



2012 NATIONAL GALLERY DC CASE

Cyber Forensics & Information Technology - Assignment



TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	3
METHODOLOGY.....	4
EVIDENCE.....	7
• EVIDENCE RELATED TO THE HEIST	
• Finding 1: Conspiracy for Theft of the Stamps.....	7
• Finding 2: Tracy's Financial Conditions.....	10
• Finding 3: Tracy Logging into Coral's Email Account.....	11
• Finding 4: King's Involvement in the Heist.....	13
• EVIDENCE RELATED TO THE DEFACEMENT OF ARTWORK AT NGDC	
• Finding 5: Krasnovian and Anti-American Sentiments.....	15
• Finding 6: Email Conversation Between Carry and Alex.....	16
• Finding 7: Video Containing Information about Defacing Artwork.....	17
• Finding 8: Carry in Touch with a Mob Organizer.....	19
• Finding 9: Carry Seeking Tracy for Help.....	20
• Finding 10: Information about Security Personnel Schedule.....	23
• Finding 11: Carry's Tablet Containing the Map for NGDC.....	24
• Finding 12: Images of Security Cameras from the N GDC.....	25
• Finding 13: Carry's Search History.....	26
• Finding 14: Tracy Receives Suspicious Amount.....	27
CONCLUSIONS AND SUMMARY.....	28

APPENDIX

- Appendix I: Description of Persons of Interest.....30
- Appendix II: Association Diagram of Persons of Interest.....31
- Appendix III: Evidence Listing.....31
- Appendix IV: Plot Timeline.....34
- Appendix V: Software and Tools Used in the Investigation.....36
- Appendix VI: Other Important Listings and Information.....39
- Appendix VII: Integrity of Analysed Evidence.....42

REFERENCES.....45

EXECUTIVE SUMMARY

We have written a forensic report referring to the case that involves exclusive plans to vandalize artwork displayed at the National Gallery DC art gallery and commit theft. In our report, we will document and investigate all the key pieces of evidence confiscated during the acquisition of devices belonging to the suspects.

Description of events: The suspects involved in the criminal plans for theft and defacement are Alex, a wealthy Krasnovian businessman whose sole interest is to embarrass the United States of America by defacing foreign works on exhibit in the National Gallery DC. In order for him to accomplish this, seeing as he could not carry it out alone, he brings on a fellow Krasnovian Carry, whom he got to know through extended family connections and similar family ties. Carry is on board with this and discusses it with Tracy, a supervisor at the National Gallery, seeing that she is somewhat familiar with her.

Carry promises to compensate Tracy handsomely for her part in the defacement plot, and seeing as Tracy has money troubles, she is keen on ignoring the suspicious nature of the requests and is willing to help. The plot for defacement shattered after Joe, Tracy's ex-husband, tried to monitor their child, Terry, and came across conspiracies to commit theft after installing a keylogger on Tracy's computer.

METHODOLOGY

The methodology followed for the investigation of the crime poised towards the National Gallery DC involves the identification of relevant devices, handling as well as preserving of evidence securely, carefully investigating the acquired evidence, and finally, reporting all our findings to the right individuals.

Evidence for the investigation: The following evidence were sized for the investigation.

- A Tablet that belongs to Carry
- A phone that belongs to Carry
- A phone that belongs to Tracy
- Emails gotten from the keylogger that Joe put on Tracy's computer.
- A Computer belonging to Tracy

As soon as these devices were imaged as well as hashed, we created a copy of the digital evidence images for use as the working copy in the investigation, as it is a proper procedure for handling digital evidence. These drive images and files were analysed using forensic tools like

- Autopsy
- SQLite
- BitRecover

With their help, we were able to carry out this investigation successfully. To hash the files required during our investigation we used Windows PowerShell. Our findings have been documented in this report, including details of the evidence recovered, the analysis conducted, and the conclusions drawn from the evidence. The table below shows the suspects' contacts Information found in the evidence sources:

Name	Phone number	Email	Relationship	Status
------	--------------	-------	--------------	--------

Tracy Alias name: Coral Blue	+703 340 9961	Email: tracysumtwelve@gmail.com Work email: Tracy.sumtwelve@nationalgallerydc.org Alias Email: Coralbluetwo@hotmail.com	Ex husband: Joe Daughter : Terry Brother : Pat	Accused
Pat Alias Name: Perry	+571 308 3236	Email: patsumtwelve@gmail.com Alias Email: perrypatsum@yahoo.com	Sister : Tracy	Accomplice
Joe		Email: joe.sum.twelve@gmail.com	Ex wife : Tracy Daughter : Terry	
Carry Alias name : Cat	+202 725 2124	Email : Carsumtwotwelve@yahoo.com Alias Email: cat2welve@gmail.com	Acquaintance of Tracy Neice of Alex	Accused
King		Email: Throne1996@hotmail.com	Acquaintance of Pat	Accomplice

Alex		Email: <u>Alex.jfam11@gmail.com</u>	Uncle of Carry	
------	--	---	----------------	--

The collection and preservation of evidence: As forensic investigators, it is our sole duty to ensure that all the pieces of evidence we receive maintain their integrity before and even after the investigation. To achieve this, the files were hashed before and after with the use of Windows PowerShell. This helps ensure that the data is preserved and ensures to investigators that data was not manipulated to influence decisions. Additionally, this is also helpful as there may be multiple investigations involved and by hashing before and after it will help keep a log record of all the investigators and if data has been modified.

In conclusion, we were successfully able to carry out detailed Investigation on all devices and we documented and recorded all the pieces of evidence related to this case.

EVIDENCE

EVIDENCE RELATED TO THE HEIST

The investigation begins by capturing Tracy's home computer, external drive, and phone.

The major essential findings obtained from all these devices are as follows:

The files that were investigated:

- tracy-phone-2012-07-15-final.E01
- tracy-external-2012-07-16-final.E01
- tracy-home-2012-07-16-final.E01

Finding – 1: Conspiracy for theft of the stamps

Discussion

While searching through Tracy's external hard drive, inculpatory evidence was discovered. At first, the folder was put into autopsy for a thorough study that later revealed some questionable images, pictures, and PDF files related to the case. During the analysis, all these files, which were considered relevant in the analysis, were instantly exported to the local directory of the system. Following the timeline, Pat and Tracy started scheming on how to steal stamps in July 2012. They are discussing the possibility of using insider information from their workplace to make some money. The insurance documents that come across Tracy's desk may contain information about the value of certain objects, which could help them identify items that are worth stealing or selling. Therefore, the documents would potentially benefit them in their plan to make money outside of their regular jobs.

The photos in their hard drives show that Tracy was part of a conspiracy to steal stamps from the National Gallery. A Memorandum of Insurance assurance was extracted in PDF format from the deleted files.



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 11. Woman's Profile	\$31,000.00
Lot # 12. Stamp of Kazakhstan	\$29,000.00
Lot# 13. 1929 Nepal	\$27,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann


President National Gallery DC



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 1. Douglas MacArthur	\$35,000.00
Lot # 2. Nederland	\$30,000.00
Lot# 3. Mongolia	\$24,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann


President National Gallery DC



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 25. Armed Forces Reserve	\$43,000.00
Lot # 26. Stamp of Kazakhstan2	\$29,000.00
Lot# 27. BradyCo.	\$12,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann


President National Gallery DC

Figure 1.1. PDF files of NGDC stamp insurance

Analysis of Tracy's phone also revealed that there were images of stamps. Apparently, the photograph of the stamp images was taken before the theft and has been used for other purposes by some people. Tracy had taken the images from the museum as per timestamp location. Figure 1.1 illustrates this situation.

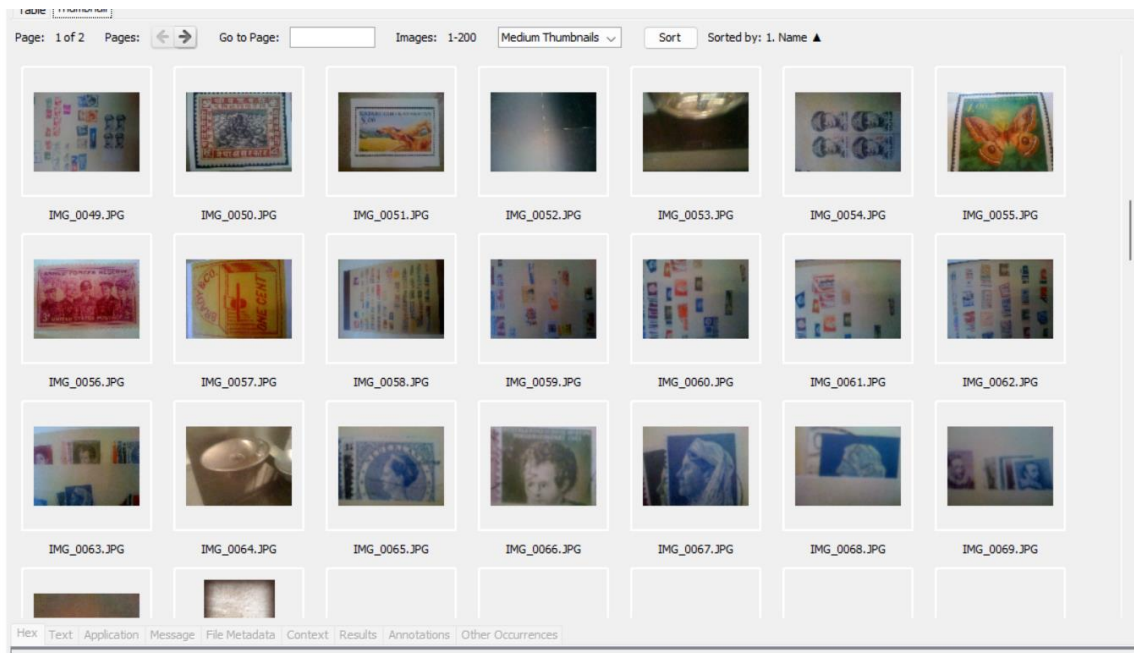


Figure 1.2: Images of stamp analyzed using Autopsy

In addition, a documents.zip file was extracted to the local disk and contained a PDF version of the stamp's insurance document.

