



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.

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.

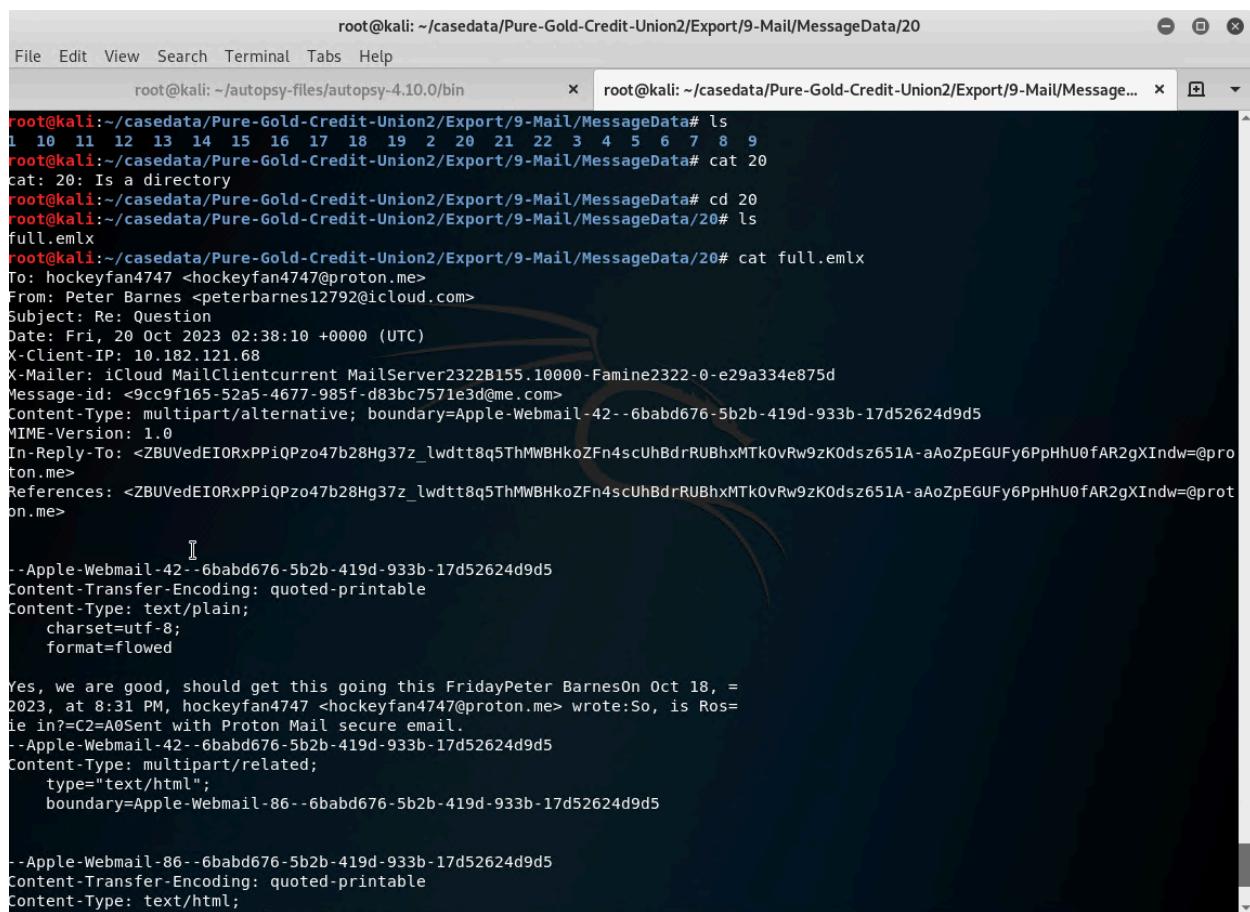
Mr. Barnes had also communicated with District Manager, Mr. Oliver Bell through email, SMS and voicemail communications. We were able to determine that Mr. Bell was using the email hockeyfan4747@proton.me because we were able to triangulate the timestamps associated with his text messages he sent corresponding 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, hockeyfan4747@proton.me asks if Rosie is "in" and Peter Barnes replies, "Yes we are all set. Should get this going on Friday."



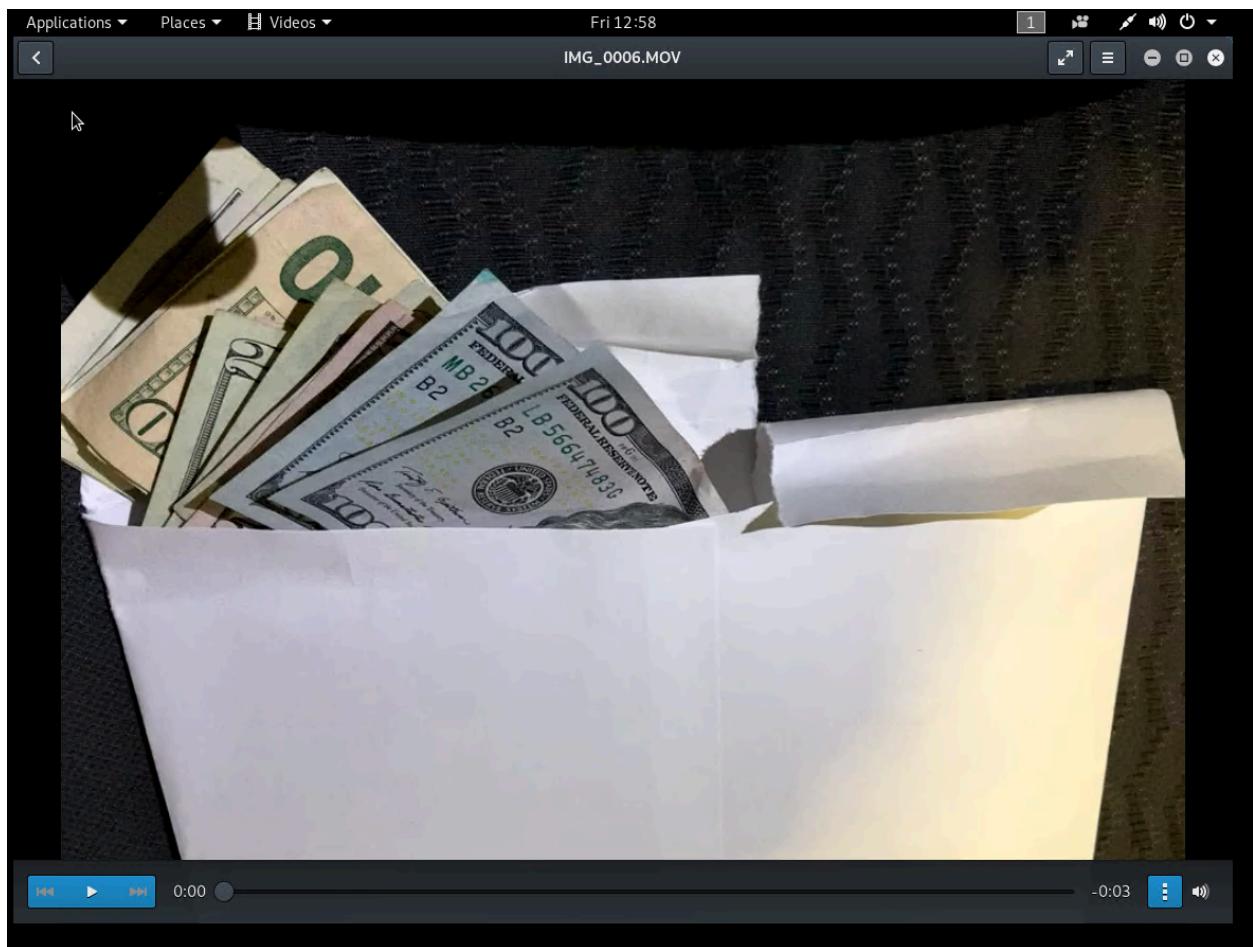
```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin      x  root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/Message...
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# ls
1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 3 4 5 6 7 8 9
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cat 20
cat: 20: Is a directory
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cd 20
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20# ls
full.emlx
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20# cat full.emlx
To: hockeyfan4747 <hockeyfan4747@proton.me>
From: Peter Barnes <peterbarnes12792@icloud.com>
Subject: Re: Question
Date: Fri, 20 Oct 2023 02:38:10 +0000 (UTC)
X-Client-IP: 10.182.121.68
X-Mailer: iCloud MailClientcurrent MailServer2322B155.10000-Famine2322-0-e29a334e875d
Message-id: <9cc9f165-52a5-4677-985f-d83bc7571e3d@me.com>
Content-Type: multipart/alternative; boundary=Apple-Webmail-42--6babd676-5b2b-419d-933b-17d52624d9d5
MIME-Version: 1.0
In-Reply-To: <ZBUVedEI0RxPPiQPzo47b28Hg37z_lwdtt8q5ThMWBHkoZFn4scUhBdrRUBhxMTk0vRw9zK0dsz651A-aAoZpEGUFy6PpHhU0fAR2gXIndw=@proton.me>
References: <ZBUVedEI0RxPPiQPzo47b28Hg37z_lwdtt8q5ThMWBHkoZFn4scUhBdrRUBhxMTk0vRw9zK0dsz651A-aAoZpEGUFy6PpHhU0fAR2gXIndw=@proton.me>

--Apple-Webmail-42--6babd676-5b2b-419d-933b-17d52624d9d5
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

Yes, we are good, should get this going this FridayPeter BarnesOn Oct 18, = 2023, at 8:31 PM, hockeyfan4747 <hockeyfan4747@proton.me> wrote:So, is Rosie in?=C2=A0Sent with Proton Mail secure email.
--Apple-Webmail-42--6babd676-5b2b-419d-933b-17d52624d9d5
Content-Type: multipart/related;
type="text/html";
boundary=Apple-Webmail-86--6babd676-5b2b-419d-933b-17d52624d9d5

--Apple-Webmail-86--6babd676-5b2b-419d-933b-17d52624d9d5
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
```

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.



