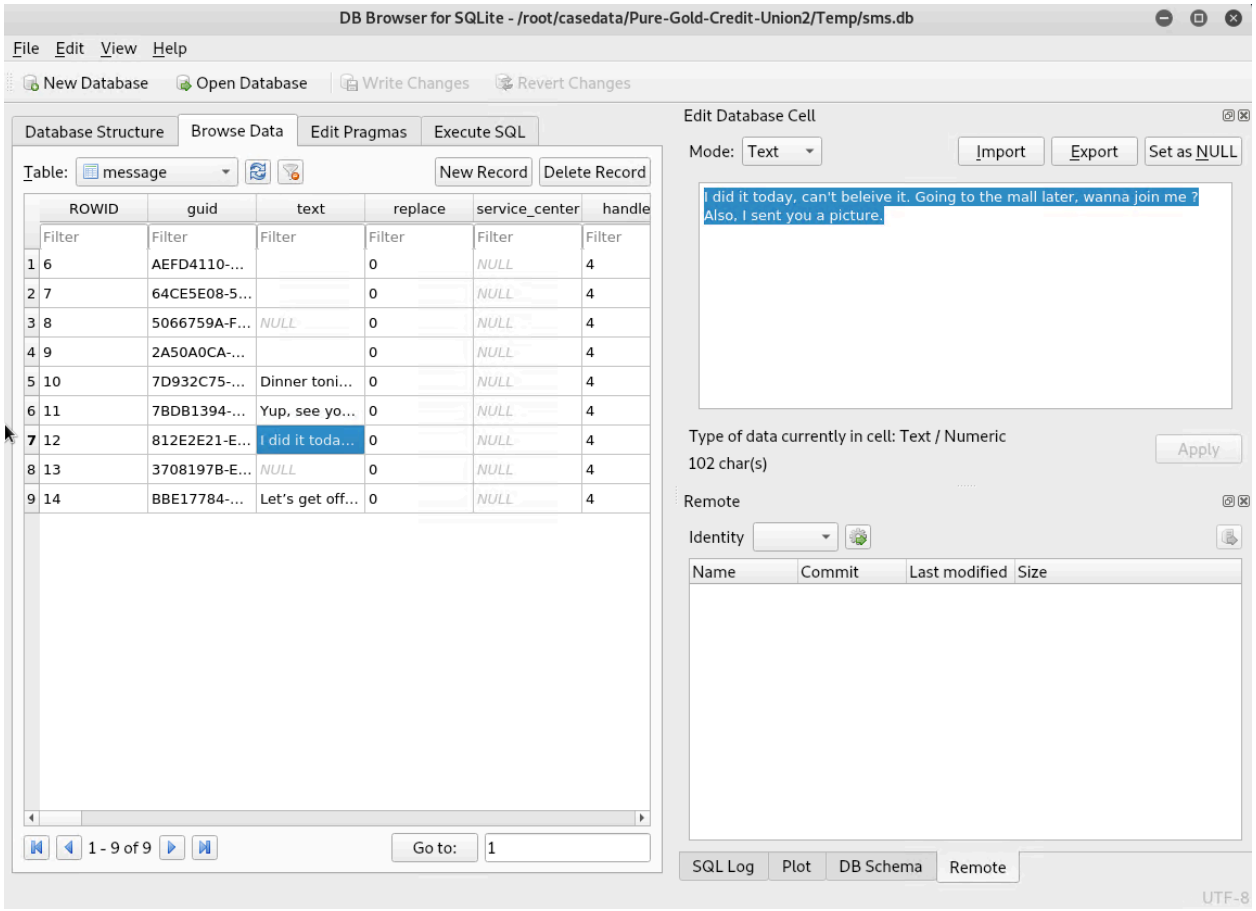
**Note: All time stamps were converted to GMT (Greenwich Mean Time)*

Detailed plans were coordinated over email correspondence. In the Master Timeline of Email Messages table, under Artifact 20, hockyfan4747@proton.me asks if Rosie is “in” and Peter Barnes replies, “Yes we are all set. Should get this going on Friday.”

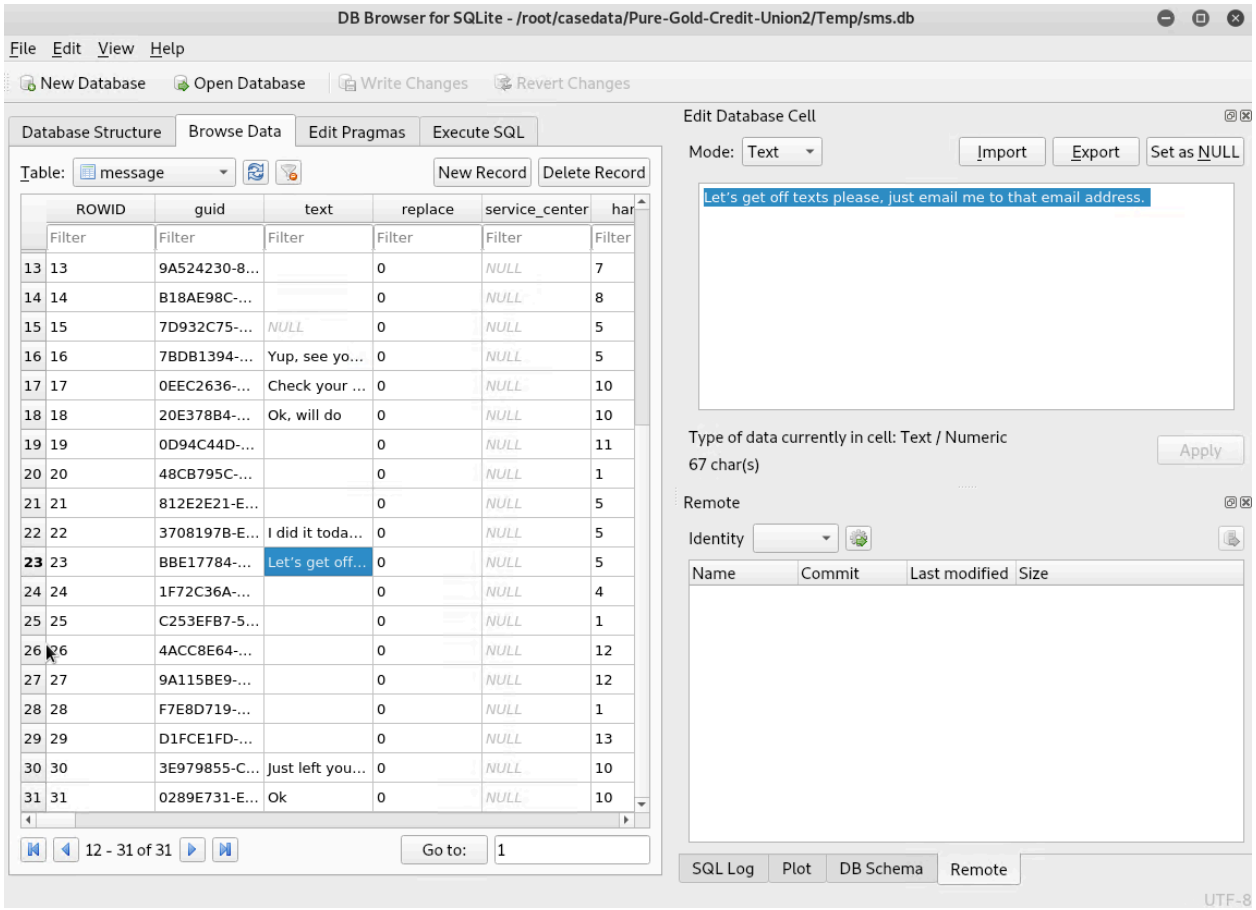


Referring to artifact number 7 on the Master Timeline of SMS messages, on October 21st 2023 at 00:56:49 GMT Rosie Lloyd had sent a picture/video message to Peter Barnes of an envelope of cash. A few seconds later, she texted Peter at 00:56:57 saying “I did it today, can't believe it. Going to the mall later, wanna join me? Also I sent you a picture.” The timestamp shows that this message was sent after midnight on Saturday the 21st, adjusting for United States time zones this would place the crime happening on Friday evening of October 20th.