The pdf files named securedownload.pdf was extracted from the location /Tracy Phone/tracy-phone-2012-07-15-final.tar/./private/var/mobile/Library/Mail/POP-

[coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs/Stamp Insurance .pdf](mailto:coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs/Stamp%20Insurance.pdf)

Figure 1.3: documents.zip file extracted using autopsy

The screenshot shows the Autopsy forensic tool interface. At the top, there's a path: /img_tracy-home-2012-07-16-final.E01/Users/tracysumtwelve/Library/Mail/V2/IMAP-tracysumtwelve@imap.gmail.com/Sent Messages.mbox/AF896150-6E64-488B-88E7-BE642B218542/Data/Attachments/411/3/docs 5 Res. Below this is a table of extracted files. The table has columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), and Known. The files listed are: [parent folder], .DS_Store, Stamp insurance 1.pdf, Stamp Insurance 2.pdf, and Stamp insurance 3.pdf. The 'Stamp insurance 1.pdf' row has a yellow highlight on the 'Change Time' column, which shows '2012-07-09 17:42:58 GST'. Below the table is a section for 'Encryption Detected' with tabs for Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, and Other Occurrences. The 'Results' tab is selected, showing 'Result: 1 of 1'. The table below this shows: Type: Content-only Encryption (Archive File), Source File Path: /img_tracy-phone-2012-07-15-final.E01/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/2/documents.zip, and Artifact ID: -9223372036854775688.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[parent folder]			2012-07-09 18:52:00 GST	2012-07-09 18:52:00 GST	2012-07-09 18:52:00 GST	2012-07-09 18:52:00 GST	0	Allocated	Allocated	unknown
.DS_Store			2012-07-09 17:42:58 GST	2012-07-09 18:52:00 GST	2012-07-09 17:42:58 GST	2012-07-09 17:42:58 GST	6148	Allocated	Allocated	unknown
Stamp insurance 1.pdf			2012-07-06 17:39:52 GST	2012-07-09 17:42:58 GST	2012-07-06 17:39:52 GST	2012-07-06 17:39:52 GST	189553	Allocated	Allocated	unknown
Stamp Insurance 2.pdf			2012-07-06 17:39:52 GST	2012-07-09 18:52:00 GST	2012-07-06 17:39:52 GST	2012-07-06 17:39:52 GST	183592	Allocated	Allocated	unknown
Stamp insurance 3.pdf			2012-07-06 17:39:52 GST	2012-07-09 18:52:00 GST	2012-07-06 17:39:52 GST	2012-07-06 17:39:52 GST	182641	Allocated	Allocated	unknown

Type	Value	Source(s)
Comment	Content-only Encryption (Archive File)	Embedded File Extract
Source File Path	/img_tracy-phone-2012-07-15-final.E01/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/2/documents.zip	
Artifact ID	-9223372036854775688	

Figure 1.4: Extracted files of Stamp Insurance from mail

Finding – 2: Tracy’s Financial conditions

Discussion

The evidence presented here is inculpatory.

The email messages provide an implication that Tracy is having a hard time financially. Terry has also refused to move to another school in the fear of losing her old friend. The SMS was extracted from the SMS database and was opened and investigated using SQLite DB browser

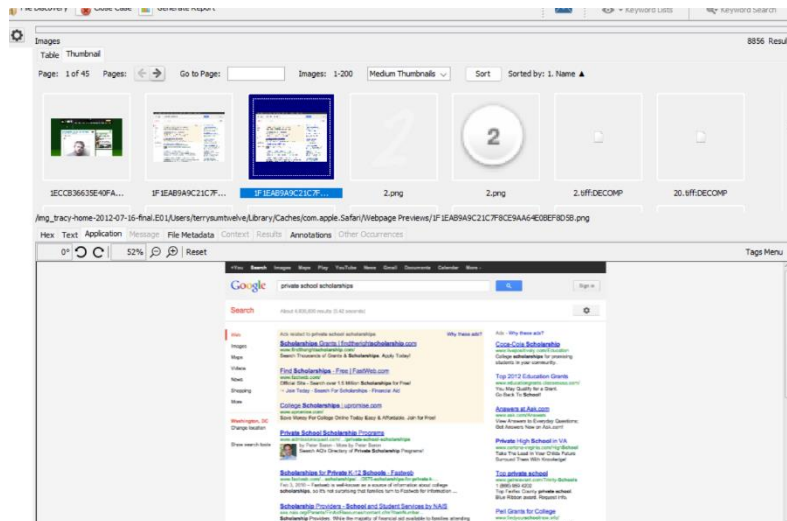


Figure 2.1: Browser screenshots from Tracy's home computer

Regarding Terry
Tracy Sumtwelve <tracysumtwelve@gmail.com> Date: 02/07/2012 20:07

Joe,

Sorry to bother you, but I have a serious question about Terry and her school. Her tuition is getting a bit too much for me right now and I could use a little help. I hate to impose on you for this, but is there any way you would be willing to help me out with her tuition this year?

Please get back to me,
Tracy

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>date-sent</key>
  <real>1341259619</real>
  <key>flags</key>
  <integer>8590195713</integer>
  <key>original-mailbox</key>
  <string>imap://tracysumtwelve@imap.gmail.com/%5BGmail%5D/All%20Mail</string>
  <key>remote-id</key>
  <string>104</string>
  <key>subject</key>
  <string>Regarding Terry</string>

```

Figure 2.2: conversation between Tracy asking her ex-husband for financial support.