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	AEFD4110-...		0	NULL	4
2	64CE5E08-5...		0	NULL	4
3	5066759A-F...	NULL	0	NULL	4
4	2A50A0CA-...		0	NULL	4
5	7D932C75-...	Dinner toni...	0	NULL	4
6	7BDB1394-...	Yup, see yo...	0	NULL	4
7	812E2E21-E...	I did it toda...	0	NULL	4
8	3708197B-E...	NULL	0	NULL	4
9	B8E17784-...	Let's get off...	0	NULL	4

1 - 9 of 9 Go to: 1

Edit Database Cell
Mode: Text Import Export Set as NULL

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

Type of data currently in cell: Text / Numeric
102 char(s) Apply

Remote Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

SQL Log Plot DB Schema Remote

UTF-8

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"

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	har
13	13	9A524230-8...	0	NULL	7
14	14	B18AE98C-...	0	NULL	8
15	15	7D932C75-...	NULL	0	5
16	16	7BDB1394-...	Yup, see yo...	0	5
17	17	0EEC2636-...	Check your ...	0	10
18	18	20E378B4-...	Ok, will do	0	10
19	19	0D94C44D-...		0	11
20	20	48CB795C-...		0	1
21	21	812E2E21-E...		0	5
22	22	3708197B-E...	I did it toda...	0	5
23	23	BBE17784-...	Let's get off...	0	5
24	24	1F72C36A-...		0	4
25	25	C253EFB7-5...		0	1
26	26	4ACC8E64-...		0	12
27	27	9A115BE9-...		0	12
28	28	F7E8D719-...		0	1
29	29	D1FCE1FD-...		0	13
30	30	3E979855-C...	Just left you...	0	10
31	31	0289E731-E...	Ok	0	10

12 - 31 of 31 Go to: 1

Edit Database Cell Mode: Text Import Export Set as NULL

Let's get off texts please, just email me to that email address.

Type of data currently in cell: Text / Numeric 67 char(s) Apply

Remote Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

SQL Log Plot DB Schema Remote

UTF-8

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
1	1	1698259010	<17290279...	+16158070...	NULL

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

1 - 1 of 1 Go to: 1

The screenshot shows the DB Browser for SQLite interface. The main window displays a table named 'voicemail' with one row. The columns are 'ROWID', 'remote_uid', 'date', 'token', 'sender', and 'callback'. The data for the first row is: ROWID=1, remote_uid=1, date=1698259010, token=<17290279..., sender=+16158070..., callback=NULL. The 'Edit Pragmas' tab is selected. On the right, there's an 'Edit Database Cell' panel with the value '+16158070242' and a dropdown set to 'Text'. Below it, a message says 'Type of data currently in cell: Text / Numeric 12 char(s)' with an 'Apply' button. A 'Remote' section is also visible.

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
1	1	1698259010	<17290279...	+16158070...	NULL

Edit Database Cell

Mode: Text Import Export Set as NULL

1698259010

Type of data currently in cell: Text / Numeric
10 char(s)
Apply

Remote

Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

SQL Log Plot DB Schema Remote

1 - 1 of 1 Go to: 1

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”

```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/10
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin x root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/10#
full.emlx
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/10# cat full.emlx
To: rosielloyd071292@icloud.com
From: Peter Barnes <peterbarnes12792@icloud.com>
Subject: Dinner
Date: Thu, 12 Oct 2023 00:47:25 +0000 (UTC)
X-Client-IP: 10.182.149.140
X-Mailer: iCloud MailClientcurrent MailServer2322B155.10000-Famine2322-0-e29a334e875d
Message-id: <0bf02314-7420-4010-b0f4-c16f0e96844d@me.com>
Content-Type: multipart/alternative; boundary=Apple-Webmail-42--7cf28b23-0202-4563-8c70-36f17308df19
 MIME-Version: 1.0

--Apple-Webmail-42--7cf28b23-0202-4563-8c70-36f17308df19
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
 charset=utf-8;
 format=flowed

Hey Rosie, great hanging out with you this weekend! Always good to hang ou=
t and talk about non work things.Peter Barnes
--Apple-Webmail-42--7cf28b23-0202-4563-8c70-36f17308df19
Content-Type: multipart/related;
 type="text/html";
 boundary=Apple-Webmail-86--7cf28b23-0202-4563-8c70-36f17308df19

--Apple-Webmail-86--7cf28b23-0202-4563-8c70-36f17308df19
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
 charset=utf-8;

<html><body><div>Hey Rosie, great hanging out with you this weekend! Always good to ha=
ng out and talk about non work things.<br></div><div><br></div><div>Peter =
Barnes</div></body></html>
--Apple-Webmail-86--7cf28b23-0202-4563-8c70-36f17308df19--
--Apple-Webmail-42--7cf28b23-0202-4563-8c70-36f17308df19--

root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/10#
```

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"

```
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

Hey=0A Peter, Likewise, was so great to get a chance to hang out, outside=
of=0A work.=C2=A0 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 p=
ulling up in sports cars.=C2=A0 Its really frustrating :( .Rosie Llyod@0=
ct 11, 2023, at 7:47 PM, Peter Barnes <peterbarnes12792@icloud.com> wrote:=
Hey Rosie, great hanging out with you this weekend! Always good to hang ou=
t 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 &lt;peterbarnes12792@icloud.com&gt; wrote:<br><=
div><br><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><br><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--

root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/11# S
```

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."

```

root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/12
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin      x  root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/12#
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cd 12
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/12# ls
full.emlx
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/12# cat full.emlx
To: Rosie Lloyd <rosielloyd071292@icloud.com>
From: Peter Barnes <peterbarnes12792@icloud.com>
Subject: Re: Dinner
Date: Thu, 12 Oct 2023 22:59:41 +0000 (UTC)
X-Client-IP: 10.182.151.232
X-Mailer: icloud MailClientcurrent MailServer2322B155.10000-Famine2322-0-e29a334e875d
Message-ID: <2e73a5a0-650f-4720-92cd-4804d64243dd@me.com>
Content-Type: multipart/alternative; boundary=Apple-Webmail-42--55d11a3c-7623-4b1c-be9e-408e7f33b059
MIME-Version: 1.0
In-Reply-To: <97eafb56-cb36-4f52-b21c-6bf9bea75ac8@me.com>
References: <0bf02314-7420-4010-b0f4-c16f0e96844d@me.com>
<97eafb56-cb36-4f52-b21c-6bf9bea75ac8@me.com>

--Apple-Webmail-42--55d11a3c-7623-4b1c-be9e-408e7f33b059
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

I hear=0A you, I=E2=80=99m really frustrated as well. Lets get together a=
fter work tonight.=0A wanted to run something by you.Peter BarnesOn Oct 1=
2, 2023, at 5:36 PM, Rosie Lloyd <rosielloyd071292@icloud.com> wrote:Hey=0A=
Peter, Likewise, was so great to get a chance to hang out, outside of=0A=
work.=C2=A0 Sounds like we both feel that we=0A aren't being paid enoug=
h, and on top of that all the Gold Credit Union=0A executives are pulling=
up in sports cars.=C2=A0 Its really frustrating :( .Rosie LlyodOn Oct 11, =
2023, at 7:47 PM, Peter Barnes <peterbarnes12792@icloud.com> wrote:Hey Ro=
sie, great hanging out with you this weekend! Always good to hang out and =
talk about non work things.Peter Barnes
--Apple-Webmail-42--55d11a3c-7623-4b1c-be9e-408e7f33b059
Content-Type: multipart/related;
type="text/html";
boundary=Apple-Webmail-86--55d11a3c-7623-4b1c-be9e-408e7f33b059

--Apple-Webmail-86--55d11a3c-7623-4b1c-be9e-408e7f33b059

```

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.