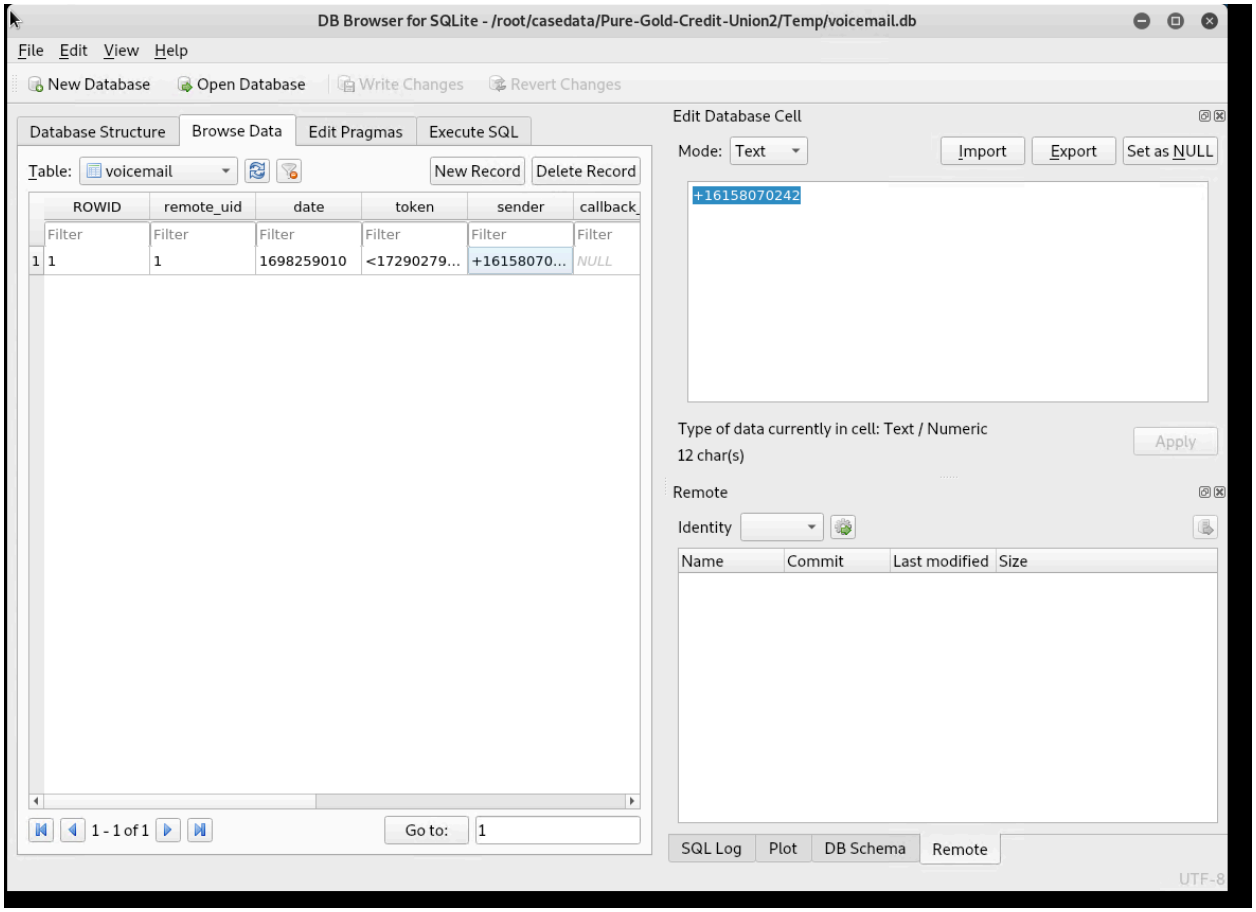

Applications
Places
Videos
Fri 12:58
1
IMG_0006.MOV
0:00
-0:03

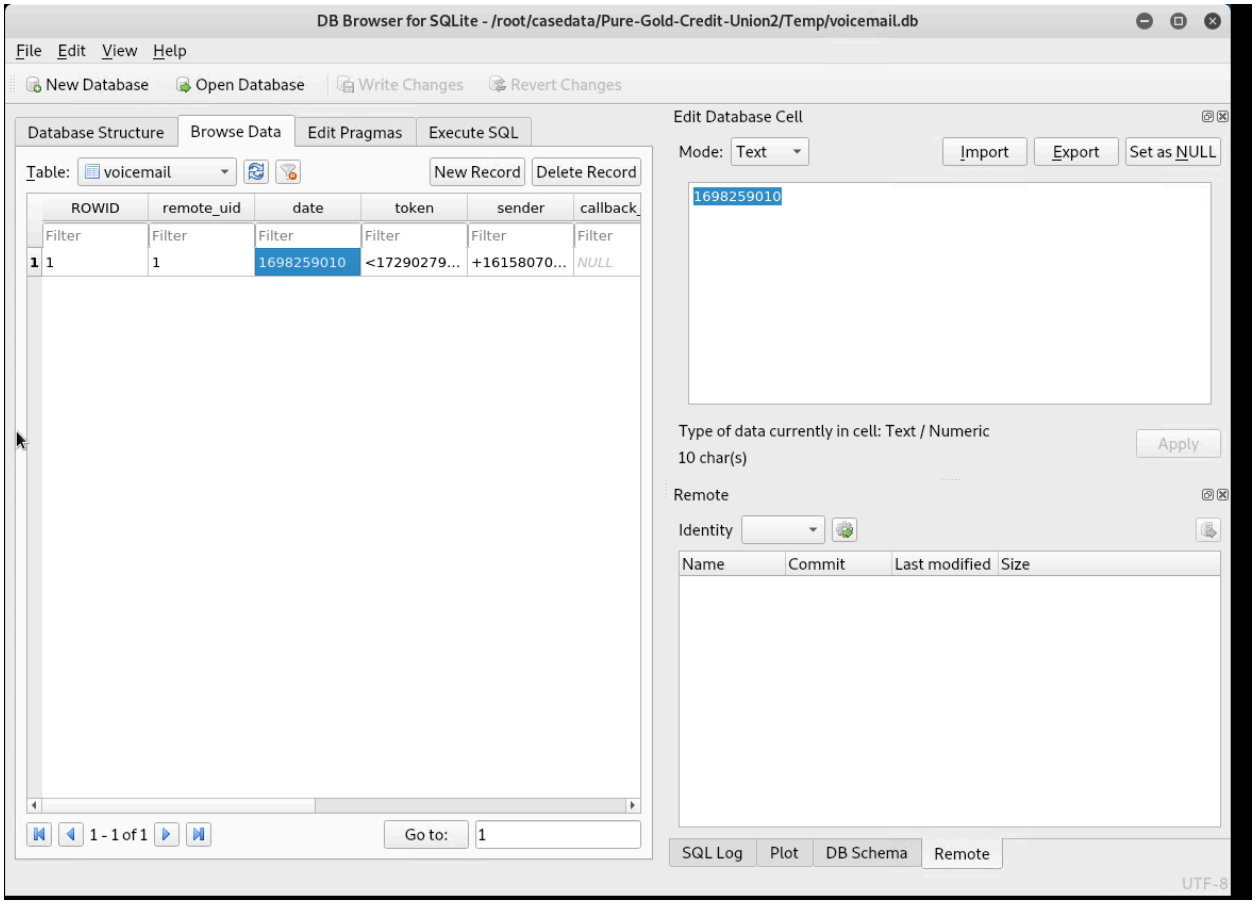


On artifact number 8 on the Master Timeline of SMS Messages, Peter expresses discomfort receiving messages like that via text messages and says:“Let’s get off texts please, just email me to that email address”



Finally, on October 25th 2023 at 18:36:50 GMT, referring to artifact number VM-1, the voicemail that Oliver Bell had sent had implicated both Rosie and Peter in the crime stating they both cleared over $125,000 in cash. Mr. Bell also implied he will “keep clearing the audit records so Evelyn can never catch you.” He instructs Peter to send him his cut of the money in an envelope left at Mr. Bell’s back door. He concludes the message stating “Pleasure doing business with you.”


DB Browser for SQLite - /root/casedata/Pure-Gold-Credit-Union2/Temp/voicemail.db
File Edit View Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: voicemail
New Record
Delete Record
ROWID
remote_uid
date
token
sender
callback
Filter
1
1
1
1698259010
<17290279...
+16158070...
NULL
1 - 1 of 1
Go to:
1
Edit Database Cell
Mode: Text
Import
Export
Set as NULL
+16158070242
Type of data currently in cell: Text / Numeric
12 char(s)
Apply
Remote
Identity
Name
Commit
Last modified
Size
SQL Log
Plot
DB Schema
Remote
UTF-8

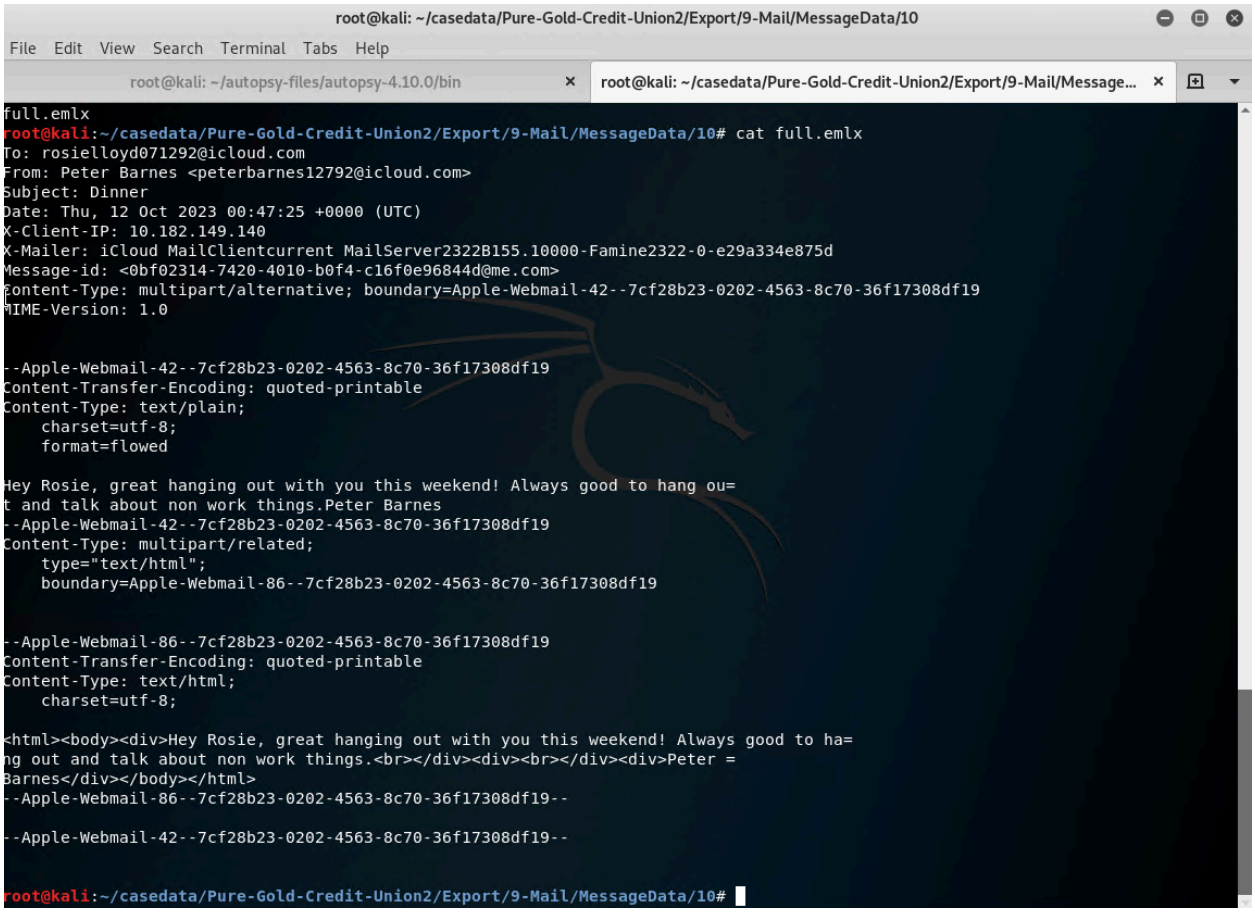


Plot Timeline

October 12th, 2023

Email correspondence between Rosie Lloyd and Peter Barnes suggest the two had spent time together outside of work.
Peter sent the initial message at 00:47:25 GMT
“Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk

about non-work things. Peter Barnes”



Rosie replied at 22:36:10 GMT

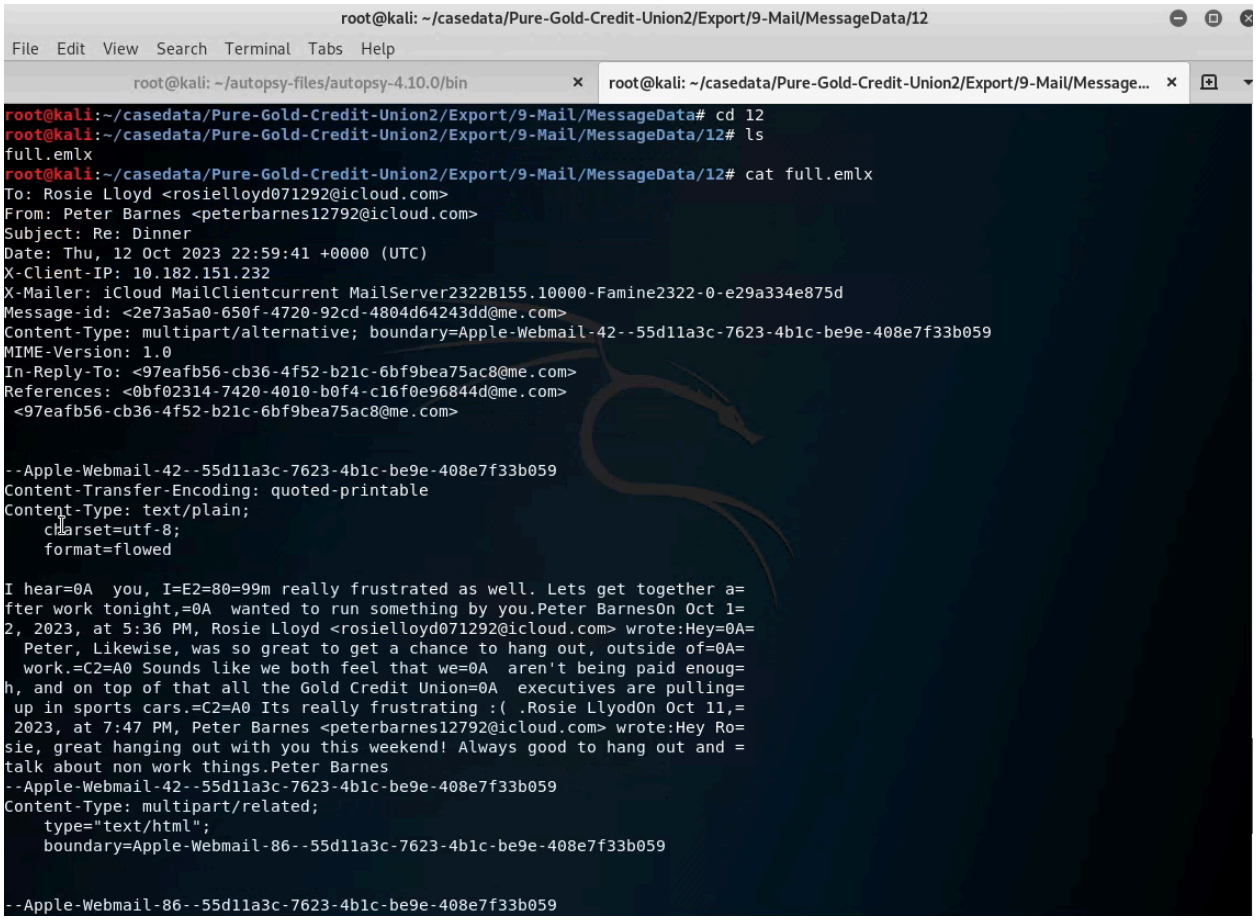
In this message, she expressed a bit of resentment towards credit union executives and expressed frustration about her pay:

“Hey Peter, Likewise, was so great to get a chance to hang out, outside of work. Sounds like we both feel that we aren’t being paid enough and on top of that all the Gold Credit

Union executives are pulling up in sports cars. Its really frustrating :(Rosie Lloyd”

Peter responded at 22:59:41 GMT

“**I hear you. I'm really frustrated as well. Let's get together after work tonight. I wanted to run something by you. Peter Barnes.”**



In this message, Peter appears to also be angry and frustrated with his job. He states he wants to “run something by” Rosie. It’s possible he may be referring to the details of the crime.