```

4 9 +17038296071 1339612426 Ok, sounds good.
5 12 +17038296071 1341322911 Hey honey, I'm not sure if we can ...
6 13 +17038296071 134132427 ... b...
7 14 +12027252124 1341512303 Sounds good let's shoot for one at ...
8 15 +12027252124 1341512426 Okay that sounds great. See you there
9 16 +15713083236 1341586939 Hey can you give me a call
10 17 +15713083236 1341587317 Sis I'm really busy can we can do this...
11 18 +15713083236 1341587514 ...
12 19 +15713083236 1341587611 Ok ok I'll call in 5
13 20 +12027252124 1341592036 I have a table inside
14 21 +12027252124 1341592070 Okay brt
15 22 +12069100932 1341689795 Congratulations, your entry in last ...
16 23 +15713083236 1341933979 hey sis yo friend coral got a email th...
17 24 +15713083236 1341935884 Sure thing I'll get on it
18 26 1341938229
19 27 +17038296071 1341940718 Going to lunch. You want to go?????
20 28 +17038296071 1341944364 Back at work
21 29 +17038296071 1341946704 I'm busy. Maybe this weekend if dad ...
22 30 +12027252124 1342010505 I'm almost there where should I mee...
23 31 +12027252124 1342010948 Just meet me out front, I'll take the ...
24 32 +12027252124 1342112805 How's the flashmob going
25 33 +17038296071 1342141330 I really want to go to Dad's this ...

```

Figure 2.3: SMS message showing Terry's and Tracy's conversation extracted using DB Browser for SQLite

The email eml files were extracted from Tracy's home computer using autopsy and were opened and viewed using BitRecover EMLX Viewer.

Finding – 3: Tracy logging into Coral's Email Account

Discussion

This is inculpatory evidence.

Tracy appears to have been using the alias of 'Coral' to communicate information between herself and her associates. We have obtained this information from Tracy's phone, which shows that she has logged into coralbluetwo@hotmail.com. The analysis of some email messages between Pat and Tracy indicates that both were involved in the planning of using an aliased email address.

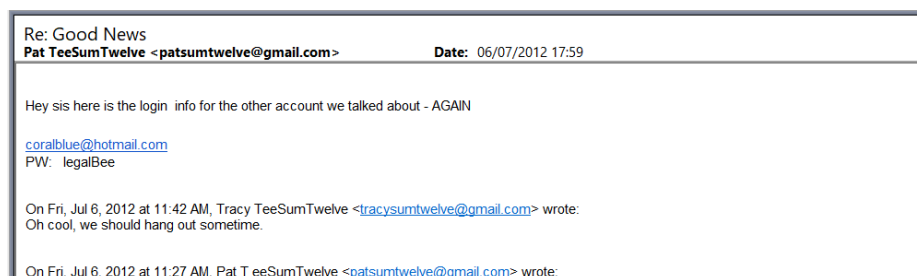


Figure 3.1: Pat sending account details to Tracy.

In addition, Pat has provided some instructions for the installation of VM, which were concealed in a song file entitled Crazy Dave. It was extracted from Tracy's external hard drive located at

/img_VM.vmdk/vol_vol3/Users/Coral/AppData/Roaming/Thunderbird/Profiles/7rmkl1x3.default/Mail/pop3.live.com/Inbox/Crazydave1.mp3.

Tracy had set up this VM to communicate with her brother Pat as it appeared to Tracy that the setup would provide a safe means of communication.

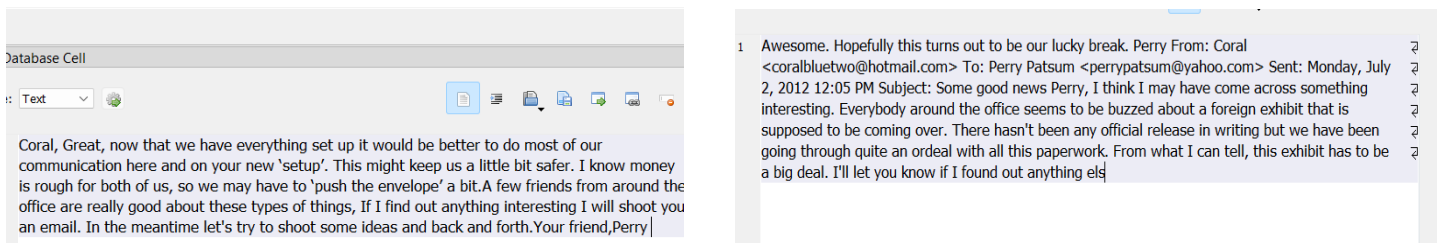


Figure 3.2: Email conversations : Pat and Tracy planning to start communication using alternative secure setup.

.localized	2012-06-12 19:17:50 GST	2012-06-12 19:17:50 GST	2012-06-12 19:17:50 GST
Crazydave1.mp3	2012-06-21 17:02:56 GST	2012-06-21 17:03:02 GST	2012-06-21 17:03:02 GST
VirtualBox-4.1.18-78361-OSX.dmg	2012-06-21 17:54:41 GST	2012-06-21 18:57:37 GST	2012-07-02 18:57:37 GST
parent folder	2012-06-15 21:37:32 GST	2012-06-15 21:37:32 GST	2012-07-09 21:37:32 GST

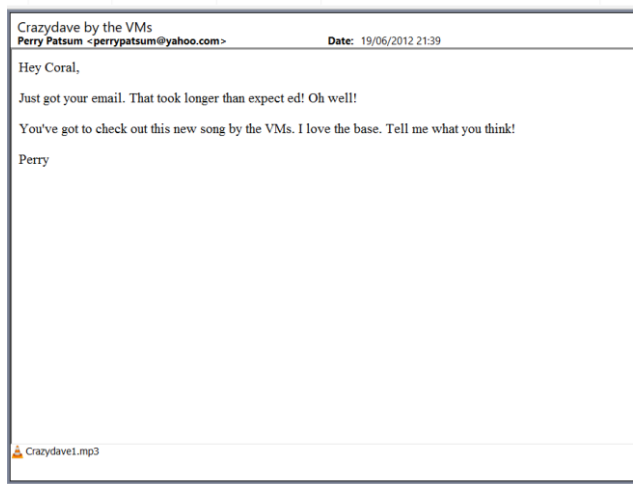


Figure 3.3: Proof of Pat sending Tracy Instructions to download VM concealed in a mp3 file.

Finding – 4: King’s involvement in the heist

Discussion

This is inculpatory evidence.

King's involvement in executing the heist has been revealed in several email messages. The email messages contain information regarding Pat's proposal to recruit King for the heist. Pat recruited the king who is a former convict on parole to join the heist. The king accepted the proposal for stealing the stamps which was confirmed from the email messages in figure 4.1. It is explicitly stated in the email that the real implementation of the plan will start two weeks from now. The heist that was carried out on the 20th of July 2012 was planned as a message sent on July 6th, 2012.

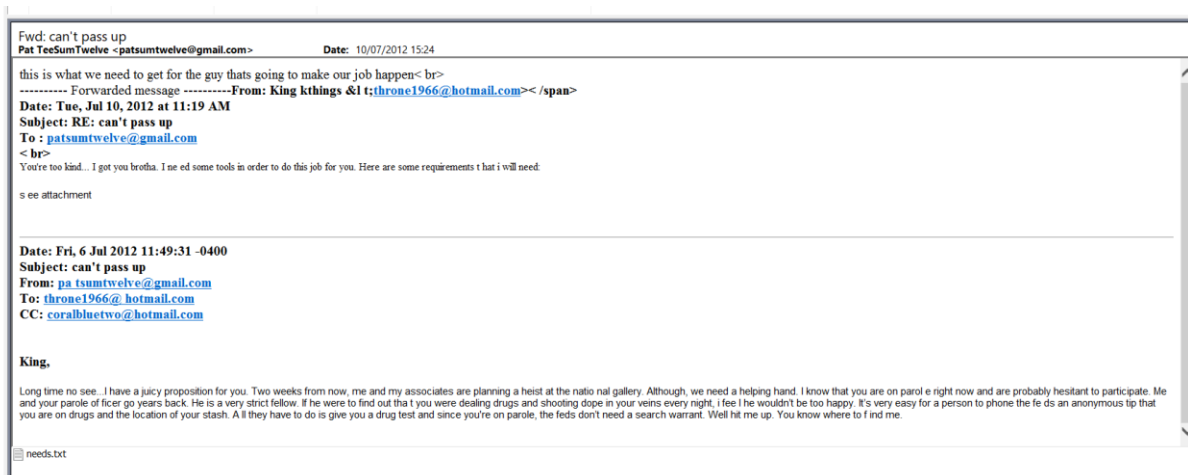


Figure 4.1: Email evidence of King accepting Pat's proposal

Besides these messages, King has also requested some crucial tools which will help during this plan. Support for this claim is provided in figure 4.2. A file called "needs.txt" was located elsewhere with an attachment referred to in the email. Figure 4.3 shows the contents of the file.

Table

Thumbnail

Save Table as CSV

▲ Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
<input type="checkbox"/> log-bb-live-stats.txt			2012-07-15 13:25:19 GST	2012-07-15 13:25:19 GST	2012-07-15 13:25:19 GST	2012-07-15 13:25:19 GST	133	Allocated	Allocated	unknown
<input checked="" type="checkbox"/> needs.txt			2012-07-12 22:51:14 GST	2012-07-12 22:51:14 GST	2012-07-12 22:51:14 GST	2012-07-12 22:51:14 GST	83992	Allocated	Allocated	unknown
<input type="checkbox"/> psk.txt			2010-10-22 08:10:24 GST	2010-11-17 12:52:25 GST	2010-10-22 08:10:24 GST	2010-10-22 08:10:24 GST	272	Allocated	Allocated	unknown

Hex

Text

Application

Message

File Metadata

Context

Results

Annotations

Other Occurrences

Result: 1	of 1	Result	↩	↪	Extension Mismatch Detected
Type	Value				Source(s)
Source File Path	/img_tracy-phone-2012-07-15-final.E01/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/60/2/needs.txt				
Artifact ID	-9223372036854775689				

Figure 4.2: Proof: King's required tools in a txt file

psk.txt		2010-10-22 08:10:24 GST	2010-11-17 12:52:25 GST	2010-10-22 08:10:24 GST	2010-10-22 08:10:24 GST	272