October 18th, 2023

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	B8E17784-...	Let's get off...	0	NULL	4

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

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	har
13	13	9A524230-8...		0	NULL
14	14	B18AE98C-...		0	NULL
15	15	7D932C75-...	NULL	0	NULL
16	16	7BDB1394-...	Yup, see you then		5
17	17	0EEC2636-...	Check your ...	0	NULL
18	18	20E378B4-...	Ok, will do	0	NULL
19	19	0D94C44D-...		0	NULL
20	20	48CB795C-...		0	NULL
21	21	812E2E21-E...		0	NULL
22	22	3708197B-E...	I did it toda...	0	NULL
23	23	BBE17784-...	Let's get off...	0	NULL
24	24	1F72C36A-...		0	NULL
25	25	C253EFB7-5...		0	NULL
26	26	4ACC8E64-...		0	NULL
27	27	9A115BE9-...		0	NULL
28	28	F7E8D719-...		0	NULL
29	29	D1FCE1FD-...		0	NULL
30	30	3E979855-C...	just left you...	0	NULL
31	31	0289E731-E...	Ok	0	NULL

12 - 31 of 31 Go to: 1

Edit Database Cell Mode: Text Import Export Set as NULL

Yup, see you then

Type of data currently in cell: Text / Numeric
18 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

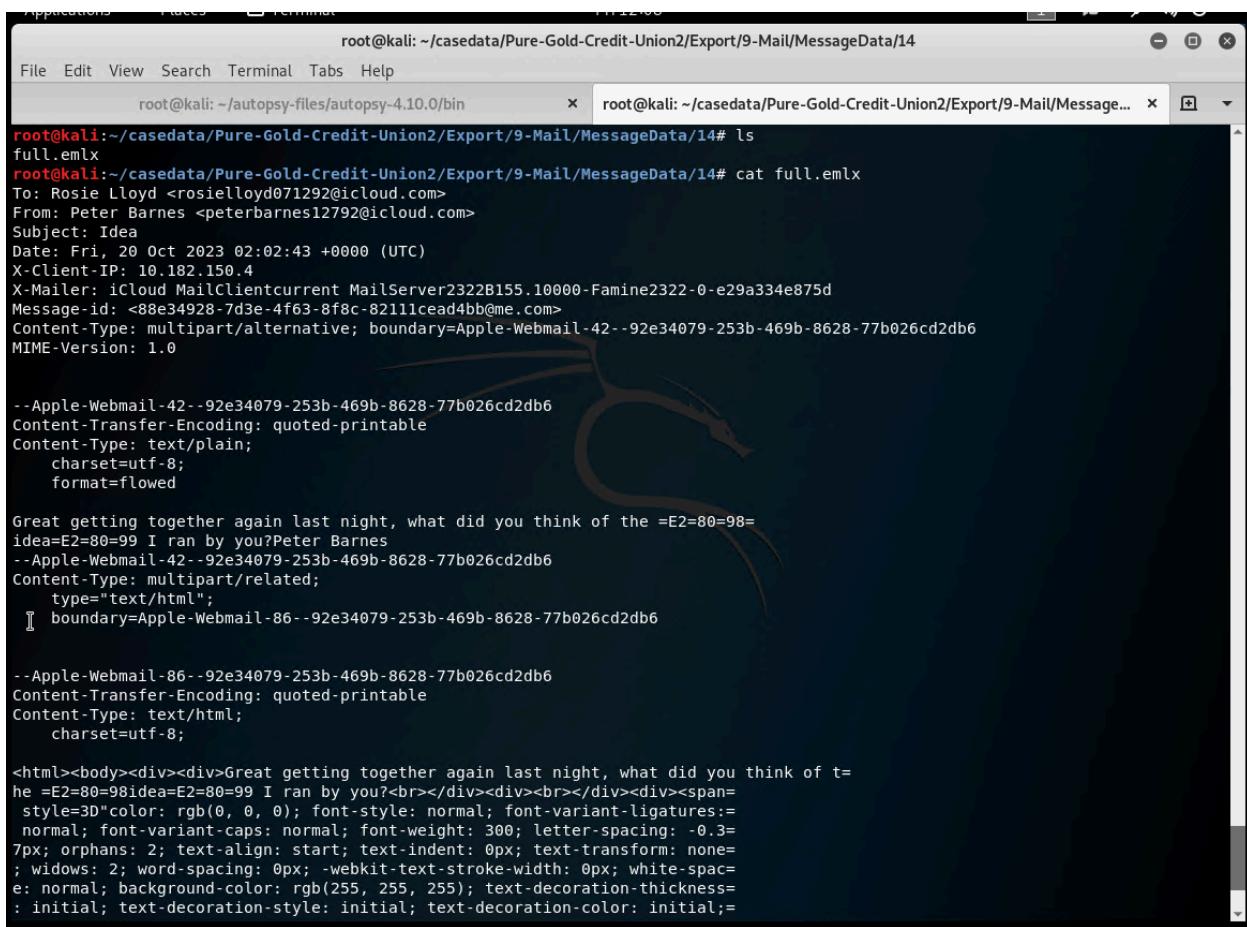
message or a file had been sent over.

```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/13
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin x root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData...
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/12# cd ..
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cd 13
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/13# ls
full.emlx
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/13# cat full.emlx
Return-path: <hockeyfan4747@proton.me>
Original-recipient: rfc822;peterbarnes12792@icloud.com
Received: from ci74p00im-qukt09070101.me.com by p115-mailgateway-smtp-6c5746c486-7z8g2 (mailgateway 2401B119)
    with SMTP id 90a6b59a-51e8-4d40-8130-0df83b960873
        for <peterbarnes12792@icloud.com>; Thu, 19 Oct 2023 01:31:24 GMT
X-Apple-MoveToFolder: INBOX
X-Apple-Action: MOVE_TO_FOLDER/INBOX
X-Apple-UUID: 90a6b59a-51e8-4d40-8130-0df83b960873
Received: from mail-40138.protonmail.ch (mail-40138.protonmail.ch [185.70.40.138])
    by ci74p00im-qukt09070101.me.com (Postfix) with ESMTPS id 3789A1200239
        for <peterbarnes12792@icloud.com>; Thu, 19 Oct 2023 01:31:21 +0000 (UTC)
X-ICL-SCORE: 3.333033230041
X-ICL-INFO: GatbVUseBVFGSVVEsgMGUKFIRFcUWUIPApbVRYSFhEAREQZF15TqFUcAkpaWFkBhHwfERLeAlVB
TiYHcl9CDRTxCxjaEFAGSFsWBrdEWQxbFANVWFnfkhbv09NhgFSw01WwukDdkBvEQMbFw0UDxQQ
ClpMAAdRTVcWBrdEWQwYGA8bVlNeQFUJEgVFElSDHBVLQ0gBBVpbCRQYDF9YDxQQC1kbWBRCER1b
VQhCWRYaF0gaHRIWDxwd1VEanQ3IxwCMjF/ZBolKQ8mKEpZVKibVE8wvwVVdyYKABxEQloETDf
Nwd0Kh4WPDEWBEUBIBEKewp1yAdASsjE39AMAJAHd3VEUYQ0xXLVRdw0vCSmWLXZPVCUJLh8t
AFAjJ0sBLzFeUhVI0RYFF0RZDFsUA0laEEQBFSWEgxVRAAUcwEEVUxLjh4bXFkXEVCFCGBUS
Authentication-Results: bimi.icloud.com; bimi=declined
X-ARC-Info: policy=fail; arc=None
Authentication-Results: arc.icloud.com; arc=None
Authentication-Results: dmarc.icloud.com; dmarc=pass header.from=proton.me
X-DMARC-Info: pass=pass; dmarc-policy=quarantine; s=s1; d=s1; pdomain=proton.me
X-DMARC-Policy: v=DMARC1; p=quarantine; fo=1; aspf=s; adkim=s;
Authentication-Results: dkim-verifier.icloud.com;
    dkim=pass (2048-bit key) header.d=proton.me header.i=@proton.me header.b=V8vLn/mw
Authentication-Results: spf.icloud.com; spf=pass (spf.icloud.com: domain of hockeyfan4747@proton.me designates 185.70.40.138 as permitted sender) smtp.mailfrom=hockeyfan4747@proton.me
Received-SPF: pass (spf.icloud.com: domain of hockeyfan4747@proton.me designates 185.70.40.138 as permitted sender) receiver=pf.icloud.com; client-ip=185.70.40.138; helo=mail-40138.protonmail.ch; envelope-from=hockeyfan4747@proton.me
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=proton.me;
    s=protonmail; f=t=1697679679; x=1697938279;
    b=uZMwQJc9emktV0vVLkjnMnEvDUZ5LTGsJy+vR97NXBQ=;
    h=Date:To:From:Subject:Message-ID:Feedback-ID:From:To:Cc:Date:
    Subject:Reply-To:Feedback-ID:Message-ID:BIMI-Selector;
    b=V8vLn/mwW60MYQBacnLwSEywxywilAdQqsWrCpzOr5UINox4waSQSlqJCC1gKV8
```

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”