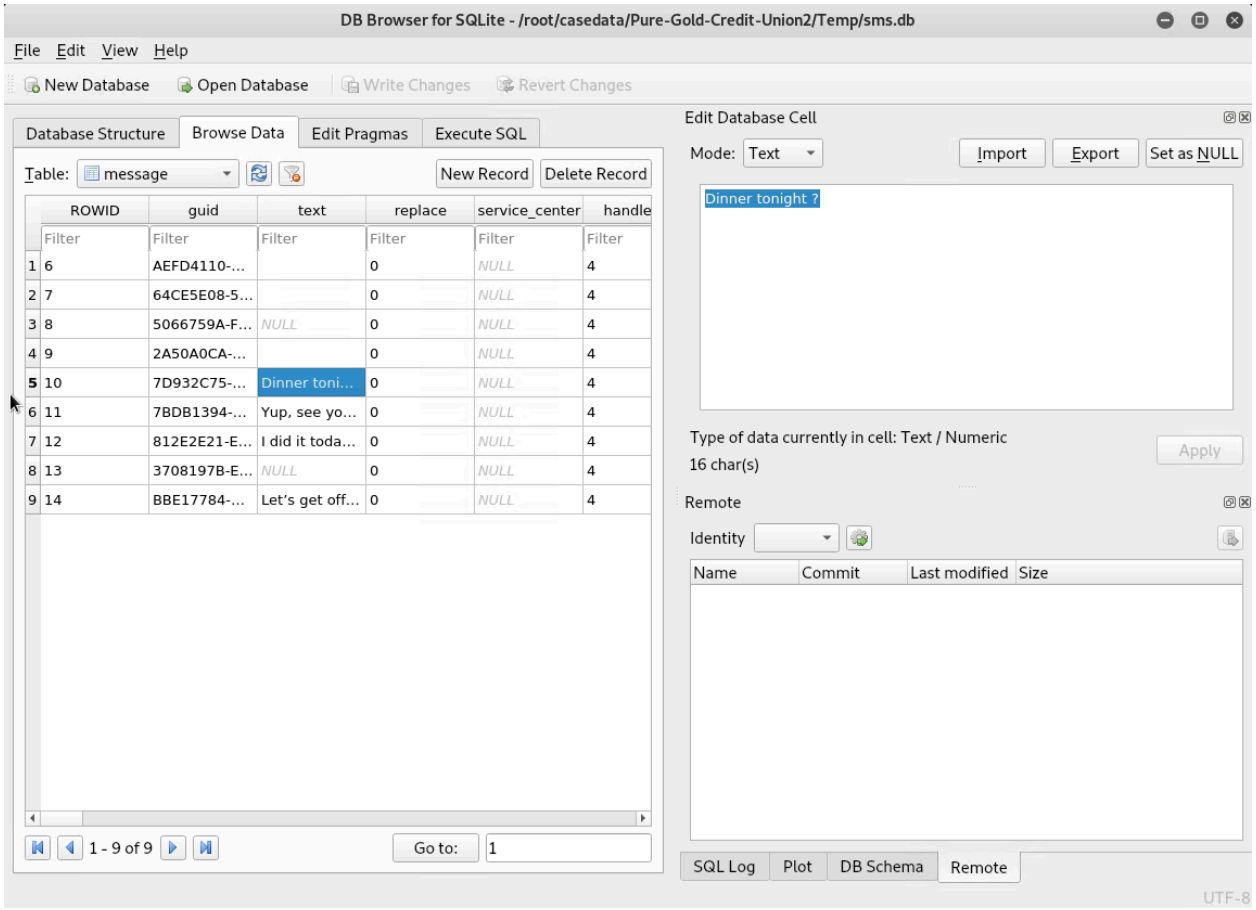
<u>October 18th, 2023</u>

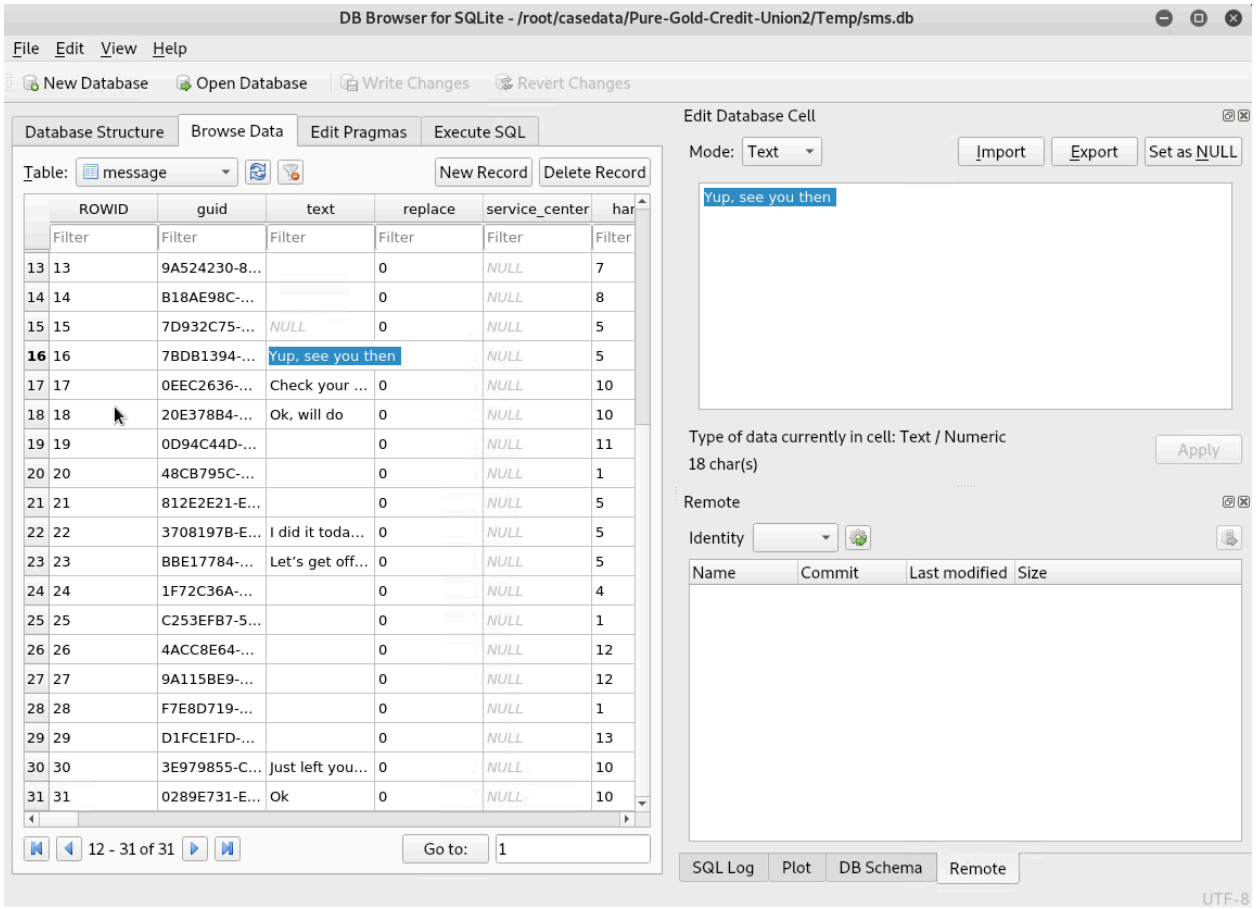
Rosie had text messaged Peter at 15:39:05 GMT:

“Dinner Tonight?”

At 15:40:48 GMT, he replies:

“Yup, see you then”

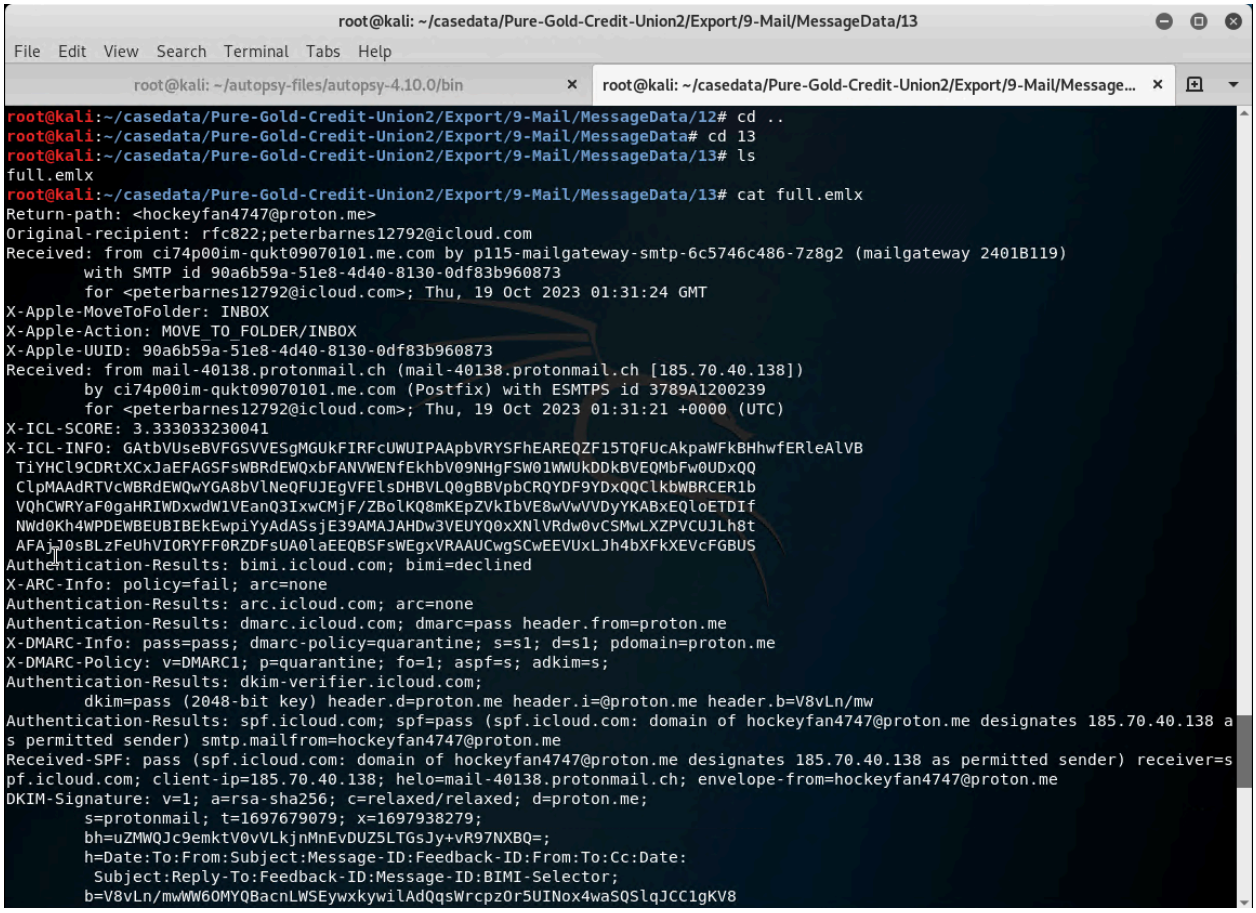

DB Browser for SQLite - /root/casedata/Pure-Gold-Credit-Union2/Temp/sms.db
File Edit View Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: message
New Record
Delete Record
ROWID guid text replace service_center handle
1 6 AEFD4110-... 0 NULL 4
2 7 64CE5E08-5... 0 NULL 4
3 8 5066759A-F... NULL 0 NULL 4
4 9 2A50A0CA-... 0 NULL 4
5 10 7D932C75-... Dinner toni... 0 NULL 4
6 11 7BDB1394-... Yup, see yo... 0 NULL 4
7 12 812E2E21-E... I did it toda... 0 NULL 4
8 13 3708197B-E... NULL 0 NULL 4
9 14 BBE17784-... Let's get off... 0 NULL 4
1 - 9 of 9
Go to: 1
Edit Database Cell
Mode: Text
Import
Export
Set as NULL
Dinner tonight ?
Type of data currently in cell: Text / Numeric
16 char(s)
Apply
Remote
Identity
Name Commit Last modified Size
SQL Log
Plot
DB Schema
Remote
UTF-8



October 19th, 2023

At 01:31:24 GMT, An encoded message was sent to Peter Barnes from hockyfan4747@proton.me. Our team was not able to decode the message, though we do believe it was correspondence from “Mr. X” to Peter containing either a purposefully encrypted

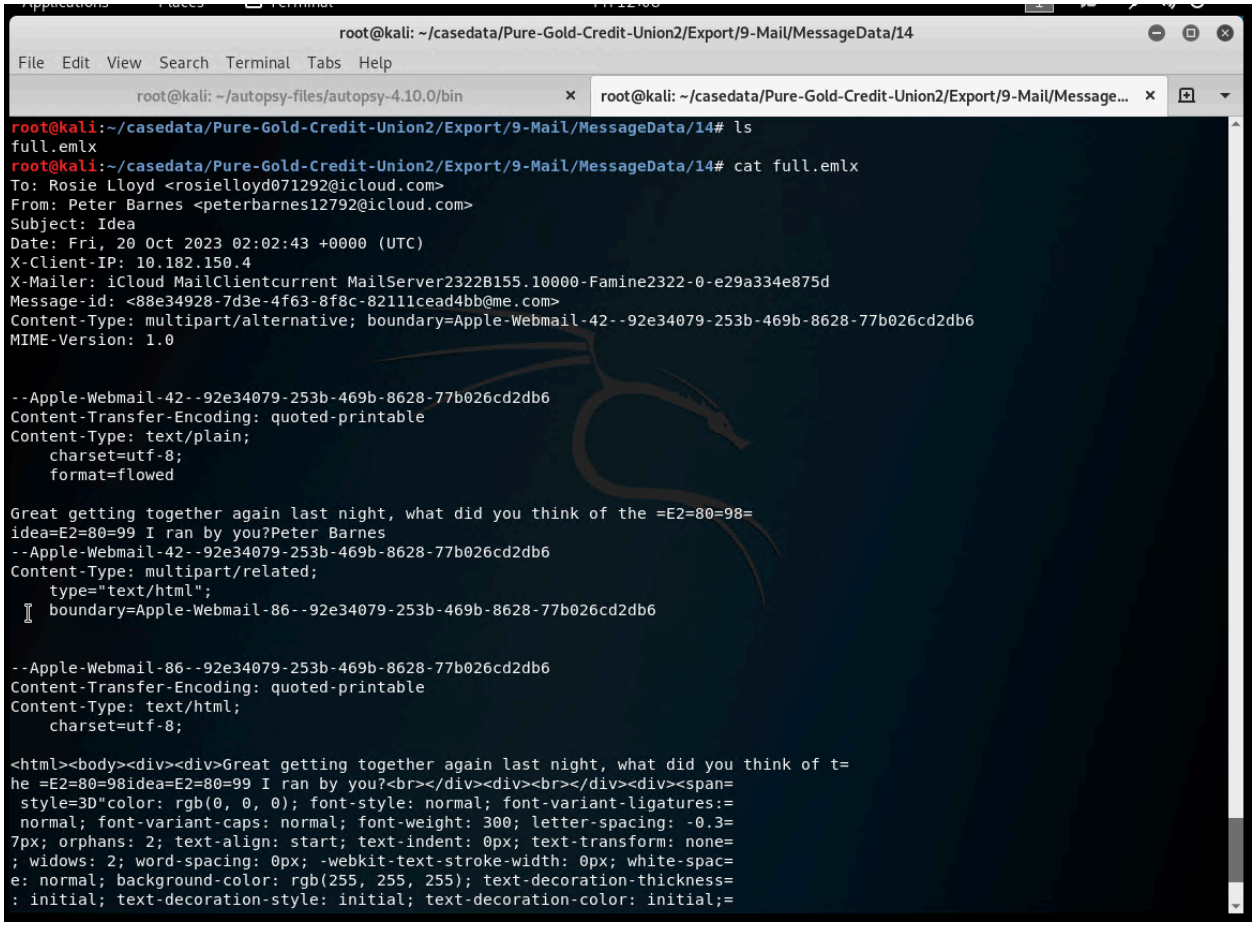
message or a file had been sent over.