needs.txt		2012-07-12 22:51:14 GST	2012-07-12 22:51:14 GST	2012-07-12 22:51:14 GST	2012-07-12 22:51:14 GST	839

HexTextApplicationMessageFile MetadataContextResultsAnnotationsOther Occurrences

StringsIndexed TextTranslation

Matches on page: - of - MatchPage: 1 of 1 Page

-A rope and javelin (using alternative means to break in)

-tactical turtle necks (what i will be wearing)

-spray paint (for the cameras)

-vibram five finger shoes (in order to walk silently)

-pack of smokes (detecting lasers)

-smoke grenades (use as a means of escape if caught)

Figure 4.3: Content of needs.txt

EVIDENCE RELATED TO THE DEFACEMENT OF ARTWORK AT NGDC

While analysing Tracy's devices, it was discovered that Carry was suspected of involvement in another separate conspiracy. The main evidence that kept Carry on in the suspect list was Tracey's email messages. It was then decided to seize Carry's devices, such as her phone and tablet, considering doubts. A comprehensive forensic analysis of her device revealed another conspiracy.

The files that were investigated:

- carry-phone-2012-07-15-final.
- carry-phone-logical-2012-07-16.
- carry-tablet-2012-07-16-final.

The following conclusions were drawn based on the information obtained from her device.

Finding -5: Krasnovian and Anti-American Sentiments

Discussion

Utilizing the Autopsy tool, we located a database named EmailproviderBody.db . After its extraction, we accessed it using SQLite database browser, revealing a series of email exchanges between Carry and her uncle, Alex. These correspondences unveiled their deep-seated animosity and hatred towards America.

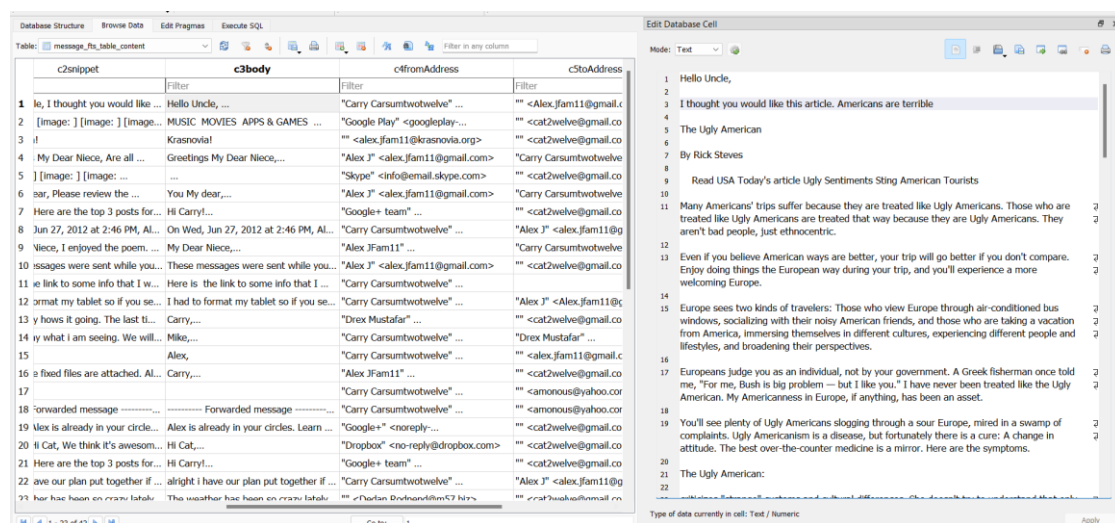


Figure 5.1: Email evidence of Alex and Carry disliking Americans.

Finding –6: Email Conversation between Carry and Alex

Discussion

This is an inculpatory evidence.

The data has been extracted from Carry's tablet and highlights email conversation between Carry and Alex sharing information about the aids sent by Alex from Krasnovia and the video shared by Alex containing information about defacing the Majavian artwork at display.

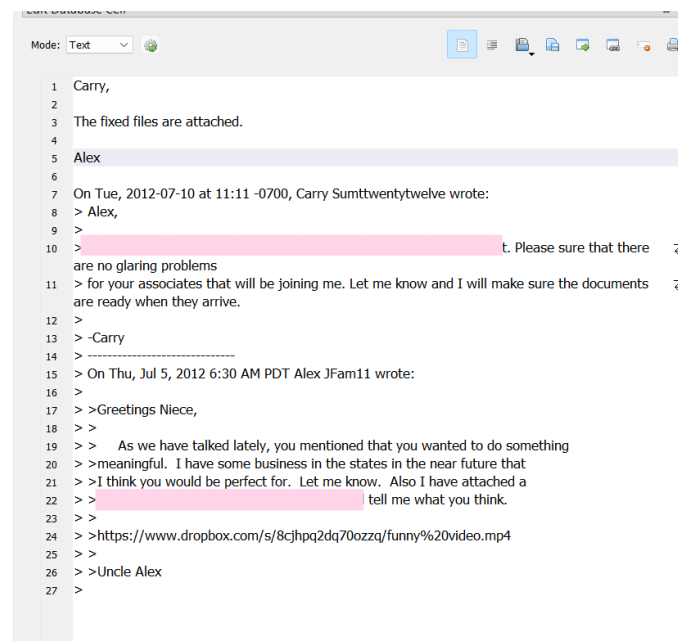


Figure 6.1 : Alex sending details to Carry.

Finding -7: Video containing information about Defacing artwork

Discussion

Inculpatory evidence has been presented.

The funny video-1.mp4 from Carry's tablet was a crucial piece of evidence. To find this file in the videos collected within this device, autopsy was used. The video first begins by displaying a 'Forensics Analysis Hospital' that has two characters represented by hands. A closer examination of the clip shows that at 00:00:35 (Figure 7.1), the video transitions to another video with a message from Alex introducing himself and proposing the idea of defacing Majavian artwork to cause a dispute. Additionally, the video provides information about Alex sending in Krasnovian aids to conduct these activities, which can be seen at 00:01:25 in the video.

Following is a transcription of the audio content.

"Hello Carry, I am Alex, and I am looking for your help both as a family friend and as a fellow Krasnovian. We must embarrass the United States and add attention to their relations with Majavian by defacing the rare Majavian artwork that is being put on display in the National Gallery. The opportunity to strike against both America and Majavia cannot be passed up. We may not get another chance. I understand you are a capable individual, so I am leaving the planning to you. I will be sending some of my associates over to the states to aid you. They will arrive early this month at your International Airport. Here is a picture so you can recognize them. In the meantime, you may contact me at alex.j.sam11@gmail.com. Please be discreet."

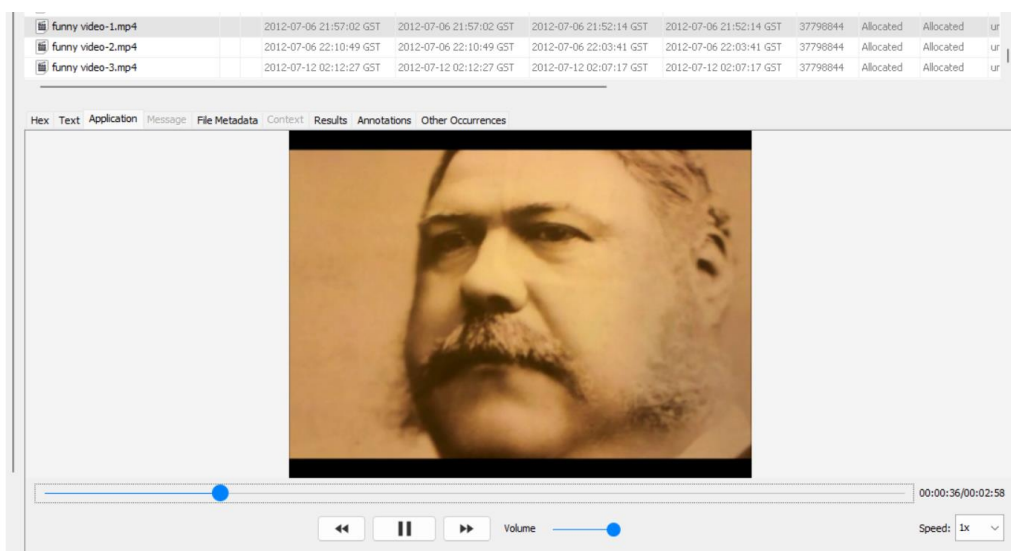
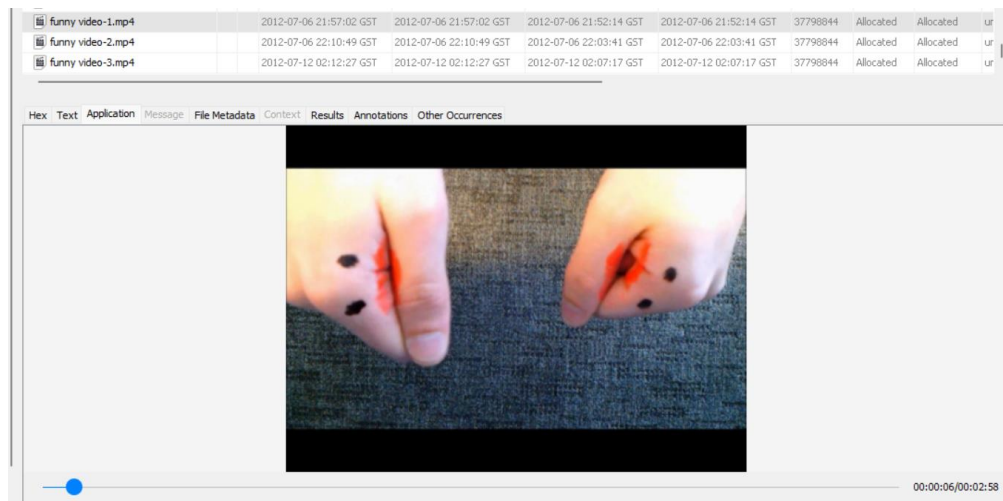


Figure 7.1: funnyvideo.mp4



Figure 7.2: Image of accomplices for the defacement plan

So basically, Alex informed Carry about the plan through a “funny video”. The video, which seemed like a joke initially, had information about the defacement plan and informed Carry that Alex would be sending “associates” to assist in their plan. The information also said that the associates would be arriving at the international airport and had a picture of the said associates so that Carry could identify them.

Finding -8: Carry in touch with a mob organiser.

Another SQLite file (*mailstore.cat2welve@gmail.com.db*) indicated that Carry also had gotten in touch with a mob organizer, the screenshot for which has been provided below.

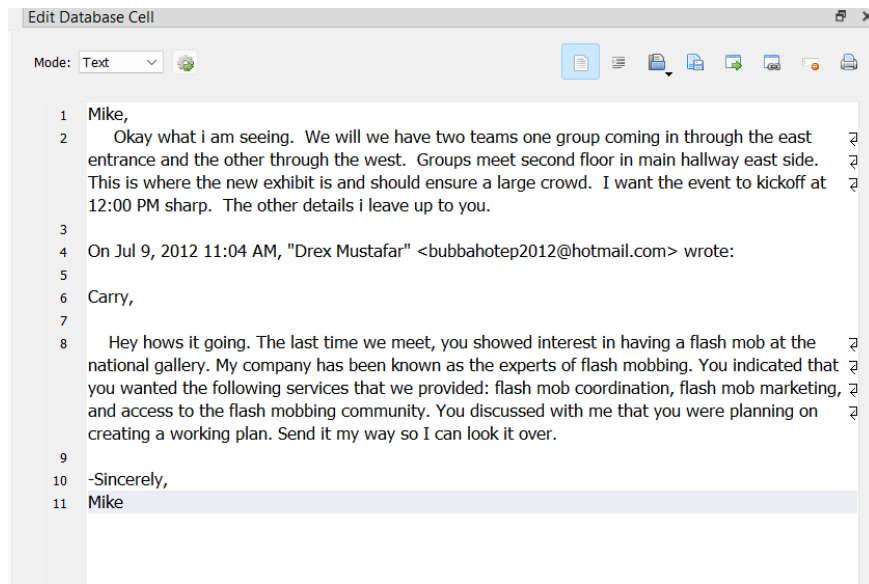


Figure 8.1: conversation between carry and mike discussing the flashmob.

Finding - 9: Carry seeking Tracy for help.

Discussion

This is an inculpatory evidence.

Carry approached Tracy to seek help after watching her Facebook post about recent struggles. The following day, Carry contacts Tracy via email messages and approaches Tracy with the objective of showcasing a flash mob at the art gallery and offers her financial assistance if she can assist Carry with all the necessary details. This was followed by several email exchanges between both parties. Despite Tracy's suspicions, she was bribed with some money. As part of the email messages, it was also stated that Carry had requested assistance in taking her tablet in for this purpose, by offering Tracy lunch in return.