The screenshot shows a terminal window with two tabs. The left tab shows the command 'ls' being run in the directory '/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/14'. The right tab shows the command 'cat full.emlx' being run in the same directory. The output of the 'cat' command displays an email message in EMLX format. The message is from Rosie Lloyd to Peter Barnes, dated October 20, 2023, at 02:02:43 UTC. It contains a single-line text body: "Great getting together again last night, what did you think of the =E2=80=98=idea=E2=80=99 I ran by you?Peter Barnes". The terminal window has a dark background with a Kali Linux logo watermark.

```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/14
root@kali: ~/autopsy-files/autopsy-4.10.0/bin      x  root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/Message...
File Edit View Search Terminal Tabs Help
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/14# ls
full.emlx
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/14# cat full.emlx
To: Rosie Lloyd <rosielloyd071292@icloud.com>
From: Peter Barnes <peterbarnes12792@icloud.com>
Subject: Idea
Date: Fri, 20 Oct 2023 02:02:43 +0000 (UTC)
X-Client-IP: 10.182.150.4
X-Mailer: iCloud MailClientcurrent MailServer2322B155.10000-Famine2322-0-e29a334e875d
Message-id: <88e34928-7d3e-4f63-8f8c-82111cead4bb@me.com>
Content-Type: multipart/alternative; boundary=Apple-Webmail-42--92e34079-253b-469b-8628-77b026cd2db6
MIME-Version: 1.0

--Apple-Webmail-42--92e34079-253b-469b-8628-77b026cd2db6
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

Great getting together again last night, what did you think of the =E2=80=98=
idea=E2=80=99 I ran by you?Peter Barnes
--Apple-Webmail-42--92e34079-253b-469b-8628-77b026cd2db6
Content-Type: multipart/related;
type="text/html";
boundary=Apple-Webmail-86--92e34079-253b-469b-8628-77b026cd2db6

--Apple-Webmail-86--92e34079-253b-469b-8628-77b026cd2db6
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
charset=utf-8;

<html><body><div><div>Great getting together again last night, what did you think of t=
he =E2=80=98idea=E2=80=99 I ran by you?<br></div><br></div><div><span>
style=3D"color: rgb(0, 0, 0); font-style: normal; font-variant-ligatures:=
normal; font-variant-caps: normal; font-weight: 300; letter-spacing: -0.3=
7px; orphans: 2; text-align: start; text-indent: 0px; text-transform: none=
; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; white-spac=
e: normal; background-color: rgb(255, 255, 255); text-decoration-thickness=
: initial; text-decoration-style: initial; text-decoration-color: initial;=
```

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?”

```

root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/15
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin x root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/Message... x
X-CLX-UnSpecialScore: 305
X-CLX-Spam: false
X-Proofpoint-GUID: cDjuDAHxgMPByxypGl91MrwpK02YNrIj
X-Proofpoint-ORIG-GUID: cDjuDAHxgMPByxypGl91MrwpK02YNrIj
X-Proofpoint-Virus-Version: =?UTF-8?Q?vendor=3Dfsecure_engine=3D1.1.170-22c6f66c430a71ce266a39bfe25bc?=
=?UTF-8?Q?2903e8d5c8f:6.0.573,18.0.572,17.0.605.474.000000_definitions?=
=?UTF-8?Q?3D2023-05-17=5F02,2020-02-14=5F11,2020-01-23?=
=?UTF-8?Q?5F02_signatures=3D07=
X-Proofpoint-Spam-Details: rule=notspam policy=default score=0 phishscore=0 mlxlogscore=581
malwarescore=0 clxscore=1005 mlxscore=0 bulkscore=0 suspectscore=0
spamscore=0 adultscore=0 classifier=spam adjust=0 reason=mlx scancount=1
engine=8.12.0-2308100000 definitions=main-2310200017

--Apple-Webmail-42--db06e907-0e92-4ff6-b466-5b67df92a66a
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

Honestly, I am intrigued.=C2=A0 Was up all night thinking about it, and ho=
ut we can pull it off.=C2=A0 Are you sure =E2=80=9CX=E2=80=9D can help us o=
ut?=C2=A0 Do you trust X ?=C2=A0 How about Michaela Rokas ?Rosie LloydOn 0=
ct 19, 2023, at 9:02 PM, Peter Barnes <peterbarnes12792@icloud.com> wrote:=
Great getting together again last night, what did you think of the =E2=80=98=
idea=E2=80=99 I ran by you?Peter Barnes
--Apple-Webmail-42--db06e907-0e92-4ff6-b466-5b67df92a66a
Content-Type: multipart/related;
type="text/html";
boundary=Apple-Webmail-86--db06e907-0e92-4ff6-b466-5b67df92a66a

--Apple-Webmail-86--db06e907-0e92-4ff6-b466-5b67df92a66a
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
charset=utf-8;

<html><body><div><div>Honestly, I am intrigued.&nbsp; Was up all night thinking about =
it, and how we can pull it off.&nbsp; Are you sure =E2=80=9CX=E2=80=9D can=
help us out?&nbsp; Do you trust X ?&nbsp; How about Michaela Rokas ?<br><=
/di><div><br></div><div>Rosie Lloyd</div><div><br></div><div><br></div><div>

```

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"

```

root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/16
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin      x  root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/Message...
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/15# cd ..
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cd 16
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/16# ls
full.emlx
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/16# cat full.emlx
To: Rosie Lloyd <rosielloyd071292@icloud.com>
From: Peter Barnes <peterbarnes12792@icloud.com>
Subject: Re: Idea
Date: Fri, 20 Oct 2023 02:11:14 +0000 (UTC)
X-Client-IP: 10.182.149.48
X-Mailer: iCloud MailClientcurrent MailServer2322B155.10000-Famine2322-0-e29a334e875d
Message-ID: <3b2b3871-aac6-41f1-890a-532a6900a08d@me.com>
Content-Type: multipart/alternative; boundary=Apple-Webmail-42--72c7276e-88ce-47fc-a6ac-cc74d36cdedb
MIME-Version: 1.0
In-Reply-To: <725819e3-a47e-4f7e-a6b1-48fbfacc493a@me.com>
References: <88e34928-7d3e-4f63-8f8c-8211cead4bb@me.com>
<725819e3-a47e-4f7e-a6b1-48fbfacc493a@me.com>

--Apple-Webmail-42--72c7276e-88ce-47fc-a6ac-cc74d36cdedb
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

I trust X, it was actually X that brought this idea to me a while back.=C2=A0 I thought they were kidding, but X kept asking.=C2=A0 Now after seeing= the exec=E2=80=99s getting rich while I have trouble paying my bills, I a= m ready to put this into action.=C2=A0 But I need your help to make this w= ork. You know what to do next?Peter BarnesOn Oct 19, 2023, at 9:07 PM, Ros= ie Lloyd <rosielloyd071292@icloud.com> wrote:Honestly, I am intrigued.=C2=A0= Was up all night thinking about it, and how we can pull it off.=C2=A0 Are= you sure =E2=80=99X=E2=80=99 can help us out?=C2=A0 Do you trust X ?=C2=A0= How about Michaela Rokas ?Rosie LloydOn Oct 19, 2023, at 9:02 PM, Peter B= arnes <peterbarnes12792@icloud.com> wrote:Great getting together again las= t night, what did you think of the =E2=80=99idea=E2=80=99 I ran by you?Pet= er Barnes
--Apple-Webmail-42--72c7276e-88ce-47fc-a6ac-cc74d36cdedb
Content-Type: multipart/related;
type="text/html";
boundary=Apple-Webmail-86--72c7276e-88ce-47fc-a6ac-cc74d36cdedb

```

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”

```

X-CLX-UnSpecialScore: 110
X-CLX-Spam: false
X-Proofpoint-ORIG-GUID: KHSLCCG0EXCAVBRTXFLM1Y1XK3LXALG
X-Proofpoint-GUID: KHSLCCG0EXCAVBRTXFLM1Y1XK3LXALG
X-Proofpoint-Virus-Version: =?UTF-8?Q?2903e8d5c8f:6.0.138,18.0.957,17.11.176.26.000000_definitions?=
=?UTF-8?Q?=3D2023-07-31=5F15:2020-02-14=5F02,2023-07-31=5F15,2023-05-22?=
=?UTF-8?Q?=5F02_signatures=3D07=
X-Proofpoint-Spam-Details: rule=notspam policy=default score=0 suspectscore=0 mlxlogscore=657
mlxscore=0 bulkscore=0 phishscore=0 malwarescore=0 adultscore=0
spamscore=0 clxscore=1005 classifier=spam adjust=0 reason=mlx scancount=1
engine=8.12.0-2308100000 definitions=main-2310200019

--Apple-Webmail-42--fba50aac-cbcf-49e9-aae3-f8f20ec7ad80
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
    charset=utf-8;
    format=flowed

Yup, you explained it well last night.=C2=A0 Just get me the copies of the forged withdrawal receipts so I can get this going. Also, what about Cata=rina Mona and Lanzo, I think her last name is Agneza ?=C2=A0Rosie LloydOn = Oct 19, 2023, at 9:11 PM, Peter Barnes <peterbarnes12792@icloud.com> wrote= :I trust X, it was actually X that brought this idea to me a while back.=C2=A0 I thought they were kidding, but X kept asking.=C2=A0 Now after seeing= the exec=E2=80=99s getting rich while I have trouble paying my bills, I a= m ready to put this into action.=C2=A0 But I need your help to make this w= ork. You know what to do next?Peter BarnesOn Oct 19, 2023, at 9:07 PM, Ros= ie Lloyd <rosie@lloyd071292@icloud.com> wrote:Honestly, I am intrigued.=C2=A0= Was up all night thinking about it, and how we can pull it off.=C2=A0 Are= You sure =E2=80=9CX=E2=80=9D can help us out?=C2=A0 Do you trust X ?=C2=A0= How about Michaela Rokas ?Rosie LloydOn Oct 19, 2023, at 9:02 PM, Peter B= arnes <peterbarnes12792@icloud.com> wrote:Great getting together again las= t night, what did you think of the =E2=80=98idea=E2=80=99 I ran by you?Pet= er Barnes
--Apple-Webmail-42--fba50aac-cbcf-49e9-aae3-f8f20ec7ad80
Content-Type: multipart/related;
    type="text/html";
    boundary=Apple-Webmail-86--fba50aac-cbcf-49e9-aae3-f8f20ec7ad80