October 20th, 2023

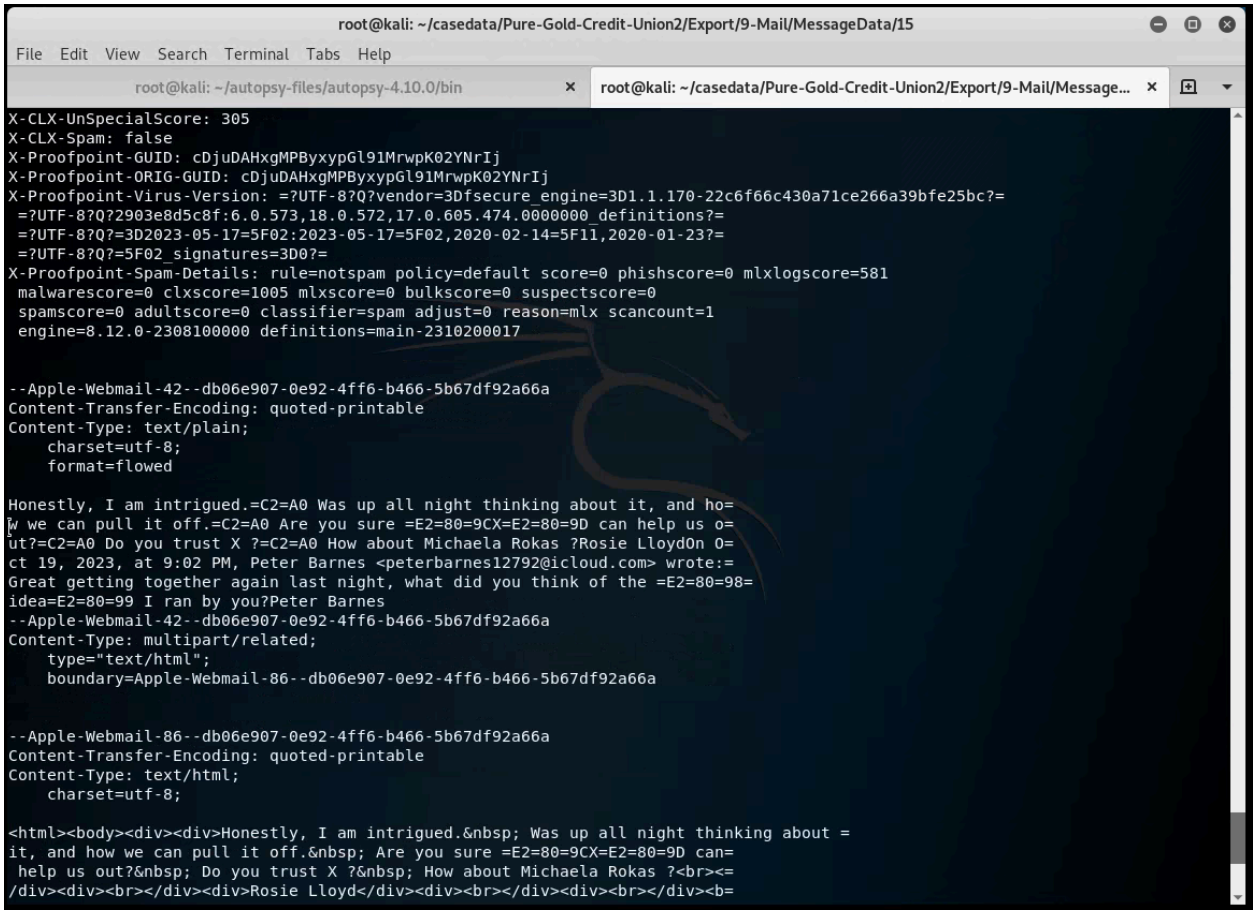
The suspects met once more the night previously, apparently having discussed the details of the heist they were planning. Peter initiated the first message that night at 02:02:43 GMT asking Rosie what she thought of the idea they discussed:

“Great getting together again last night, what did you think of the idea I ran by you? Peter Barnes”



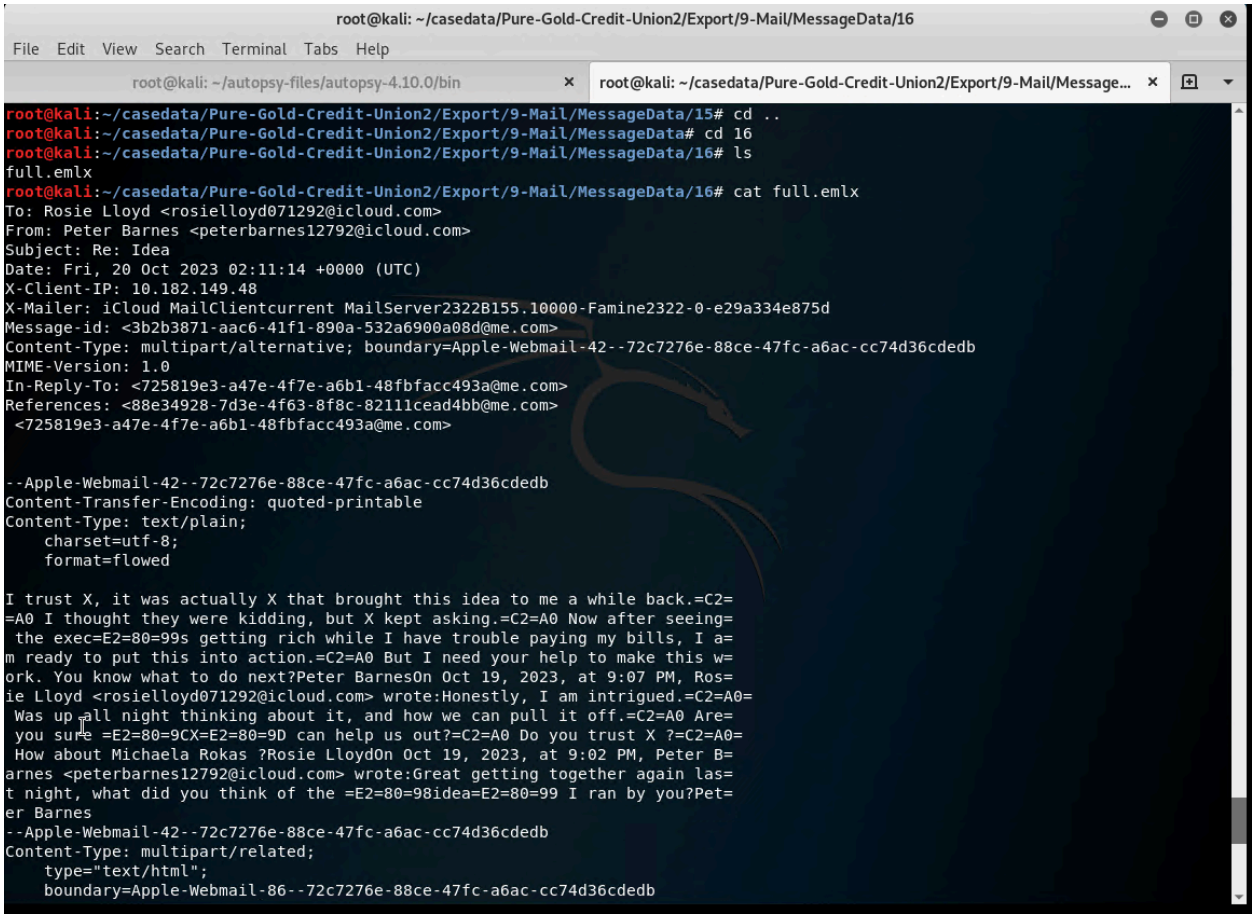
At 02:07:43 GMT, Rosie had responded, interested in the plan. She asks Peter who can help them out and who they can trust:

“Honestly, I am intrigued. Was up all night thinking about it, and how we can pull it off. Are you sure =E2=90=9CX=E2=80=9D can help us out? Do you trust X? How about Michaela Rokas?”

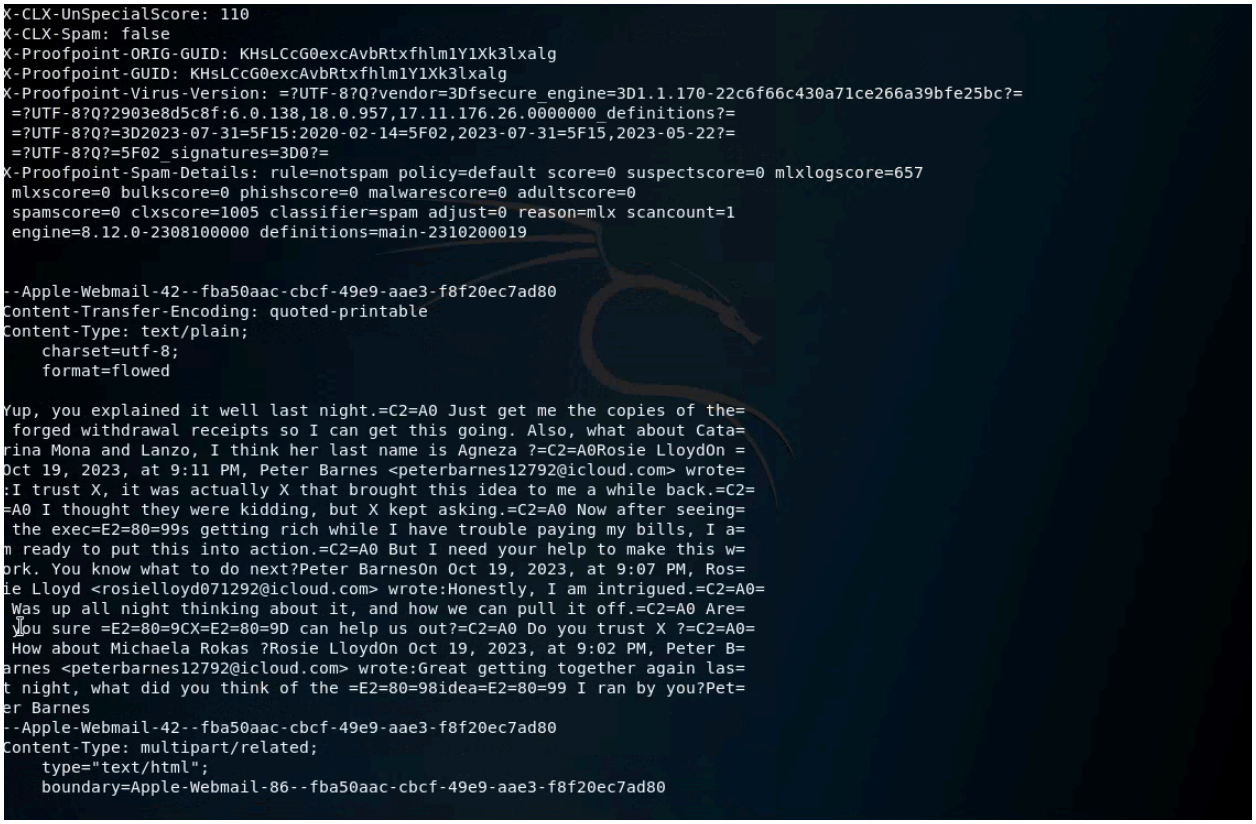


At 02:11:14 GMT, Peter replies to Rosie's message stating he trusts "X" and that it was his idea to begin with. He also adds that he is ready to go ahead with the plans for the heist. He asks Rosie if she knows what to do next:

"I trust X, it was actually X that brought this idea to me a while back. I thought they were kidding but X kept asking. Now after seeing the exec's getting rich while I have trouble paying my bills, I am ready to put this into action. But I need your help to make this work. You know what to do next? Peter Barnes"