```

1  Carry,
2
3  I would love to. It has been a rough couple of weeks. I have barely had a
4  moment for anything fun. Text me where you think would be good, and I will
5  meet you there around 1 on friday.
6
7  -Tracy
8
9  On Thu, Jul 5, 2012 at 11:51 AM, Carry Sumttwentytwelve <
10 carrysum2012@yahoo.com> wrote:
11
12 > |
13 > Hi,
14 >
15 >
16 > realized that we haven't spoken face to face in quite a while. I was really
17 > hoping that we could get together and have lunch. Does this Friday sound
18 > good? Let me know.
19 >
20 > -Carry
21 >
22

```

Figure 9.1: Carry reaching out to Tracy.

```

< <
> >On Jul 9, 2012, at 2:18 PM, Carry Sumttwentytwelve wrote:
> >
> >>
> >>
> >> Hey I was wondering
> >> if there was any
> I know security isn't to keen on computers and the like in the gallery,
> but maybe you could pull some strings and get it in for me? I can make it
> worth your while :) But really I would happy to get lunch again or
> something else for your help. I want to get some pictures for my flash mob
> event I told you about. Let me know.
> >>
> >>
> >> -----
> >> On Fri, Jul 6, 2012 10:55 AM PDT Tracy Sumtwelve wrote:
> >>
> >> Hey Carry,
> >>
> >> Just wanted to say thanks for lunch. I had a great time and it was good
> catching up with you. We should do lunch more often.
> >>

```

Figure 9.2: Carry wanting her tablet to be sneaked in the gallery.

```

1 Yea sure, that sounds good. See you tommorow!
2
3 Tracy
4
5 On Tue, Jul 10, 2012 at 9:48 AM, Carry Sumttwentytwelve <
6 carrysum2012@yahoo.com> wrote:
7
8 >
9 >
10 > Awesome this will be a big help. Can i come in tommorrow, around 9?
11 >
12 >
13 > -----
14 > On Tue, Jul 10, 2012 6:29 AM PDT Tracy Sumtwelve wrote:
15 >
16 > >Hey,
17 > >
18 > [REDACTED]
19 > pretty ridiculous sometimes! When would you want to get in and take a look
20 > around?
21 > >
22 > >Tracy
23 > >
24 > >On Jul 9, 2012, at 2:18 PM, Carry Sumttwentytwelve wrote:
25 > >
26 > >

```

Figure 9.3: Tracy agreeing to do so.

```

1 Okay carrie I'm going to send this but you need to make sure no one else
2 sees it okay I could get in a bunch of trouble. I want to help you and I
3 c [REDACTED] p [REDACTED]
4
5 On Wed, Jul 11, 2012 at 2:53 PM, Carry Sumttwentytwelve <
6 carrysum2012@yahoo.com> wrote:
7
8 >
9 >
10 > I [REDACTED] want to make
11 > it as painless as possible. I know that your security folk sometimes get
12 > a little out of sorts. Is there a good time or maybe you could just let
13 > know the shift changes so you dont have to know when i am going to do this.
14 > I have a pretty good budget for the event if you would like a little
15 > something for the info.
16 > -----
17 > On Tue, Jul 10, 2012 8:15 AM PDT Tracy TeeSumTwelve wrote:
18 >
19 > >Yea sure, that sounds good. See you tommorow!
20 > >
21 > >Tracy
22 > >
23 > >On Tue, Jul 10, 2012 at 9:48 AM, Carry Sumttwentytwelve <
24 > >carrysum2012@yahoo.com> wrote:
25 > >
26 > >>
27 > >>
28 > >> Awesome this will be a big help. Can i come in tommorrow, around 9?
29 > >>