```

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.”

```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/18
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin x root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/Message... x
In-Reply-To: <bd0edf6f-b2b7-4847-81e7-5f1dc669eef4@me.com>
References: <88e34928-7d3e-4f63-8f8c-8211cead4bb@me.com>
<725819e3-a47e-4f7e-a6b1-48fbacc493a@me.com>
<3b2b3871-aac6-41f1-890a-532a6900a08d@me.com>
<bd0edf6f-b2b7-4847-81e7-5f1dc669eef4@me.com>

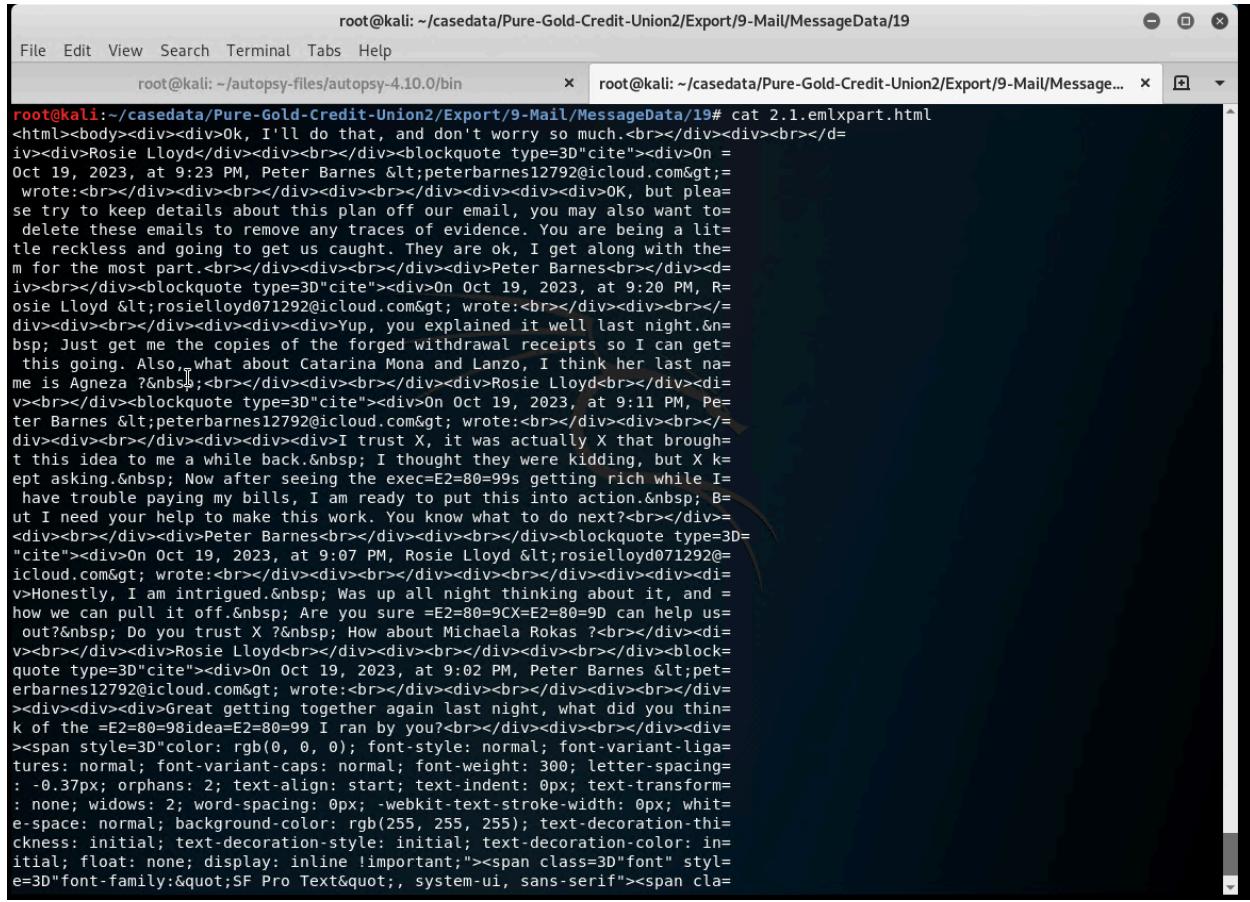
--Apple-Webmail-42--8c916441-07b1-4508-98b8-c26c01f865df
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
    charset=utf-8;
    format=flowed

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 al=
ong with them for the most part.Peter BarnesOn Oct 19, 2023, at 9:20 PM, R=
osie Lloyd <rosielloyd071292@icloud.com> wrote:Yup, you explained it well =
last night.=C2=A0 Just get me the copies of the forged withdrawal receipts=
so I can get this going. Also, what about Catarina Mona and Lanzo, I thin=
k her last name is Agneza ?=C2=A0Rosie LloydOn Oct 19, 2023, at 9:11 PM, P=
eter Barnes <peterbarnes12792@icloud.com> wrote:I trust X, it was actually=
X,that brought this idea to me a while back.=C2=A0 I thought they were ki=
dding, but X kept asking.=C2=A0 Now after seeing the exec=E2=80=99s gettin=
g rich while I have trouble paying my bills, I am ready to put this into a=
ction.=C2=A0 But I need your help to make this work. You know what to do n=
ext?Peter BarnesOn Oct 19, 2023, at 9:07 PM, Rosie Lloyd <rosielloyd071292@=
icloud.com> wrote:Honestly, I am intrigued.=C2=A0 Was up all night thinki=
ng about it, and how we can pull it off.=C2=A0 Are you sure =E2=80=9CX=E2=80=
=9D can help us out?=C2=A0 Do you trust X ?=C2=A0 How about Michaela Rokas=
?=Rosie LloydOn Oct 19, 2023, at 9:02 PM, Peter Barnes <peterbarnes12792@i=
cloud.com> wrote:Great getting together again last night, what did you thi=
nk of the =E2=80=98idea=E2=80=99 I ran by you?Peter Barnes
--Apple-Webmail-42--8c916441-07b1-4508-98b8-c26c01f865df
Content-Type: multipart/related;
    type="text/html";
    boundary=Apple-Webmail-86--8c916441-07b1-4508-98b8-c26c01f865df

--Apple-Webmail-86--8c916441-07b1-4508-98b8-c26c01f865df
Content-Transfer-Encoding: quoted-printable
```

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”