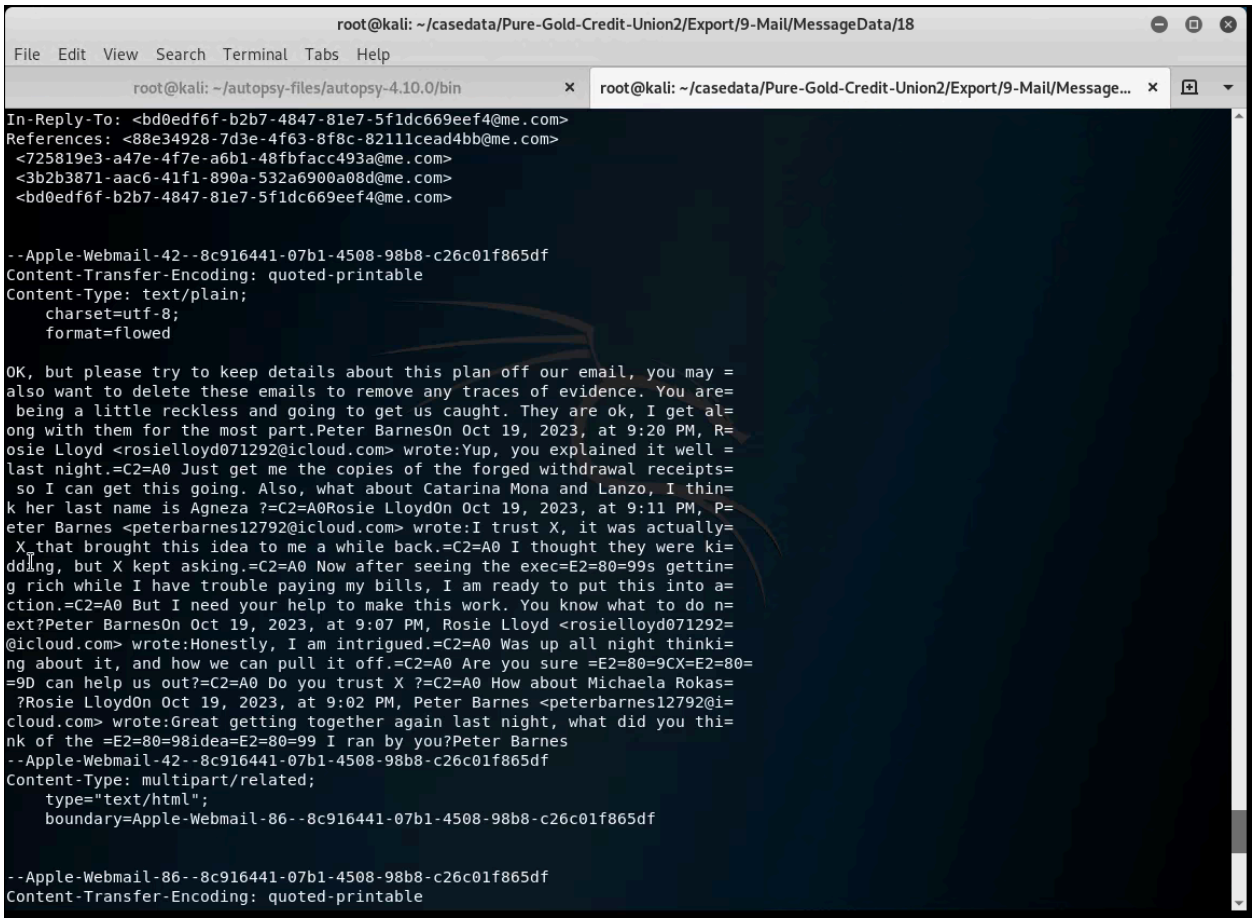
At 2:20:57 GMT, Rosie replied saying she understands what to do and says she will forge the withdrawal receipts from the credit union. She also asks about their other co-workers:
“Yup, you explained it well last night. Just get me the copies of the forged withdrawal receipts so I can get this going. Also what about Catarina Mona and Lanzo, I think her last name is Agneza? Rosie Lloyd”



Peter replies at 2:20:00 GMT

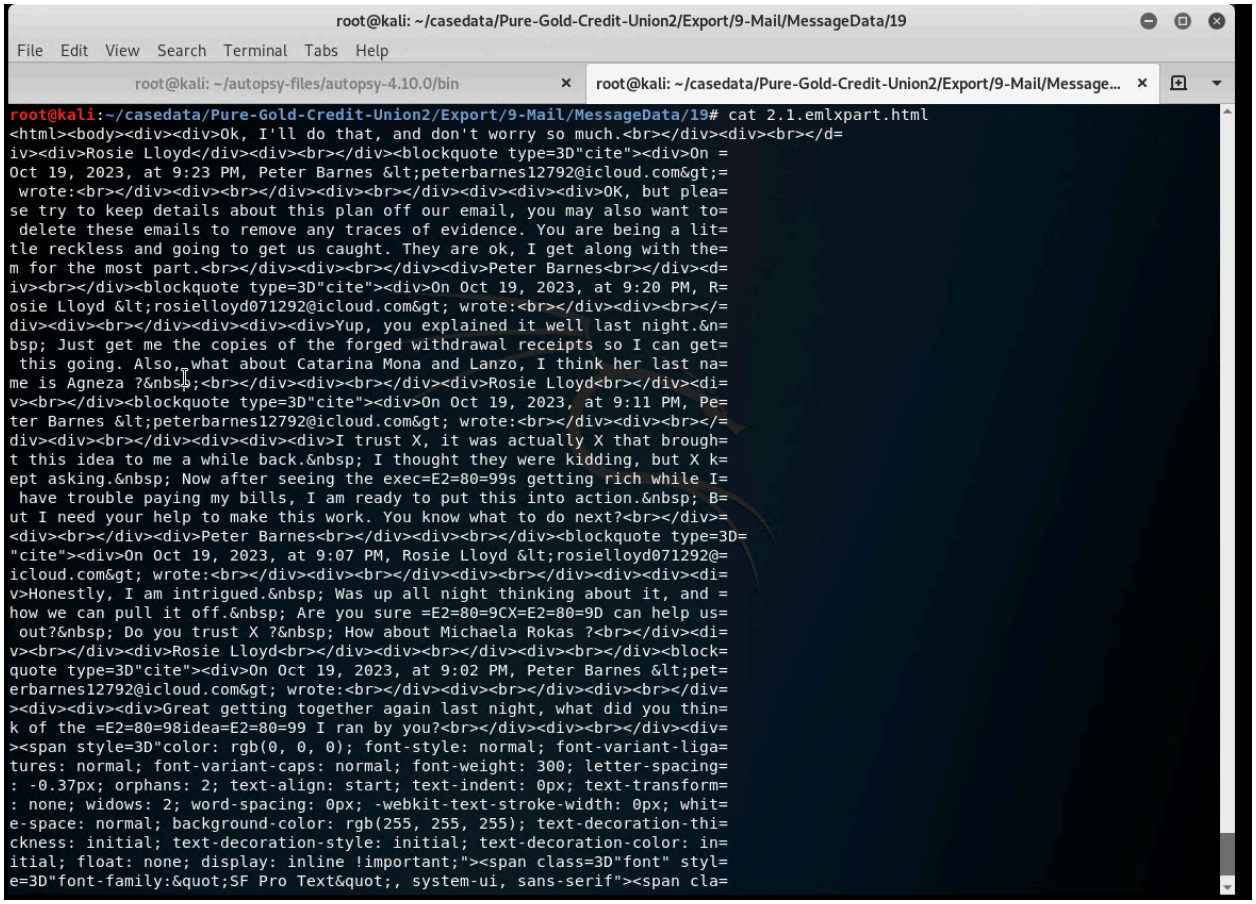
At this moment, Peter expresses concern about getting caught and suggests to Rosie she delete her emails:

“Ok, but please try to keep details about this plan off our email. You may also want to delete these emails to remove any traces of evidence. You are being a little reckless and going to get us caught. They are ok, I get along with them for the most part. Peter Barnes.”



Rosie’s last correspondence with Peter is sent to him at 02:33:47 GMT, attempting to calm his concerns:

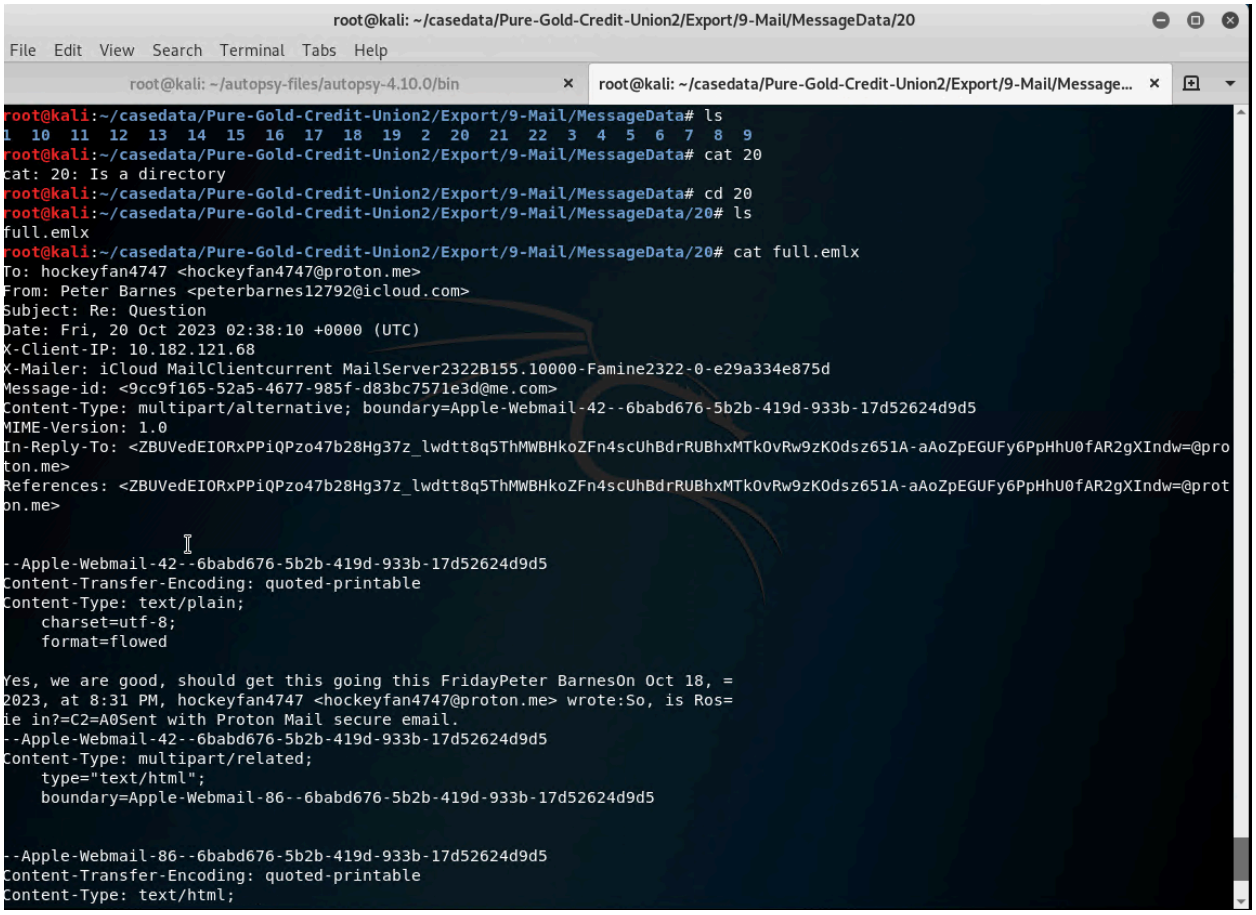
“Ok, I’ll do that, and don’t worry so much. Rosie Lloyd”



A few minutes later Peter gets an email from hockeyfan4747@proton.me, believed to be “Mr.X.” We suspect that this email is part of a thread of messages in which the earlier messages where deleted. Mr. X is asking if Rosie is in.

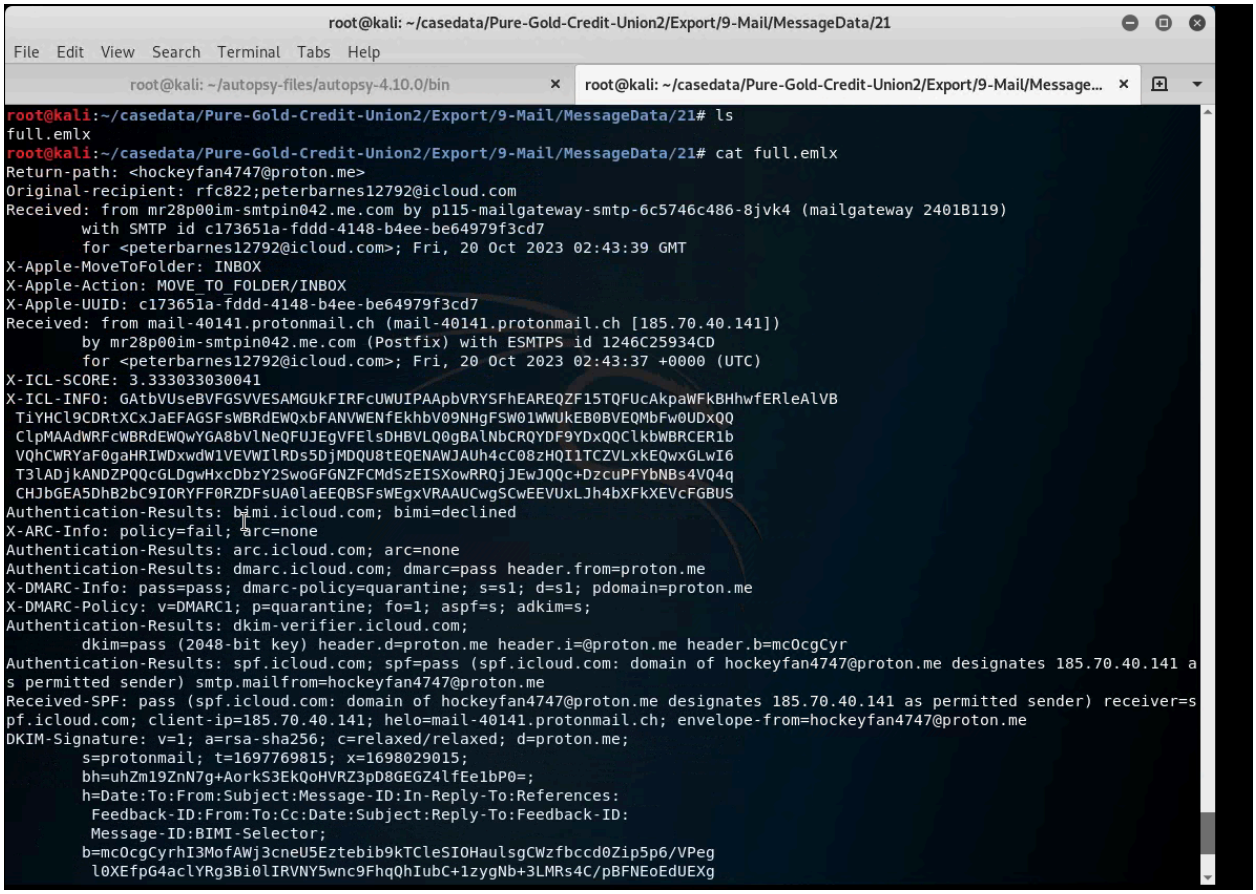
Hockyfan4747@proton.me asks:
“So, is Rosie in?

peterbarnes12792@icloud.com replies:
“Yes, we are good, should get this going this Friday.”