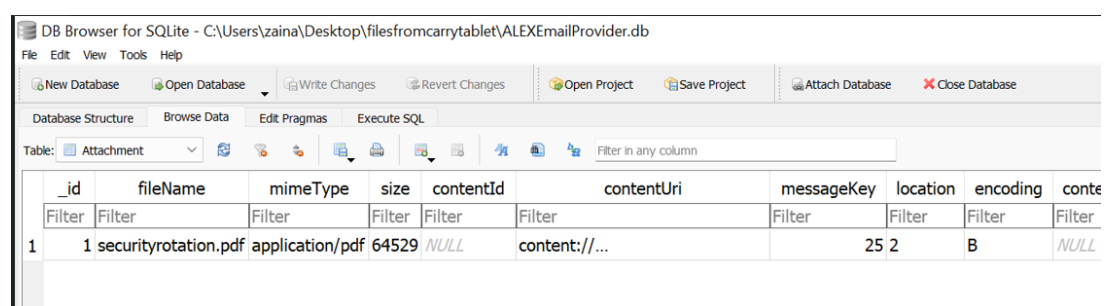
```

Figure 9.4: Tracy agreeing to accept cash in return.

Finding -10: Information about Security Personnel Schedule

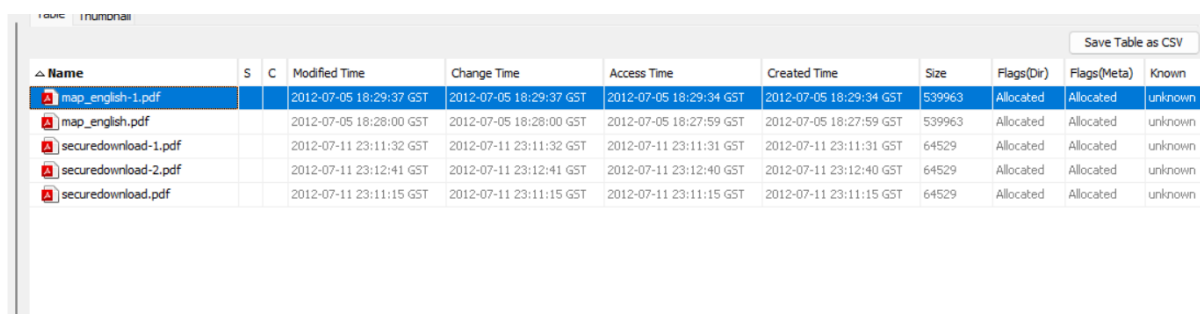
Discussion

Another piece of inculpatory evidence was uncovered while investigating Tracy's and Carry's phones. The evidence is extracted from drive image carry-tablet-2012-07-16-final.tar. Evidence can be found in mnt/sdcard/Download. The name of the file is securedownload-1.pdf. It was also found that this file named securedownload.pdf was forwarded by Tracy to Carry, which contained details about the shifts of the security personnel. It was an official letter from the Office of Personnel Management which outlined the duty schedule for security personnel. This is crucial to the case as it can prove that the heist planned by the suspects can be executed without interference or detection by other employees.



_id	fileName	mimeType	size	contentId	contentUri	messageKey	location	encoding	cont
1	securityrotation.pdf	application/pdf	64529	NULL	content://...	25 2	B	NULL	

Figure 10.1: attachment found in EmailProvider.db viewed in SQLite DB Browser.



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
map_english-1.pdf			2012-07-05 18:29:37 GST	2012-07-05 18:29:37 GST	2012-07-05 18:29:34 GST	2012-07-05 18:29:34 GST	539963	Allocated	Allocated	unknown
map_english.pdf			2012-07-05 18:28:00 GST	2012-07-05 18:28:00 GST	2012-07-05 18:27:59 GST	2012-07-05 18:27:59 GST	539963	Allocated	Allocated	unknown
securedownload-1.pdf			2012-07-11 23:11:32 GST	2012-07-11 23:11:32 GST	2012-07-11 23:11:31 GST	2012-07-11 23:11:31 GST	64529	Allocated	Allocated	unknown
securedownload-2.pdf			2012-07-11 23:12:41 GST	2012-07-11 23:12:41 GST	2012-07-11 23:12:40 GST	2012-07-11 23:12:40 GST	64529	Allocated	Allocated	unknown
securedownload.pdf			2012-07-11 23:11:15 GST	2012-07-11 23:11:15 GST	2012-07-11 23:11:15 GST	2012-07-11 23:11:15 GST	64529	Allocated	Allocated	unknown

Figure 10.2 : PDF evidence found in mnt/sdcard/Download of Carry's tablet.



Security Personnel Duty Schedule:

Shift A1 and A2 Personnel: In designated positions as of 6:00 AM till 3:00 PM F-T except for designated relief time or specific authorization via issued communication channels.

Shift B1 and B2 Personnel: In designated positions as of 6:00 AM till 3:00 PM W-SU except for designated relief times or specific authorization via issued communication channels.

Shift C Personnel: In designated positions as of 3:00 PM till 9:00 PM M-F except for designated relief time or specific authorization via issued communication channels.

Shift D Personnel: In designated positions as of 6:00 PM till 9:00 PM W-SU except for designated relief times or specific authorization via issued communication channels.

Support shift 1 Personnel: Relieve Shift A1 from 12:00 PM to 1:00 PM, Relieve Shift A2 from 1:15 pm to 2:15 PM

Support shift 2 Personnel: Relieve Shift B1 from 12:00 PM to 1:00 PM, Relieve Shift B2 from 1:15 pm to 2:15 PM

Office of Personnel Management

Figure 10.3: Content of the PDF – Security Duty schedule.

Finding -11: Carry's Tablet containing the map for National Gallery of Art DC

Discussion

This is an inculpatory evidence. It serves as further evidence of her involvement in the case. The tablet had detailed maps and floor plans of the National Gallery DC which the suspects could use to plan their activities and identify certain artwork. The maps also showed the gallery's location, address, hours of operation, and on-site services. This evidence was discovered on Carry's tablet in the form of a PDF document located at /carry's tablet/carry-tablet-2012-07-16-final.tar/mnt/sdcard/Download/map_english.pdf.

Upon further investigation, it can be found that a few pages were bookmarked. These pages were the museum's floor plans, including the exit and entry points. Moreover, the map gives a general idea about what will be displayed at the museum and its locations. This information

can help Carry and Alex carry out their plan since they will have a better understanding of the museum.

Save Table as CSV										
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
map_english-1.pdf			2012-07-05 18:29:37 GST	2012-07-05 18:29:37 GST	2012-07-05 18:29:34 GST	2012-07-05 18:29:34 GST	539963	Allocated	Allocated	unknown
map_english.pdf			2012-07-05 18:28:00 GST	2012-07-05 18:28:00 GST	2012-07-05 18:27:59 GST	2012-07-05 18:27:59 GST	539963	Allocated	Allocated	unknown
securedownload-1.pdf			2012-07-11 23:11:32 GST	2012-07-11 23:11:32 GST	2012-07-11 23:11:31 GST	2012-07-11 23:11:31 GST	64529	Allocated	Allocated	unknown
securedownload-2.pdf			2012-07-11 23:12:41 GST	2012-07-11 23:12:41 GST	2012-07-11 23:12:40 GST	2012-07-11 23:12:40 GST	64529	Allocated	Allocated	unknown
securedownload.pdf			2012-07-11 23:11:15 GST	2012-07-11 23:11:15 GST	2012-07-11 23:11:15 GST	2012-07-11 23:11:15 GST	64529	Allocated	Allocated	unknown

Figure 11.1 : PDF of the map found in Carry's tablet.



Figure 11.2 : Floor Map of NGDC.

Finding –12: Images of security Cameras from the National gallery DC

Discussion

A few more pieces of inculpatory evidence are obtained from Carry's Tablet, including photos of security cameras at the National Gallery DC. The suspects wanted to compromise their location to avoid these security cameras photos, hence they revealed their location.

These images were found in a specific location within the tablet's files, at the path/img_carry-tablet-2012-07-16-final.E01/vol_vol7/media/DCIM/Camera/IMG_20120711_090114.jpg

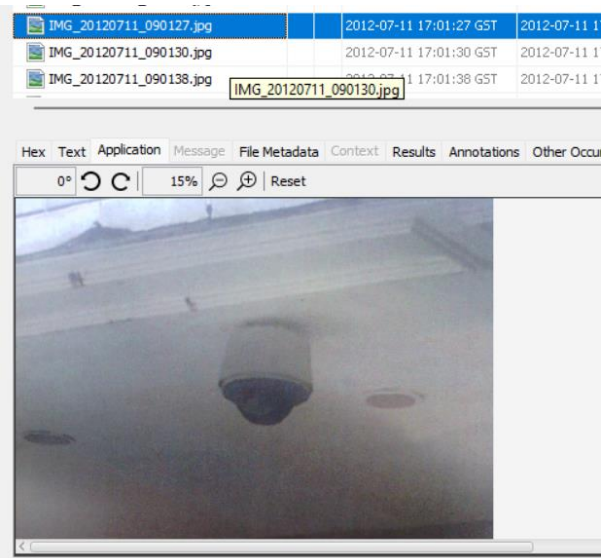
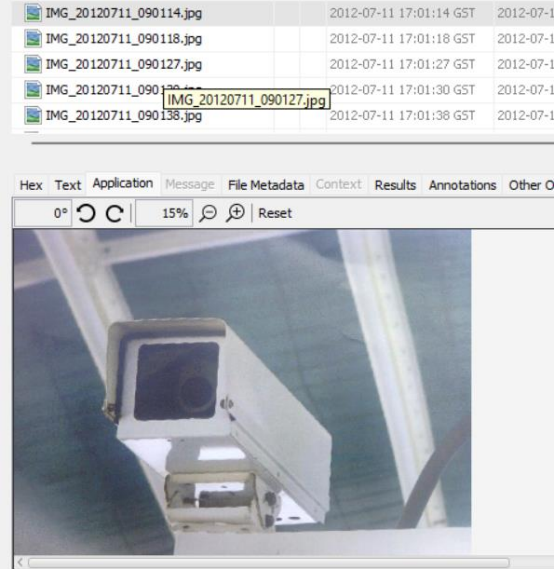


Figure 12.1: Security Cameras

Finding- 13: Carry's search history

Discussion

A few interesting keywords pointed to the browsing history on Carry's tablet. To open these files, SQLite viewer (*DB Browser for SQLite*) was used, and browser2.db file pointed at the preparation that was underway to carry out the attack.

The browsing history also included the National Gallery of Art, Decatur House, DAR Museum, and Library of Congress (potential targets), and search history for shopping spray paints, graffiti suppliers, stealing art, and art forgery techniques was found.

101	101	Mail: Inbox (9)	http://m.yahoo.com/w/ygo-mail/...	0	1341928170787	1
102	102		http://chemistry.about.com/od/...	0	1341935796880	1
103	103		http://www.google.com/...	0	1341935810786	1
104	104		http://m.wikihow.com/Open-a-Door-...	0	1341935948903	2
105	105		http://m.wikihow.com/Make-a-...	0	1341935959154	1
106	106		http://www.google.com/...	0	1341935971746	1
107	107	Make a Smoke Bomb - wikiHow	http://m.wikihow.com/Make-a-Smok...	0	1341936014880	2
108	108		http://m.wikihow.com/Make-a-Smok...	0	1341936140038	2
109	109	Blind a Surveillance Camera - wikiHow	http://m.wikihow.com/Blind-a-...	0	1341936179318	2
110	110	How To Do Stuff: How to Blind a ...	http://how2dostuff.blogspot.com/...	0	1341936228172	1
111	111		http://waynet.hubpages.com/hub/...	0	1341936304461	1
112	112	Crack a "Master Lock" Combination ...	http://m.wikihow.com/Crack-a-...	0	1341936329376	2