The screenshot shows a terminal window with two tabs. The left tab is titled "root@kali: ~/autopsy-files/autopsy-4.10.0/bin" and the right tab is titled "root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/19". The content of the right tab shows an email message in HTML format. The message is from "Rosie Lloyd" to "Peter Barnes". It discusses plans to delete details about a plan off their email and mentions forged withdrawal receipts. It also references a previous message from Peter Barnes about a trust and asks if Rosie is in.

```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/19# cat 2.1.emlxpart.html
<html><body><div>Ok, I'll do that, and don't worry so much.<br></div><div><br></div>
<div>Rosie Lloyd</div><div><br></div><blockquote type="3D" cite=""><div>On =
Oct 19, 2023, at 9:23 PM, Peter Barnes &lt;peterbarnes12792@icloud.com&gt;=
wrote:<br></div><div><br></div><div><br></div><div>OK, but plea=
se 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 lit=
tle reckless and going to get us caught. They are ok, I get along with the=
m for the most part.<br></div><div><br></div><div>Peter Barnes<br></div><d=
iv><br></div><blockquote type="3D" cite=""><div>On Oct 19, 2023, at 9:20 PM, R=
osie Lloyd &lt;rosielloyd071292@icloud.com&gt; wrote:<br></div><br></d=
iv><div><br></div><div><br></div><div>Yup, you explained it well last night.&n=
bsp; 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 na=
me is Agneza ?&br><br></div><div><br></div><div>Rosie Lloyd<br></div><d=
v><br></div><blockquote type="3D" cite=""><div>On Oct 19, 2023, at 9:11 PM, Pe=
ter Barnes &lt;peterbarnes12792@icloud.com&gt; wrote:<br></div><br></d=
iv><div><br></div><div><br></div><div>I trust X, it was actually X that brough=
t this idea to me a while back.&nbsp; I thought they were kidding, but X k=
ept asking.&nbsp; Now after seeing the exec=E2=80=99s getting rich while I=
have trouble paying my bills, I am ready to put this into action.&nbsp; B=
ut I need your help to make this work. You know what to do next?<br></div>
<div><br></div><div>Peter Barnes<br></div><div><br></div><blockquote type="3D"=
cite=""><div>On Oct 19, 2023, at 9:07 PM, Rosie Lloyd &lt;rosielloyd071292@i=
cloud.com&gt; wrote:<br></div><div><br></div><div><br></div><div><d=
v>Honestly, I am intrigued.&nbsp; Was up all night thinking about it, and =
how we can pull it off.&nbsp; Are you sure =E2=80=9CX=E2=80=9D can help us=
out?&nbsp; Do you trust X ?&nbsp; How about Michaela Rokas ?<br></div><d=
v><br></div><div>Rosie Lloyd<br></div><div><br></div><div><br></div><block=
quote type="3D" cite=""><div>On Oct 19, 2023, at 9:02 PM, Peter Barnes &lt;pet=
erbarnes12792@icloud.com&gt; wrote:<br></div><div><br></div><div><br></div>
<div><br></div><div>Great getting together again last night, what did you thin=
k of the =E2=80=98idea=E2=80=99 I ran by you?<br></div><div><br></div><div>
<span style="color: #000000; font-style: normal; font-variant-ligat=
ures: normal; font-variant-caps: normal; font-weight: 300; letter-spacing=
: -0.37px; orphans: 2; text-align: start; text-indent: 0px; text-transform=
: none; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; whit=
e-space: normal; background-color: #000000; text-decoration-thi=
ckness: initial; text-decoration-style: initial; text-decoration-color: in=
itial; float: none; display: inline important;"><span class="font" styl=
e="color: #000000; font-family: SF Pro Text, system-ui, sans-serif"><span cla=
```

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.

Hockeyfan4747@proton.me asks:

“So, is Rosie in?

peterbarnes12792@icloud.com replies:

“Yes, we are good, should get this going this Friday.”

```
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin      x  root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20...
root@kali:~/casedata/Pure-Gold-Credit-Union2/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
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cat 20
cat: 20: Is a directory
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData# cd 20
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20# ls
full.emlx
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/20# cat full.emlx
To: hockeyfan4747 <hockeyfan4747@proton.me>
From: Peter Barnes <peterbarnes12792@icloud.com>
Subject: Re: Question
Date: Fri, 20 Oct 2023 02:38:10 +0000 (UTC)
X-Client-IP: 10.182.121.68
X-Mailer: iCloud Mailclientcurrent MailServer2322B155.10000-Famine2322-0-e29a334e875d
Message-id: <9cc9f165-52a5-4677-985f-d83bc7571e3d@me.com>
Content-Type: multipart/alternative; boundary=Apple-Webmail-42--6babd676-5b2b-419d-933b-17d52624d9d5
MIME-Version: 1.0
In-Reply-To: <ZBUVedEI0RxPPiQPzo47b28Hg37z_lwdtt8q5ThMWBHkoZFn4scUhBdrRUBhxMTk0vRw9zK0dsz651A-aAoZpEGUFy6PpHhU0fAR2gXIndw=@proton.me>
References: <ZBUVedEI0RxPPiQPzo47b28Hg37z_lwdtt8q5ThMWBHkoZFn4scUhBdrRUBhxMTk0vRw9zK0dsz651A-aAoZpEGUFy6PpHhU0fAR2gXIndw=@proton.me>

[[[

--Apple-Webmail-42--6babd676-5b2b-419d-933b-17d52624d9d5
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;
charset=utf-8;
format=flowed

Yes, we are good, should get this going this FridayPeter BarnesOn Oct 18, = 2023, at 8:31 PM, hockeyfan4747 <hockeyfan4747@proton.me> wrote:So, is Ros= ie in?=>C2=A0Sent with Proton Mail secure email.
--Apple-Webmail-42--6babd676-5b2b-419d-933b-17d52624d9d5
Content-Type: multipart/related;
type="text/html";
boundary=Apple-Webmail-86--6babd676-5b2b-419d-933b-17d52624d9d5

--Apple-Webmail-86--6babd676-5b2b-419d-933b-17d52624d9d5
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
```

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.

```

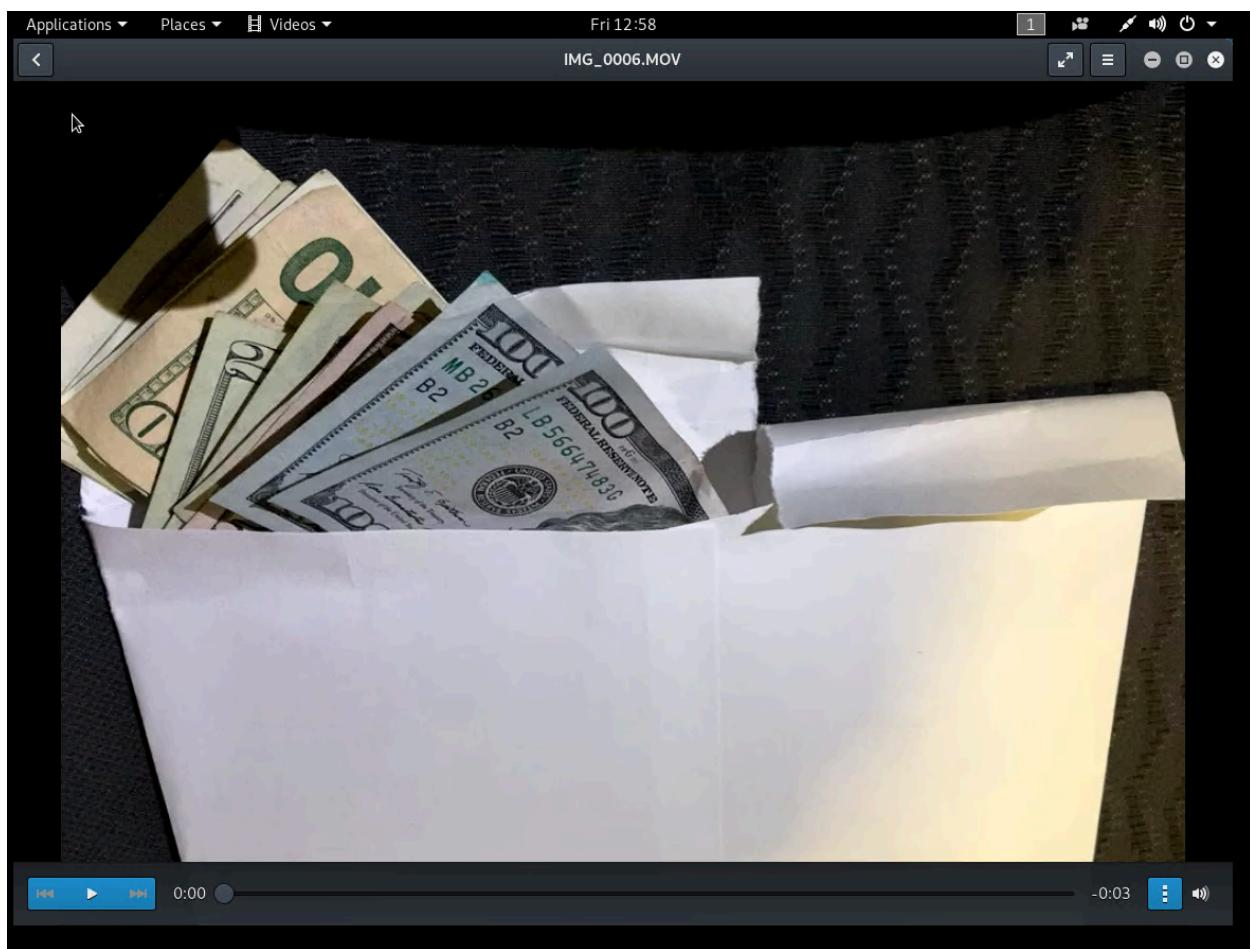
root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/21
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin      x  root@kali: ~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/Message... x
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/21# ls
full.emlx
root@kali:~/casedata/Pure-Gold-Credit-Union2/Export/9-Mail/MessageData/21# cat full.emlx
Return-path: <hockeyfan4747@proton.me>
Original-recipient: rfc822;peterbarnes12792@icloud.com
Received: from mr28p00im-smtpin042.me.com by p115-mailgateway-smtp-6c5746c486-8jvk4 (mailgateway 2401B119)
        with SMTP id c173651a-fddd-4148-b4ee-be64979f3cd7
        for <peterbarnes12792@icloud.com>; Fri, 20 Oct 2023 02:43:39 GMT
X-Apple-MoveToFolder: INBOX
X-Apple-Action: MOVE_TO_FOLDER/INBOX
X-Apple-UUID: c173651a-fddd-4148-b4ee-be64979f3cd7
Received: from mail-40141.protonmail.ch [185.70.40.141]
        by mr28p00im-smtpin042.me.com (Postfix) with ESMTPS id 1246C25934CD
        for <peterbarnes12792@icloud.com>; Fri, 20 Oct 2023 02:43:37 +0000 (UTC)
X-ICL-SCORE: 3.333033030041
X-ICL-INFO: GAtbVUSeBFVGSVVESAMGUkFIRFcUWUIPAApbVRYSFHEAREQZF15TQFUCAkpaWFkBHhwfERleAlVB
TiYHcl9CDRtCxJaFeAGSFsWBRdEWQxbFANVWErfEkhbV09NHgFSW01wUKEB0BVEQMbFw0UDxQ0
ClpMAAdwRFcWBrdEWQwyGAabvLNefUFUJegVFElxDHBVLQ0gBA1nbCRQYDF9YDxQ0C1kbwBRCEr1b
VohCWRYaF0gaHRIWDXwdW1EVWILRds5DjMDQU8tEQENAWJAUh4cC08zHQI1TCZVLxkEOwxGwI6
T3lAdjkANDZPQQcGLDgwHxDbzY2swoGFGNZFCMDs2ETISXowRRqjJEwJQ0C+DzcuPFYDNBs4V04q
CHJbgEA5Dhb2bC9IORYFF0RZDfsUA0laeEOBSFsWEgxVRAAUcvwgScwEEVUxLJh4bXFkXEvcFBUS
Authentication-Results: bimi.icloud.com; bimi=declined
X-ARC-Info: policy=fail; arc=none
Authentication-Results: arc.icloud.com; arc=none
Authentication-Results: dmarc.icloud.com; dmarc=pass header.from=proton.me
X-DMARC-Info: pass=pass; dmarc-policy=quarantine; s=s1; d=s1; pdomain=proton.me
X-DMARC-Policy: v=DMARCl; p=quarantine; fo=1; aspf=s; adkim=s;
Authentication-Results: dkim-verifier.icloud.com;
        dkim=pass (2048-bit key) header.d=proton.me header.i=@proton.me header.b=mc0cgCyr
Authentication-Results: spf.icloud.com; spf=pass (spf.icloud.com: domain of hockeyfan4747@proton.me designates 185.70.40.141 as permitted sender) smtp.mailfrom=hockeyfan4747@proton.me
Received-SPF: pass (spf.icloud.com: domain of hockeyfan4747@proton.me designates 185.70.40.141 as permitted sender) receiver=pf.icloud.com; client-ip=185.70.40.141; helo=mail-40141.protonmail.ch; envelope-from=hockeyfan4747@proton.me
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=proton.me;
        s=protonmail; t=1697769815; x=1698029015;
        bh=uhZm19ZnN7g+Aork53EkQoHVRZ3pD8GEZ4lfFe1bP0=;
        h=Date>To:From:Subject:Message-ID:In-Reply-To:References:
        Feedback-ID:From>To:Cc:Date:Subject:Reply-To:Feedback-ID:
        Message-ID:BIMI-Selector;
        b=mc0cgCyrhI3MofAWj3cneU5Eztebib9kTCleS10HaulsgCWzbcc0Zip5p6/VPeg
        l0xEfpG4aclyRg3Bi0lIRVNY5wnc9Fhq0hIubC+lzygNb+3LMRs4C/pBFNEoEdUEXg