Peter is suggesting the date of Friday the 20th of October for the date of the heist to occur.

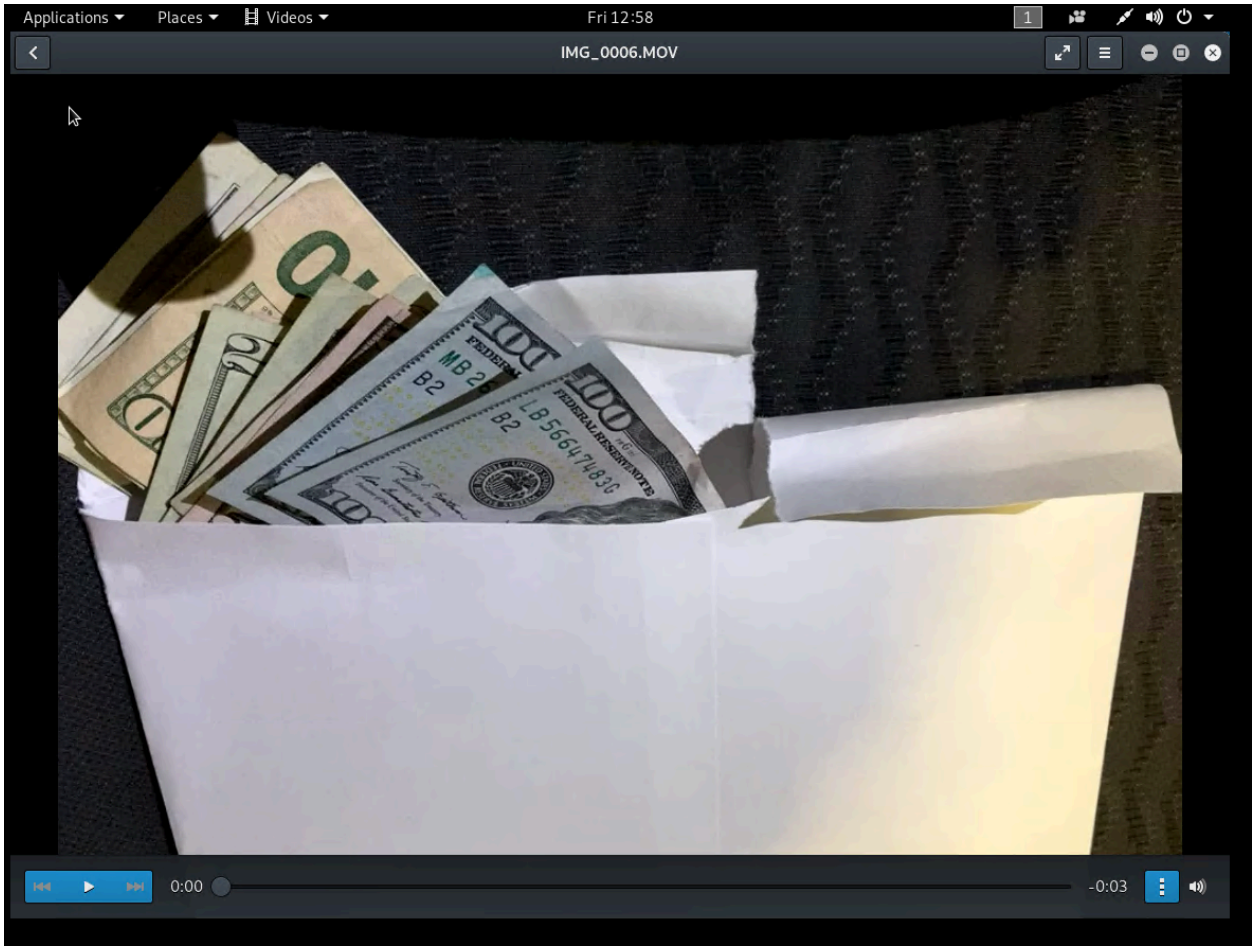
At 02:43:23 GMT, another encoded message came through from hockeyfan4747@proton.me It's possible this could be another encoded message or a file sent.



October 21st, 2023

At 00:56:49 GMT Rosie had sent Peter a multimedia message of an envelope of cash. Our team retrieved a .mov file and an .HEIC file of the envelope. Below is a screenshot of the .mov

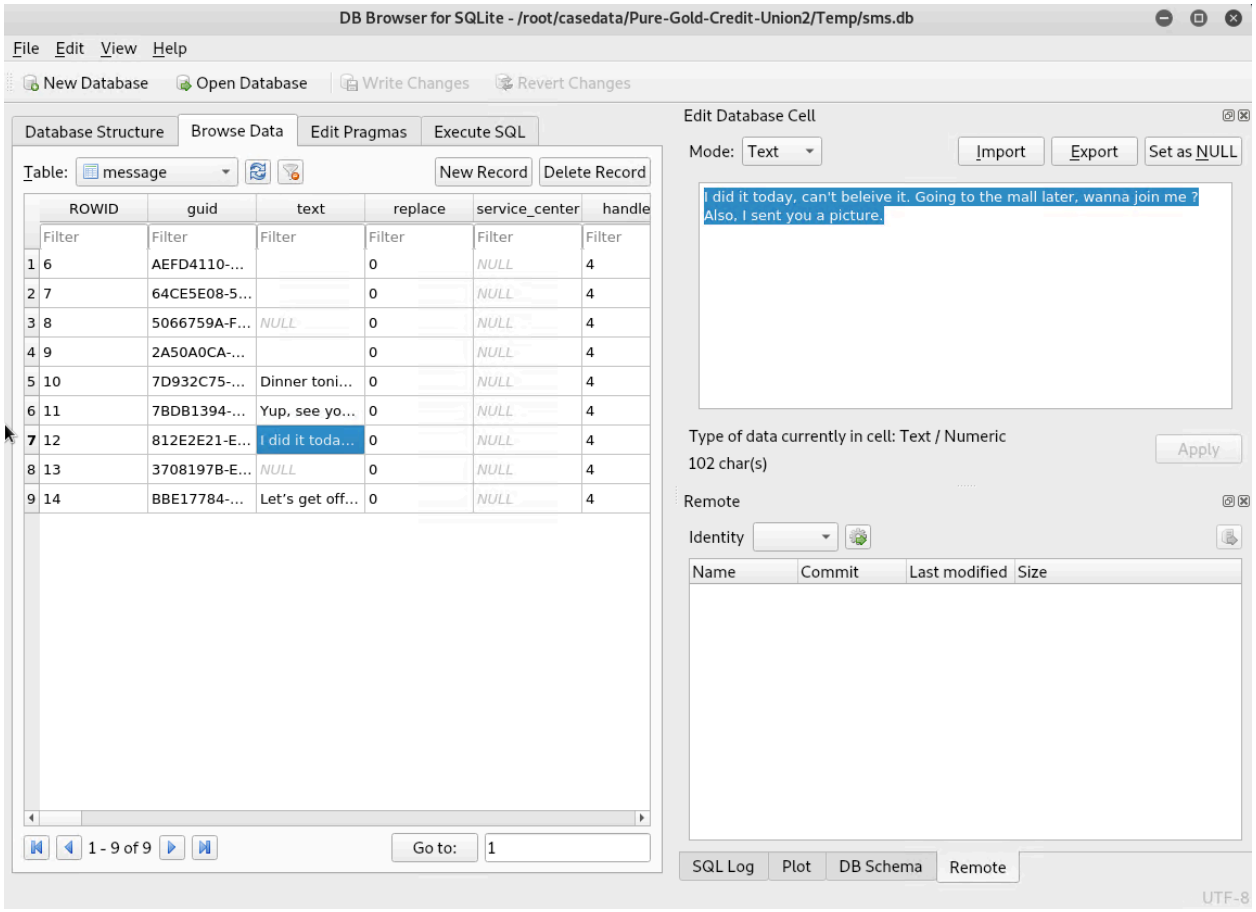
file.



A few seconds later at 00:56:57 GMT, Rosie sent a text message to Peter stating “I did it today, I can’t believe it.”

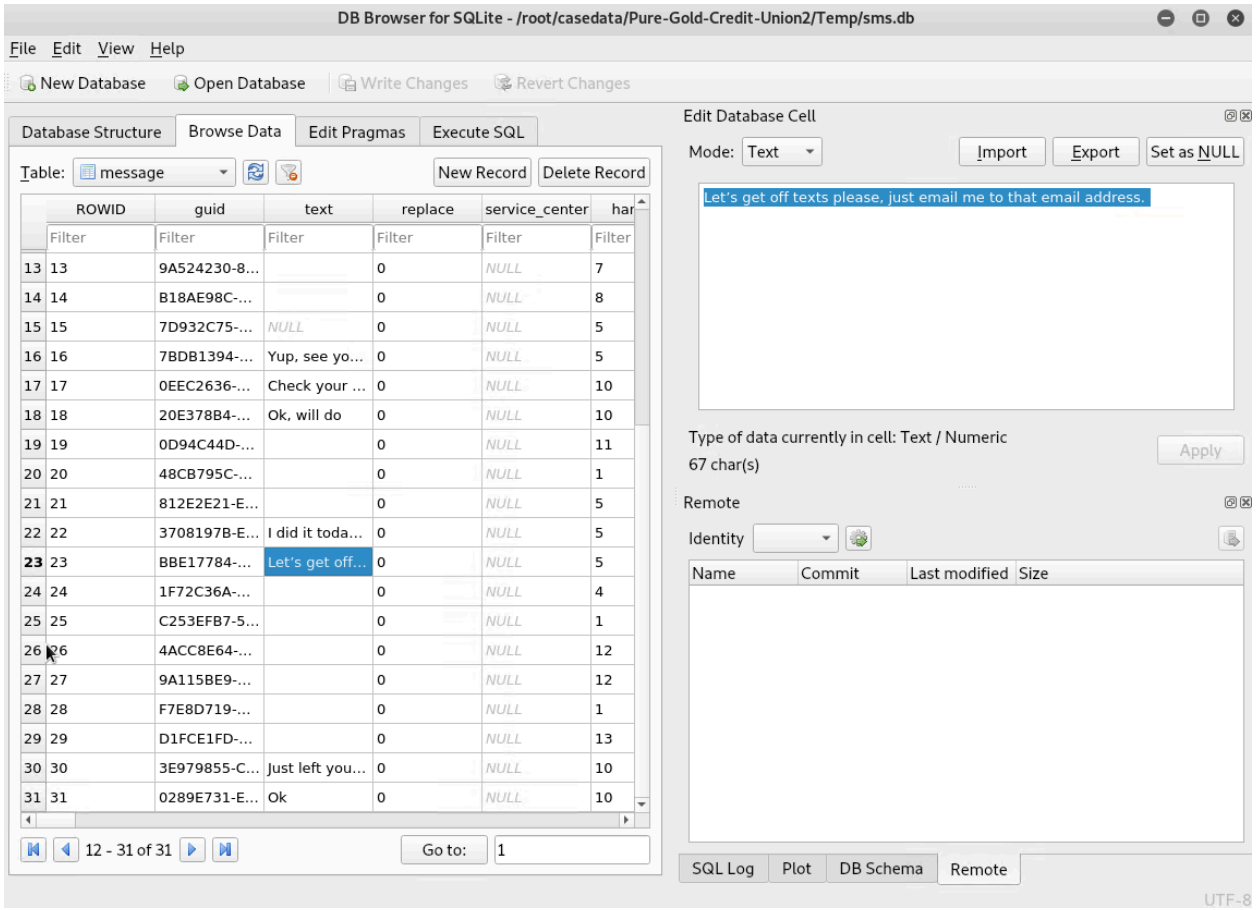
“I did it today, can’t believe it. Going to the mall later, wanna join me? Also I sent you a

picture.”



Peter replied at 00:58:50 GMT again expressing discomfort in communicating via text message and asking her to email him instead.