Figure 13.1 browser2.db viewed in SQLite DB browser.

Finding 14 Tracy receives suspicious amount of money.

Discussion

From Tracy's phone we extract the 2441-sms.db database using autopsy and view it using SQLite DB browser and find that Tracy gets a \$1000 Target Gift Card through SMS from an unidentified number at 7:36:35 PM on Saturday, July 7th, 2012.

"You've won a \$1,000 Target gift card for free thanks to your participation in last month's lottery! Tell us where to send it by typing ""703"" into the address bar at www.target.com.trdt.biz "For further information, please see the following link:"

It should be noted that the URL seems to be associated with Target Corp, but it is really a subdomain of trdt.biz, for which there is no registration information available at this moment. There is no confirmation that Alex / Carry sent this money, but it is safe to assume that they did.

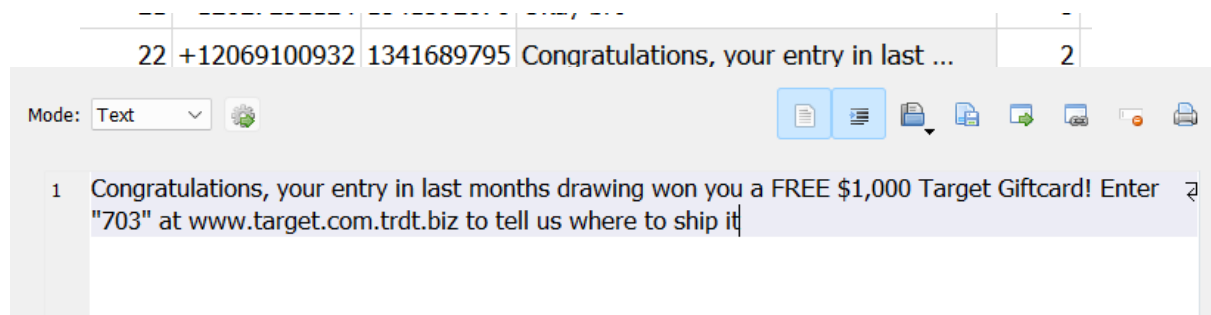


Figure 14 : SMS received by Tracy.

CONCLUSIONS AND SUMMARY

Evidence of theft and defacement:

The investigation uncovered a lot of facts that pointed out the plans of Tracy and Pat to steal with the help of King. Apart from their aliases for communication of these plans, some of the suspects have also shared insurance information documents from the National gallery DC for assessment of the worth of stolen artifacts. Tracy could have been the one who planned this theft because at the time, this plan was formulated after the Tracy and Carry met earlier.

Additionally, in the case of the defacement plot, Alex and Carry are the main suspects. However, even though Alex might not be present in the US, he is linked directly to this case.

Likewise, Tracy also participated in this plan as Carry had requested Tracy to help her take her Tablet inside the national gallery which contained sensitive information and data to carry out this plan. Furthermore, upon investigation of the tablet it contained pictures of security cameras, layout of the National gallery as well as security personnel details.

Reliability of Evidence:

This evidence could be regarded as reliable, since the data has been hashed before and after the investigation, so the forensic investigators can be sure that data was not compromised or tampered with. Additionally, the tools that have been utilized to carry out this investigation provide the investigators with accurate metadata corresponding to each evidence.

Determining whether the suspect is Innocent or Guilty:

The suspects involved in this case are Carry, Tracy and Pat who are mainly involved in planning and organizing the two cases of defacement and theft. As all the evidence found on the devices obtained from Tracy and Carry which also prove Pats involvement, it can be concluded that these suspects are guilty in planning a theft and defacement at the National Gallery DC. Carry is guilty of planning to deface the gallery artwork with her Krasnovian accomplices, while Tracy and Pat are guilty in planning a heist and additionally, Tracy aiding in the defacement plot by allowing Carry's request to take her tablet inside the gallery.

CONCLUSION

All the evidence we've gathered is solid and dependable. It strongly suggests that there were discussions between Carry and Tracy, outlining plans to deface art at the National Gallery Museum and to steal insurance stamps. Moreover, professionals in forensic analysis used the right tools to collect this evidence, making the process highly reliable. The investigation strictly followed the rules, and more than one expert thoroughly examined the drive images.

It can be concluded that the individuals involved, Carry and Tracy, are found guilty. All the evidence gathered from their devices and drive images suggests that they were planning a theft and defacement scheme against the United States. In Tracy's situation, she didn't steal anything, but she is guilty of planning the theft. Carry is also found guilty of planning the defacement;

however, since they were apprehended before executing the plan, and she will not be charged for it.

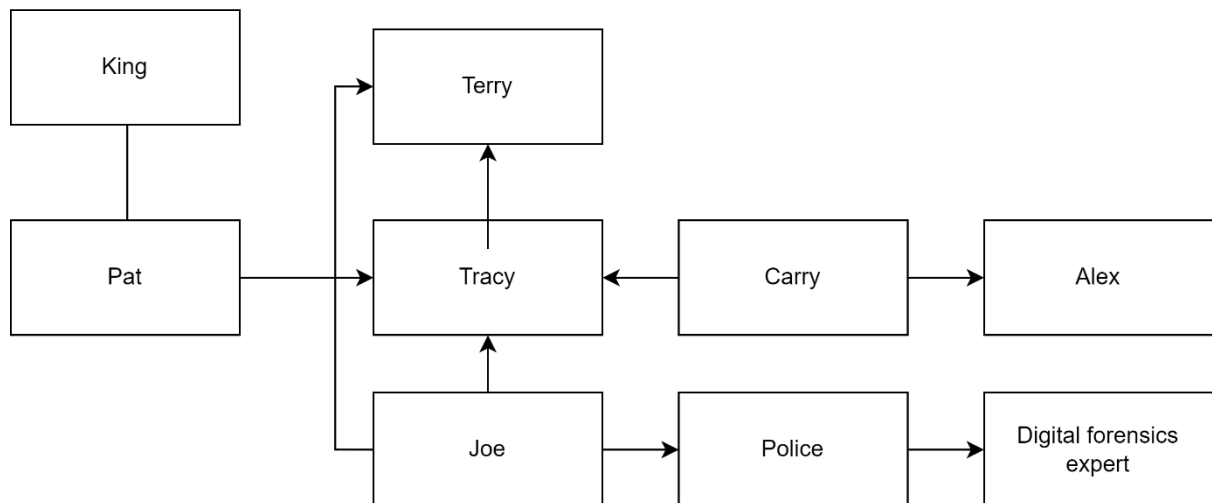
APPENDIX

Appendix I – Description of Persons of Interest

Person of interest	Description
Alex	Alex, a Krasonovian entrepreneur, aims to vandalize artworks from other countries, intending to shame the United States and damage its standing with the foreign nation. He is acquainted with Carry through shared family connections.
Carry	Possesses a criminal record. Shares familial connections with Alex. Supporter of Krasonovia. Possesses a background in technology and actively uses social media. Consents to collaborate with Alex due to their common origin and shared family ties.
Tracy	A mother who recently went through a divorce and is currently in a custody battle. Works at the National Gallery. Facing financial problems, she accepts money from Carry to arrange a flash mob at the museum.
Joe	Tracy's former spouse and Terry's dad. Presently undergoing a divorce. He reported to the police upon discovering Tracy involved in a suspicious plot with her brother.

Terry	The daughter of Joe and Tracy. She desires to remain with her father and continue attending her private school.
Pat	The brother of Tracy. He serves as a police officer in the D.C. Enforcers Bureau.
King	Acquaintance of Pat
Police	Seized the devices of Carry and Tracy due to suspicion.
Forensic investigator team	Gathered evidence from the devices provided by the police.

Appendix II – Association Diagram of Persons of Interest



Appendix III – Evidence Listing

All the artifacts recovered during the investigation have been compiled in this comprehensive list. These items were sourced from drive images generated by various tools, network logs, and emails which are listed in the table below.

Name	Images / Evidence	Description
Carry's Phone	Carry's phone on 2012-07-15 [ZIP - carry-phone-2012-07-15-final] [FTK Logical Dump - carry-phone-logical-2012-07-15-0618]	images of Carry's personal phone
Carry's Tablet	Carry's tablet on 2012-07-16 [E01 - carry-tablet-2012-07-16-final.E01] [TAR - carry-tablet-2012-07-16-final.tar]	images of Carry's tablet that she had set up to use her catsumtwelve email for account dealings with Alex and setting up the flash mob
Tracy's Phone	Tracy's phone on 2012-07-15 (encase) [L01 - Tracy-phone-2012-07-15-1316.L01] [ZIP - Tracy-phone-logical-2012-07-15-1317.zip] Tracy's phone on 2012-07-15 (other extraction tools) [EO1 - tracy-phone-2012-07-15-final.E01]_[tar - tracy-phone-2012-07-15-final.tar]	images of Tracy's personal phone
Tracy's MacBook	Tracy's home computer [E01 - tracy-home-2012-07-16-final.E01] [E02 - tracy-home-2012-07-16-final.E02 (1.4 GB)]	images of Tracy's MacBook. This is the family MacBook Air used by Tracy and Terry and was also used by Joe earlier. Joe installed a keylogger on this system to monitor Terry, which ultimately resulted in the exposure of the conspiracy.