```

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.”

The screenshot shows the DB Browser for SQLite interface with a database named 'Temp/sms.db'. The 'message' table is selected, displaying the following data:

ROWID	guid	text	replace	service_center	handle
1	AEFD4110-...		0	NULL	4
2	64CE5E08-5...		0	NULL	4
3	5066759A-F...	NULL	0	NULL	4
4	2A50A0CA-...		0	NULL	4
5	7D932C75-...	Dinner toni...	0	NULL	4
6	7BDB1394-...	Yup, see yo...	0	NULL	4
7	812E2E21-E...	I did it toda...	0	NULL	4
8	3708197B-E...	NULL	0	NULL	4
9	B8E17784-...	Let's get off...	0	NULL	4

The message at index 7 contains the text "I did it today, can't believe it. Going to the mall later, wanna join me ? Also, I sent you a picture."

Below the table, the status bar shows "1 - 9 of 9".

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”

The screenshot shows the DB Browser for SQLite interface. The main window displays a table named "message" with the following data:

ROWID	guid	text	replace	service_center	har
13	13	9A524230-8...	0	NULL	7
14	14	B18AE98C-...	0	NULL	8
15	15	7D932C75-...	NULL	0	5
16	16	7BDB1394-...	Yup, see yo...	0	5
17	17	0EEC2636-...	Check your ...	0	NULL
18	18	20E378B4-...	Ok, will do	0	10
19	19	0D94C44D-...		0	NULL
20	20	48CB795C-...		0	NULL
21	21	812E2E21-E...		0	NULL
22	22	3708197B-E...	I did it toda...	0	NULL
23	23	BBE17784-...	Let's get off...	0	NULL
24	24	1F72C36A-...		0	NULL
25	25	C253EFB7-5...		0	NULL
26	26	4ACC8E64-...		0	NULL
27	27	9A115BE9-...		0	NULL
28	28	F7EB0D719-...		0	NULL
29	29	D1FCE1FD-...		0	NULL
30	30	3E979855-C...	Just left you...	0	NULL
31	31	0289E731-E...	Ok	0	NULL

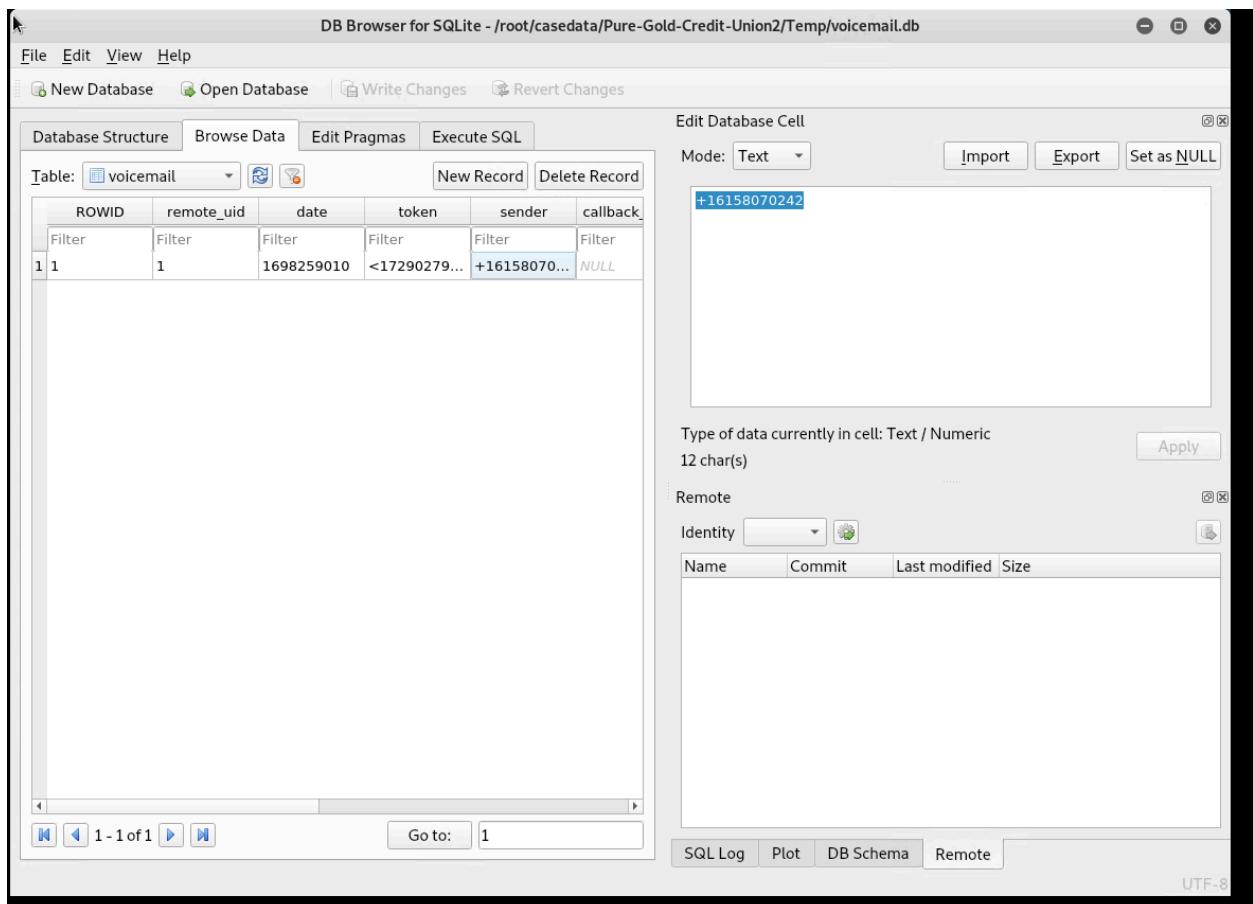
The "Edit Database Cell" panel shows the message "Let's get off texts please, just email me to that email address." in the text field. The "Mode" dropdown is set to "Text".