“Let’s get off texts please, just email me to that email address”

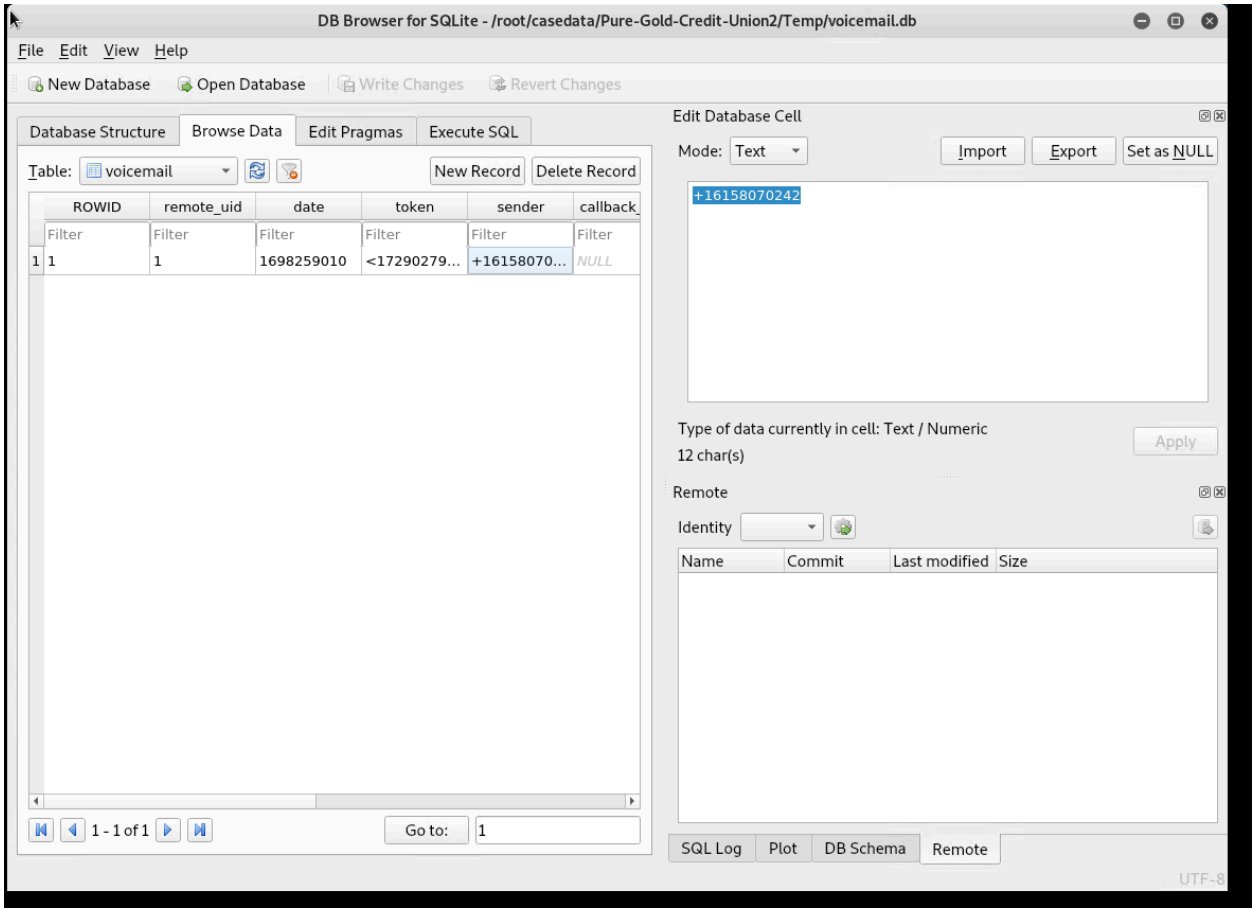


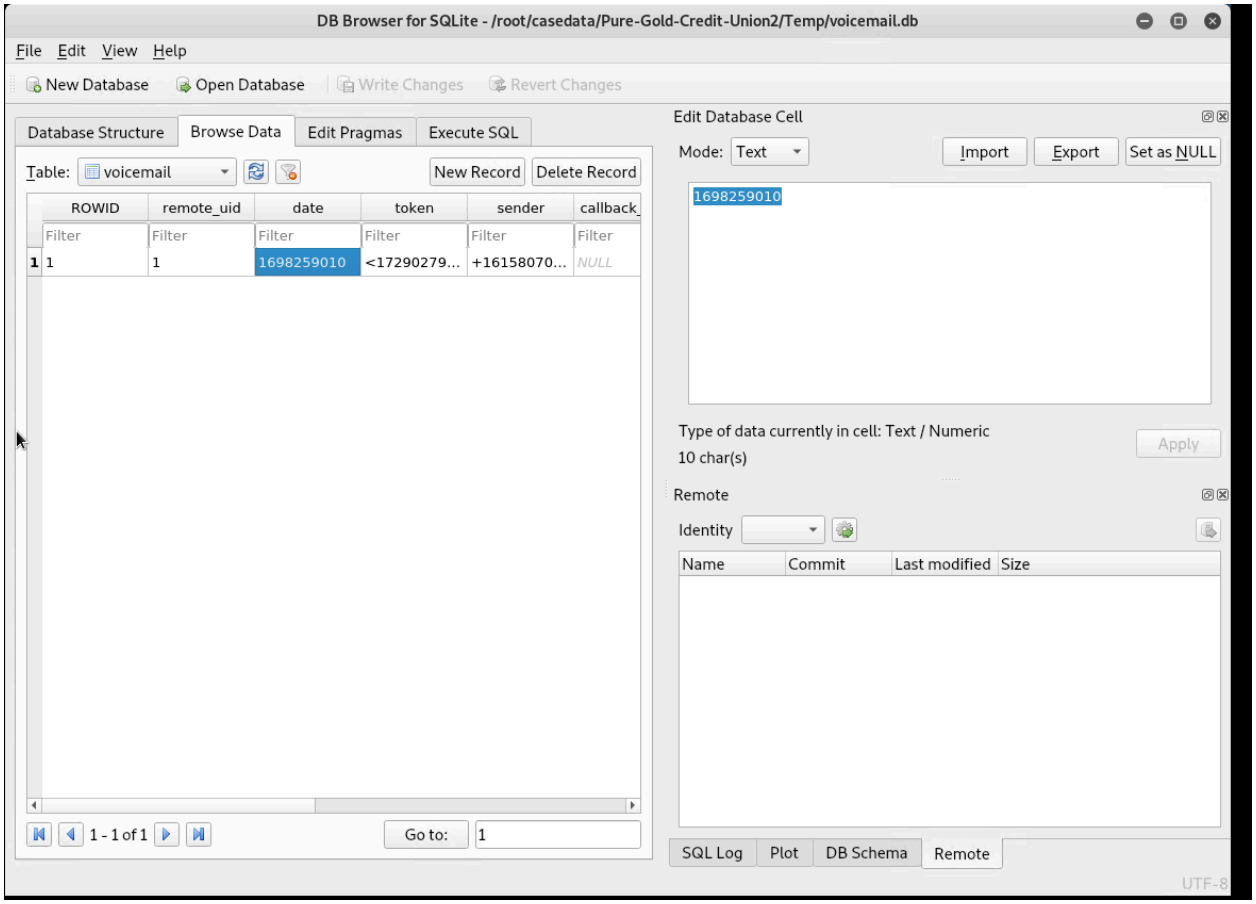
<u>October 25th 2023</u>

At 18:36:50 GMT, Peter Barnes received a voicemail from Oliver Bell. He says Peter and Rosie had cleared over $125,000 in cash. He demands payment but says he'll keep altering the audit records so Evelyn won't get suspicious:

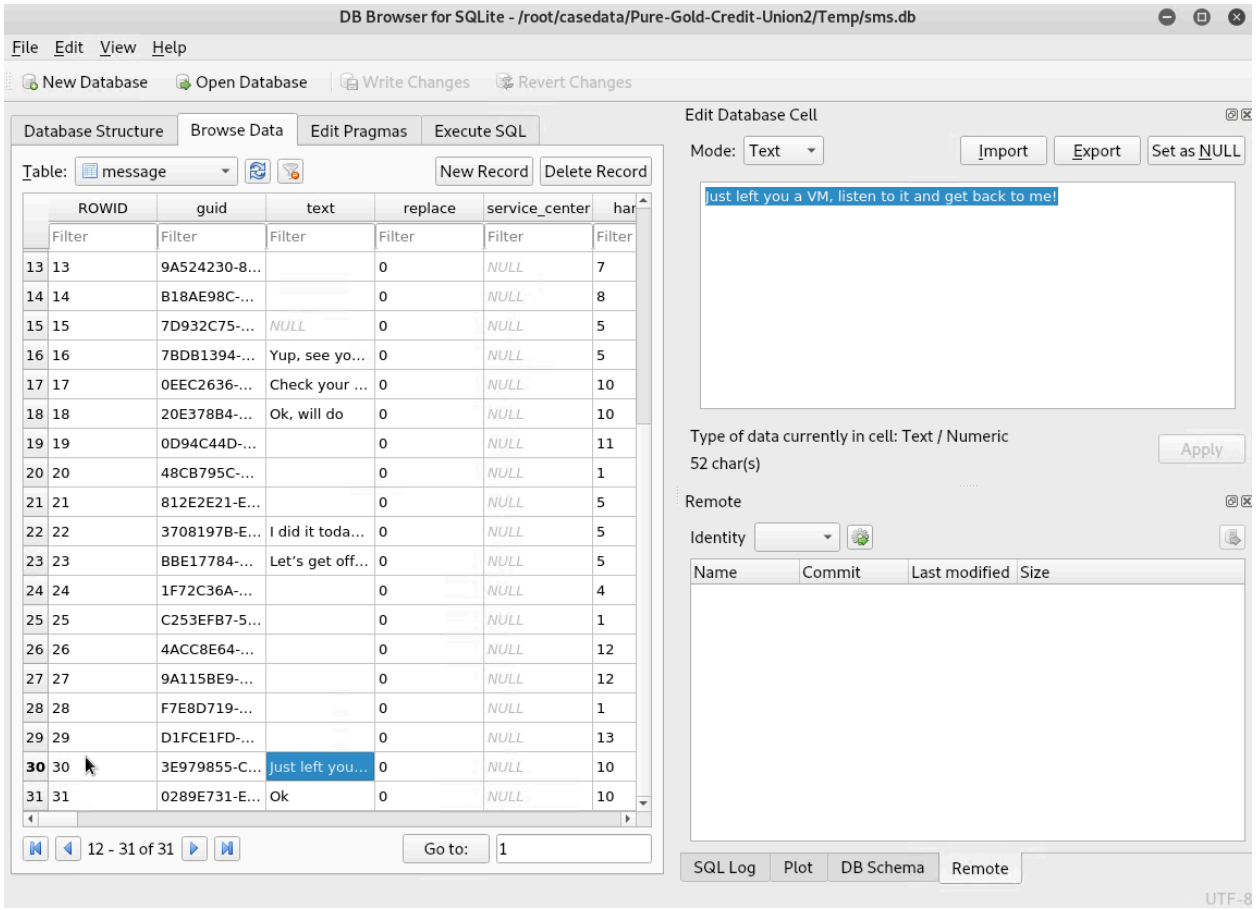
Voicemail Transcript: "Hey, Peter. It's me, your buddy Oliver. From my math, you and Rosie cleared over 125k. Remember though, I get twenty percent and I'll keep clearing the audit records so Evelyn can never catch you. Give me my cash though. Put it in an envelope– leave it at my back door. Pleasure doing business with you."

These screenshots show the voicemail timestamp and phone number captured in SQL Browser. Our team was able to locate the audio file of the voicemail and listen to it using Windows Media Player, confirming to us the identity of "X." They are also close to the time in which Oliver had sent his text message to Peter, telling him to check his voicemail, thus revealing his identity as Mr. X.

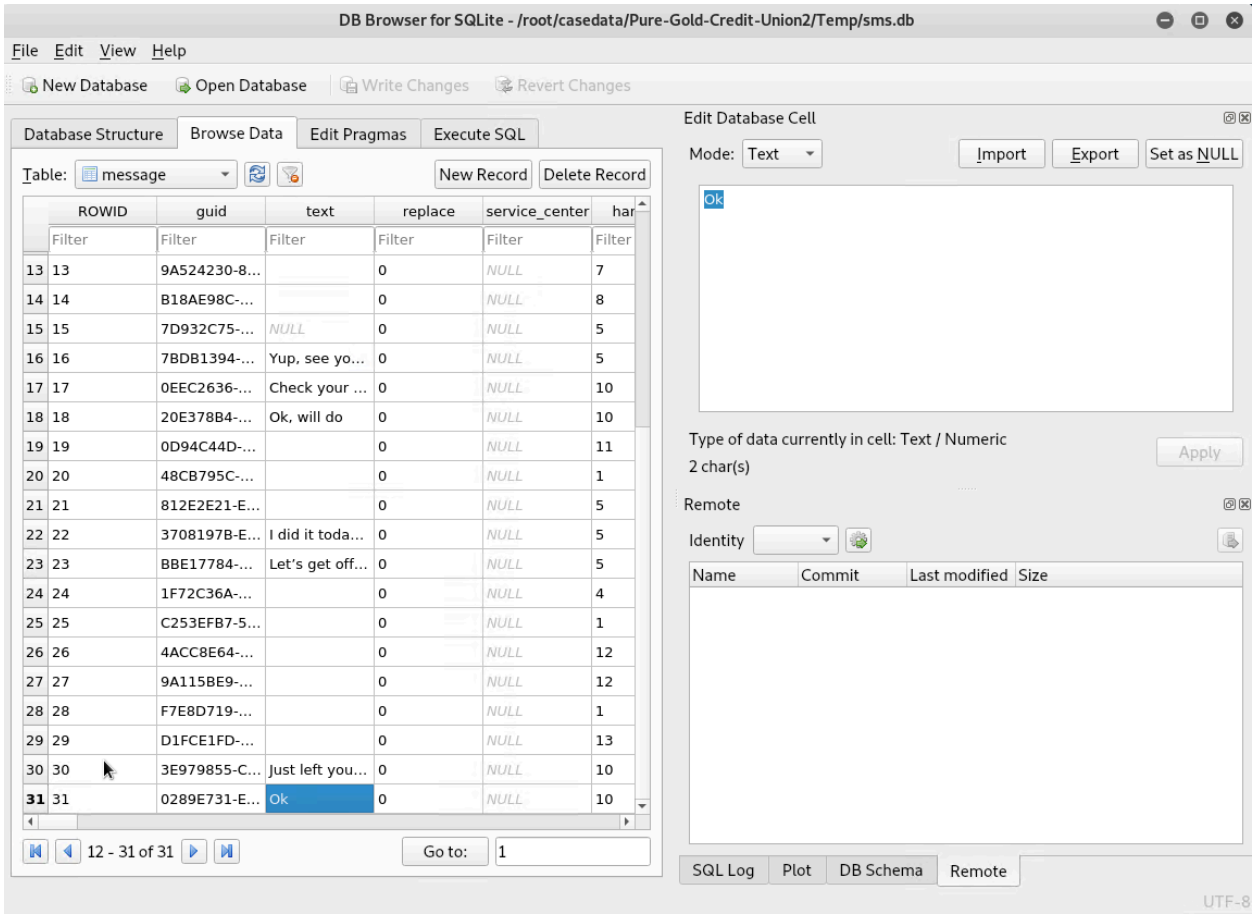

DB Browser for SQLite - /root/casedata/Pure-Gold-Credit-Union2/Temp/voicemail.db
File Edit View Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: voicemail
New Record
Delete Record
ROWID
remote_uid
date
token
sender
callback
Filter
1
1
1
1698259010
<17290279...
+16158070...
NULL
1 - 1 of 1
Go to:
1
Edit Database Cell
Mode: Text
Import
Export
Set as NULL
+16158070242
Type of data currently in cell: Text / Numeric
12 char(s)
Apply
Remote
Identity
Name
Commit
Last modified
Size
SQL Log
Plot
DB Schema
Remote
UTF-8



At 18:37:50 GMT, Peter received a text message from Mr. Bell stating he left Peter a voicemail and to get back to him:
“Just left you a VM, listen to it and get back to me!”



Peter acknowledges the message at 18:38:04 GMT
“Ok.”



Conclusion

Evidence found on Peter"s iPhone indicated the following:

- With the information our team had gathered and analyzed, we can conclude that **three** suspects: Peter Barnes, Rosie Lloyd and Oliver Bell all coordinated and executed the stealing of funds from Pure Gold Credit Union. The emails and text messages show Rosie and Peter had met in person to discuss the details of the crime and solidified their plan over email correspondence. The timestamps of the photographs sent to Peter match the time stamps in which Rosie had said she committed the crime. Also,the timestamps match the times Peter had received his voicemail from Oliver with the text message he received from Oliver telling him to check his voicemail messages. We have also analyzed several messages that proved Peter, Rosie and Oliver were actively discussing, planning and executing this crime. Furthermore, we have evidence that

suggests Peter and Rosie had the intention to cover up their crimes by deleting the evidence they had on their phones. With this evidence laid out on the timeline previously described, we believe Peter Barnes, Rosie Lloyd and Oliver Bell co-conspired with each other to coordinate and execute this crime.

Bonus Conclusion

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

- We can see on Peter's iPhone image data that a voicemail had been received. We were able to extract the information and listen to the voice message. After downloading the amr file and listening to it on our local machine, our team revealed that the identity of Mr. X was District Manager, Oliver Bell.

  Transcript:
  "Hey, Peter. It's me, your buddy Oliver. From my math, you and Rosie cleared over 125k. Remember though, I get twenty percent and I'll keep clearing the audit records so Evelyn can never catch you. Give me my cash though. Put it in an envelope– leave it at my back door. Pleasure doing business with you."

Appendix A: Correspondence Evidence

List any sms attachments and pictures found here

Master Timeline of Email Messages				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Evidence Location**
10	10/12/2023 00:47:25 GMT	To:rosielloyd071292@icloud.com From: peterbarnes12792@icloud.com Subject: Dinner	"Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk about non-work things. Peter Barnes" Peter sending rosie an email about hanging out over the weekend	MessageData/10

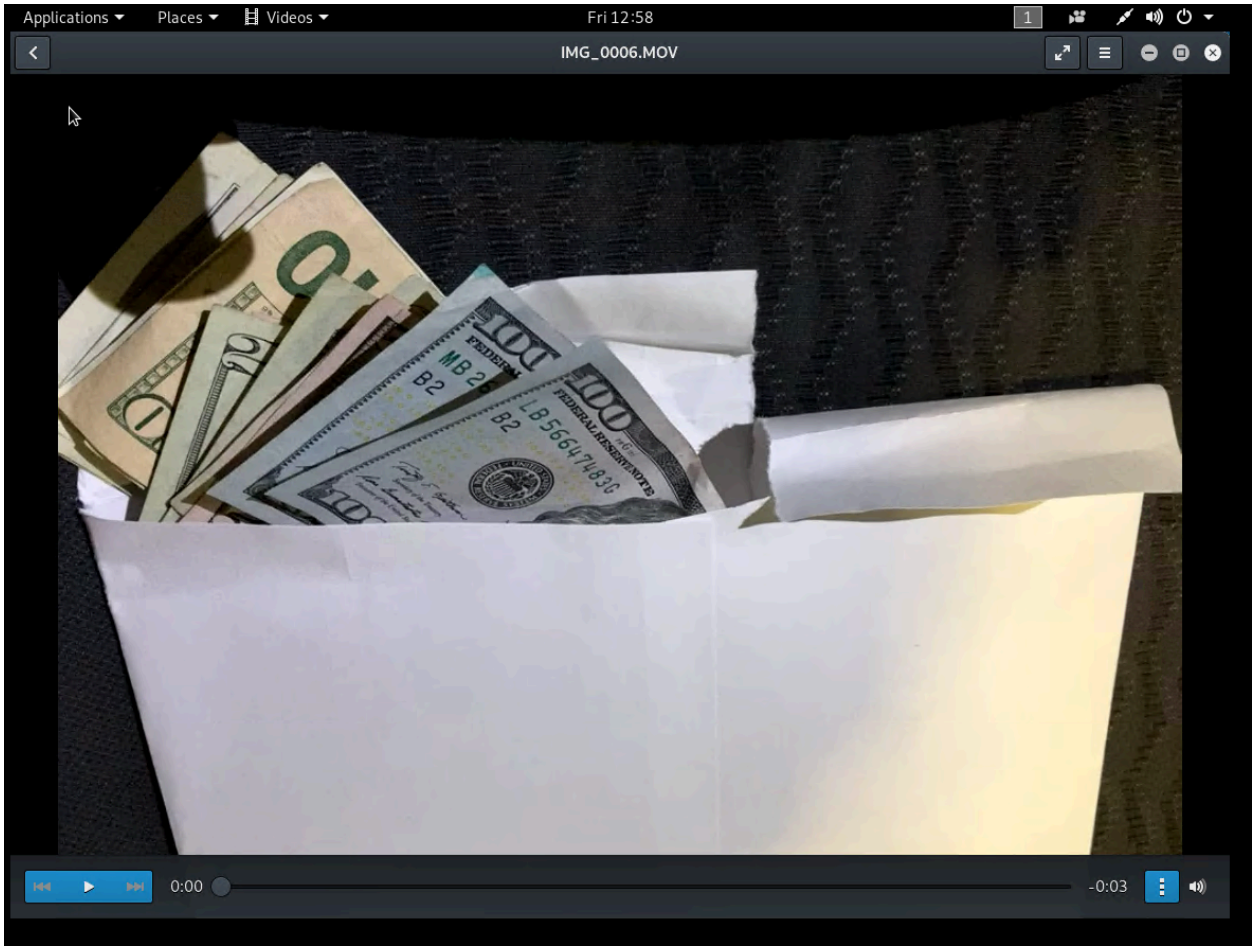
11	10/12/23 22:36:10 GMT	From: rosielloyd071292@icloud.com To: peterbarnes12792@icloud.com Subject: Re: Dinner	“Hey Peter, Likewise, was so great to get a chance to hang out, outside of work. Sounds like we both feel that we aren’t being paid enough and on top of that all the Gold Credit Union executives are pulling up in sports cars. Its really frustrating :(Rosie Lloyd” Rosie expressed resentment towards credit union executives in this email. Establishing a motive.	MessageData/11
12	10/12/23 22:59:41 GMT	From: peterbarnes12792@icloud.com To:rosielloyd071292@icloud.com Subject: Re:Dinner	“I hear you. I’m really frustrated as well. Let's get together after work tonight. I wanted to run something by you. Peter Barnes.” Peter is also resentful of the executives at the credit union. He may be referring to meeting with Rosie again to discuss details to set up the crime.	MessageData/12
13	10/19/23 01:31:24 GMT	From: hockyfan4747@proton.me To:peterbarns12792@icloud.com	Message was encoded with base 64	MessageData/13
14	10/20/23 02:02:43 GMT	From: peterbarnes12792@icloud.com To:rosielloyd071292@icloud.com Subject: Idea	“Great getting together again last night, what did you think of the idea I ran by you? Peter Barnes” Peter and Rosie met the previous night to discuss the plans for the heist.	MessageData/14
15	10/20/23 02:07:43 GMT	From:rosielloyd071292@icloud.com To:peterbarnes12792@icloud.com Subject: Re: Idea	“Honestly, I am intrigued. Was up all night thinking about it, and how we can pull it off. Are you sure =E2=90=9CX=E2=80=9D can help us out? Do you trust X? How about Michaela Rokas?”	MessageData/15

16	10/20/23 02:11:14 GMT	To: rosielloyd071292@icloud.com From: peterbarnes12792@icloud.com Subject: Re: Idea	“I trust X, it was actually X that brought this idea to me a while back. I thought they were kidding but X kept asking. Now after seeing the exec’s getting rich while I have trouble paying my bills, I am ready to put this into action. But I need your help to make this work. You know what to do next? Peter Barnes” Peter committing to executing the crime	MessageData/16
17	10/20/23 2:20:00 GMT	To:peterbarnes12792@icloud.com From:rosielloyd071292@icloud.com Subject: Re: Idea	“Yup, you explained it well last night. Just get me the copies of the forged withdrawal receipts so I can get this going. Also what about Catarina Mona and Lanzo, I think her last name is Agneza? Rosie Lloyd” Rosie and Peter planning to forge the withdrawal receipts from the credit union	MessageData/17
18	10/20/23 2:22:57 GMT	To:rosielloyd071292@icloud.com From:peterbarnes12792@icloud.com Subject: Re: Idea	“Ok, but please try to keep details about this plan off our email. You may also want to delete these emails to remove any traces of evidence. You are being a little reckless and going to get us caught. They are ok, I get along with them for the most part. Peter Barnes.” Peter asking Rosie to cover up the details of their crime.	MessageData/18
19	10/20/23 2:33:47 GMT	To:peterbarnes12792@icloud.com From: rosielloyd071292@icloud.com Subject: Re: Idea	“Ok, I’ll do that, and don’t worry so much. Rosie Lloyd”	MessageData/19
20	10/20/23 2:38:10	To:hockyfan4747@proton.me From:peterbarnes12792@i	This appears to be a reply to an email thread that may have been deleted.	MessageData/20

		cloud.com Subject: Question	Hockyfan4747@proton.me asks, “So, is Roise in? peterbarnes12792@icloud.com replies: “Yes, we are good, should get this going this Friday.” Plans made to complete the crime on Friday	
21	10/20/23 2:43:23 GMT	To:peterbarnes12792@icloud.com From: hockeyfan4747@proton.me Subject: Question	Message is encoded with base64	MessageData/21

Master Timeline of SMS Messages				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Evidence Location**
VM-1	10/25/23 18:36:50 GMT	To: Peter +16155719608 From: Oliver Bell +16158070242	Voicemail Transcript: “Hey, Peter. It’s me, your buddy Oliver. From my math, you and Rosie cleared over 125k. Remember though, I get twenty percent and I’ll keep clearing the audit records so Evelyn can never catch you. Give me my cash though. Put it in an envelope– leave it at my back door. Pleasure doing business with you.”	voicemail.db
30	10/25/23 18:37:50 GMT	To: Peter +16155719608 From: Oliver Bell +16158070242	“Just left you a VM, listen to it and get back to me!” Someone sent Peter a voicemail and is asking them to listen to it	sms.db
31	10/25/23 18:38:04	To: Oliver Bell +16158070242	Ok.	sms.db

	GMT	From: Peter +16155719608		
5	10/18/23 15:39:05 GMT	To: Peter +16155719608 From: Rosie +16154278267	“Dinner Tonight?”	sms.db
6	10/18/23 15:40:48 GMT	To: Rosie +16154278267 From: Peter +16155719608	Reply from Peter: “Yup, see you then” Rosie had texted Peter to meet for dinner to discuss the plans for the heist.	sms.db
7a	10/21/23 00:56:49 GMT	To: Peter +16155719608 From: Rosie +16154278267	**Attachment of photo/video of money sent, see attachment of photo below**	sms.db
7	10/21/23 00:56:57 GMT	To: Peter +16155719608 From: Rosie +16154278267	“I did it today, can’t believe it. Going to the mall later, wanna join me? Also I sent you a picture.” This was when the theft of the money occurred. Rosie wants to make plans to meet Peter at the mall.	sms.db
8	10/21/23 00:59:48 GMT	To: Rosie +16154278267 From:Peter +16155719608	Reply from Peter: “Let’s get off texts please, just email me to that email address” Peter is asking Rosie to get off text messages and would prefer to communicate via email correspondence. A photograph of the money was sent as an attachment	sms.db



Appendix B: GPS Location Information

GPS Evidence from https://onlineexifviewer.com/ placed the geographic data of the HEIC file south of Nashville, TN, in the City of Brentwood, Tennessee. Specifically, it appears the location is in a parking lot of a Best Buy store.

https://www.google.com/maps/place/35%C2%B058'13.6%22N+86%C2%B048'26.6%22W/@35.97045,-86.8073889,17z/data=!3m1!4b1!4m4!3m3!8m2!3d35.97045!4d-86.8073889?entry=ttu&g_ep=EgoyMDI0MDkxNi4wIKXMDSoASAFQAw%3D%3D

35° 58' 13.62" N 86° 48' 26.6" W