October 25th 2023

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
1	1	1698259010	<17290279...	+16158070...	NULL

Edit Database Cell

Mode: Text Import Export Set as NULL

1698259010

Type of data currently in cell: Text / Numeric
10 char(s) Apply

Remote

Identity Name Commit Last modified Size

SQL Log Plot DB Schema Remote

UTF-8

The screenshot shows the DB Browser for SQLite interface. The main window displays a table named 'voicemail' with one row. The columns are 'ROWID', 'remote_uid', 'date', 'token', 'sender', and 'callback'. The 'date' column contains the value '1698259010'. An 'Edit Database Cell' dialog is open over the 'date' cell, showing the value '1698259010' and indicating it is a 'Text / Numeric' type with 10 characters. Below the table, there are navigation buttons for the database and a status bar showing '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!"

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	har
13	13	9A524230-8...	0	NULL	7
14	14	B18AE98C-...	0	NULL	8
15	15	7D932C75-...	NULL	0	5
16	16	7BDB1394-...	Yup, see yo...	0	5
17	17	0EEC2636-...	Check your ...	0	10
18	18	20E378B4-...	Ok, will do	0	10
19	19	0D94C44D-...		0	11
20	20	48CB795C-...		0	1
21	21	812E2E21-E...		0	5
22	22	3708197B-E...	I did it toda...	0	5
23	23	B8E17784-...	Let's get off...	0	5
24	24	1F72C36A-...		0	4
25	25	C253EFB7-5...		0	1
26	26	4ACC8E64-...		0	12
27	27	9A115BE9-...		0	12
28	28	F7E8D719-...		0	1
29	29	D1FCE1FD-...		0	13
30	30	3E979855-C...	Just left you...	0	10
31	31	0289E731-E...	Ok	0	10

12 - 31 of 31 Go to: 1

Edit Database Cell Mode: Text Import Export Set as NULL

Just left you a VM, listen to it and get back to me!

Type of data currently in cell: Text / Numeric
52 char(s) Apply

Remote Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

SQL Log Plot DB Schema Remote

UTF-8

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

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 har

13 13 9A524230-8... 0 NULL 7
 14 14 B18AE98C-... 0 NULL 8
 15 15 7D932C75-... NULL 0 NULL 5
 16 16 7BDB1394-... Yup, see yo... 0 NULL 5
 17 17 0EEC2636-... Check your ... 0 NULL 10
 18 18 20E378B4-... Ok, will do 0 NULL 10
 19 19 0D94C44D-... 0 NULL 11
 20 20 48CB795C-... 0 NULL 1
 21 21 812E2E21-E... 0 NULL 5
 22 22 3708197B-E... I did it toda... 0 NULL 5
 23 23 BBE17784-... Let's get off... 0 NULL 5
 24 24 1F72C36A-... 0 NULL 4
 25 25 C253EFB7-5... 0 NULL 1
 26 26 4ACC8E64-... 0 NULL 12
 27 27 9A115BE9-... 0 NULL 12
 28 28 F7E8D719-... 0 NULL 1
 29 29 D1FCE1FD-... 0 NULL 13
 30 30 3E979855-C... Just left you... 0 NULL 10
 31 31 0289E731-E... Ok 0 NULL 10

12 - 31 of 31 Go to: 1

Edit Database Cell Mode: Text Import Export Set as NULL

Ok

Type of data currently in cell: Text / Numeric 2 char(s) Apply

Remote Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

SQL Log Plot DB Schema Remote

UTF-8

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

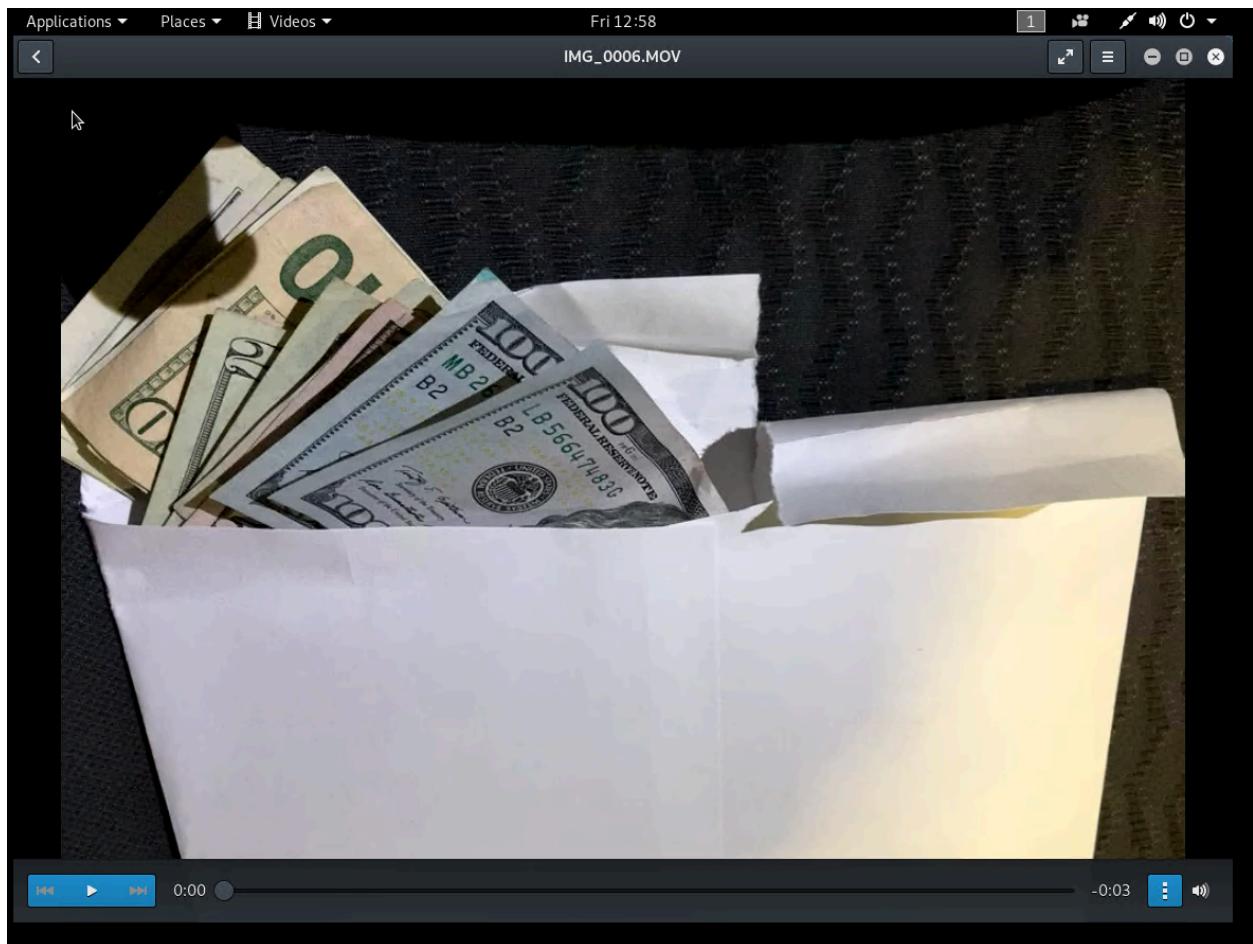
11	10/12/23 22:36:10 GMT	From: rosielloyd071292@icloud.com To: peterbarnes12792@icloud.com Subject: Re: Dinner	"Hey Peter, Likewise, was so great to get a chance to hang out, outside of work. Sounds like we both feel that we aren't being paid enough and on top of that all the Gold Credit Union executives 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: peterbarnes12792@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@icloud.com	This appears to be a reply to an email thread that may have been deleted.	MessageData/20

		<p>cloud.com</p> <p>Subject: Question</p>	<p>Hockeyfan4747@proton.me asks, “So, is Roise in?”</p> <p>peterbarnes12792@icloud.com replies: “Yes, we are good, should get this going this Friday.”</p> <p>Plans made to complete the crime on Friday</p>	
21	10/20/23 2:43:23 GMT	<p>To:peterbarnes12792@icloud.com</p> <p>From: hockeyfan4747@proton.me</p> <p>Subject: Question</p>	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	<p>To: Peter +16155719608</p> <p>From: Oliver Bell +16158070242</p>	<p>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.”</p>	voicemail.db
30	10/25/23 18:37:50 GMT	<p>To: Peter +16155719608</p> <p>From: Oliver Bell +16158070242</p>	<p>“Just left you a VM, listen to it and get back to me!”</p> <p>Someone sent Peter a voicemail and is asking them to listen to it</p>	sms.db
31	10/25/23 18:38:04	<p>To: Oliver Bell +16158070242</p>	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%B0058'13.6%22N+86%C2%B0048'26.6%22W/@35.97045,-86.8073889,17z/data=!3m1!4b1!4m4!3m3!8m2!3d35.97045!4d-86.8073889?entry=ttu&q=ep=EgoyMDI0MDkxNi4wIKXMDSoASAFOAw%3D%3D>

📍 35° 58' 13.62" N 86° 48' 26.6" W