Tracy's External Drive	Tracy's external hard drive [E01 - tracy-external-2012-07-16-final.E01]	This drive had the virtual machine, among other things, used for communication between Tracy and Pat.

Emails	ZIP - email.zip	The emails sent by the keylogger to Joe were also made available for investigation,
--------	-----------------	---

Sl. No	File name	Description	Timest amp	File location
	Bestfit.jpg	Some images of cctv camera were found in carry's tablet	2012-07-12 00:51:26 GST	/carry's tablet/carry-tablet-2012-07-16-final.tar/mnt/sdcard/Android/data/com.dropbox.android/cache/thumbs/Camera Uploads/2012-07-11 09.01.16.jpg/1024x768_bestfit.jpg
	3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx	Crazydave	2012-06-19 T21:38:59	/Tracy's phone/tracy-phone-2012-07-15-final.tar/./private/var/coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
	map_english.pdf	An image of map found on carry's tablet	2012-07-05 18:28:00 GST	/carry's tablet/carry-tablet-2012-07-16-final.tar/mnt/sdcard/Download/map_english.pdf
	Stampinsurance.pdf	Pdf related to stamp insurance found in Tracy's phone	2012-07-06 09:39:52 GST	/Tracy's phone/tracy-phone-2012-07-15-final.tar/./private/var/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs/Stamp Insurance 2.pdf

	Funny video.mp4	An audio sent within a video file by Alex	2012-07-06 22:10:49	/carry's tablet/carry-tablet-2012-07-16-final.tar/mnt/sdcard/Download/funny video-1.mp4
	img.jpg	Images of stamps found in Tracy's phone	2012-07-08 21:00:12 GST	/Tracy's phone/tracy-phone-2012-07-15-final.tar/./private/var/mobile/Media/DCIM/100APPLE/IMG_xxxx.JPG
	img.jpg	Images of security camera	2012-07-11 17:01:14 GST	/carry's tablet/carry-tablet-2012-07-16-final.tar/mnt/sdcard/DCIM/Camera/IMG_20120711_090114.jpg
	securedownload.pdf	Pdf of staff schedule	2012-07-11 23:11:15 GST	/carry's tablet/carry-tablet-2012-07-16-final.tar/mnt/sdcard/Download/securedownload.pdf
	needs.txt	This file contains the tools and requirements for the stamp robbery	2012-07-12 22:51:14 GST	/Tracy's phone/tracy-phone-2012-07-15-final.tar/./private/var/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/60/2/needs.txt

Appendix IV– Plot Timeline

1. June 19, 2012

- Tracy receives an MP3 audio recording attachment from Pat with instructions on setting up a virtual machine (perryatsum@yahoo.com).

2. June 27, 2012

- Alex emails Carry about "Krasnovia" and steganography tools.
3. **July 2, 2012**
 - Tracy informs Pat about the buzz around a foreign exhibit at the office.
 - Tracy seeks financial help from Joe regarding their daughter's tuition, but Joe declines.
 4. **July 5, 2012**
 - Tracy and Carry arrange to meet at Bubba's Grill for lunch (SMS).
 5. **July 6, 2012**
 - Pat sends an audio file to Carry with instructions for VM installation.
 - Pat introduces King to Tracy for job-related help.
 - Tracy thanks Carry for lunch.
 - Tracy receives a \$1000 Target gift card via SMS. (July 7th)
 - Tracy emails documents.zip to coralbluetwo@hotmail.com.
 - Tracy confirms helping Carry get the tablet into the gallery.
 - Tracy and Carry confirm their meeting at Bubba's Grill through SMS.
 - Pat emails King and CC's Tracy about his proposition.
 6. **July 9, 2012**
 - Tracy lists stamps for insurance.
 - Pat and "King" exchange a list of supplies needed.
 7. **July 10, 2012**
 - Pat sends Tracy a copy of the supplies list.
 - Tracy agrees to help Carry with the tablet delivery.
 - Carry schedules a meeting with Tracy for the next day.
 8. **July 11, 2012**
 - Tracy and Carry set up a tablet delivery through SMS.
 - Carry asks Tracy about the security schedule for an event.
 - Tracy advises Carry to be cautious.
 - Carry reassures Tracy about their communication's security.
 9. **July 12, 2012**
 - Tracy texts Carry to inquire about the progress of the flashmob.

- Tracy receives various files related to stamps, security, and navigation on different devices.

Appendix V- Software and Tools used in the Investigation.

Some of the forensic tools used to carry of digital investigation is as follows:

1.Autopsy:

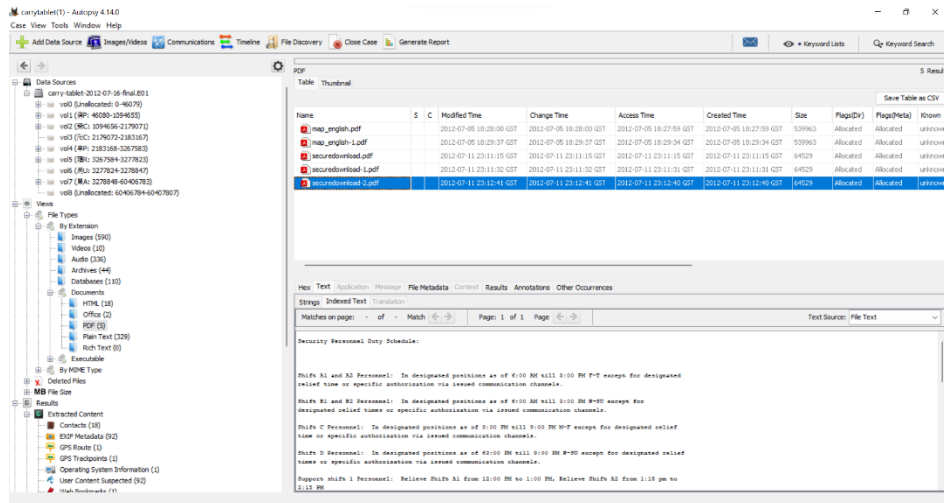
Autopsy is an open-source software platform for digital forensics. Investigators in the law enforcement or military sectors use it primarily for investigations related to digital forensics.

Pros:

- **Open-Source Flexibility:** Being open-source allows for continuous improvements and ensures transparency within the community of forensic investigators.
- **User-Friendly Interface:** Autopsy is recognized for its intuitive design, making it accessible to both seasoned professionals and those new to digital forensics.
- **File Format Support:** It accommodates various file formats crucial in forensic investigations, including E01 files, zip files, and dd files, thereby widening its applicability.
- **Cross-Platform Availability:** Its compatibility with Windows, Linux, and Mac OS ensures accessibility across different operating systems, enabling a wider user base.

Cons:

- **Processing Time for Large Files:** Ingesting larger files can be time-consuming, potentially causing delays in investigations when dealing with substantial amounts of data.



2.DB Browser for SQLite

SQLite DB Browser stands out as a user-friendly, open-source graphical interface tool tailored for managing SQLite database files. SQLite databases are used in various applications, and this tool simplifies the creation, design, and manipulation of these files.

Additional Information:

Pros:

- **Open-Source Advantage:** Its open-source nature encourages collaboration, transparency, and continuous improvement within the community of developers and users.
- **User-Friendly Interface:** The tool's intuitive design enables both novices and experienced users to navigate and utilize its functionalities effectively.
- **SQL Command Support:** Offers the capability to execute basic SQL commands, allowing users to interact with the database using familiar querying methods.
- **Cross-Platform Accessibility:** Available across Windows, Linux, and Mac OS, ensuring accessibility regardless of the operating system.

Cons:

- **Limited to SQLite:** Its functionality is restricted to managing SQLite databases exclusively, limiting its usability in scenarios involving other database systems.
- **Absence of Replication:** Lacks built-in features for database replication, which might be a drawback for users requiring this functionality for data redundancy or distributed systems.

DB Browser for SQLite - C:\Users\zaina\Desktop\EmailProviderBody.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: Body Filter in any column

_id	messageKey	htmlContent	textContent	htmlReply	textReply	source
4	8	<div>Yea sure, that sounds good. See you...	Yea sure, that sounds good. See you...	NULL	NULL	0
5	12	<DOCTYPE HTML PUBLIC "-//W3C//...	Sorry, we were unable to deliver your...	NULL	NULL	0
6	13	...	Greetings Niccs...	NULL	NULL	0
7	14	...	Sorry we haven't talked in a while, I've...	NULL	NULL	0
8	15	...	Why do you have to go?	NULL	NULL	0
9	16	...	I have to go to church.	NULL	NULL	0
10	17	...	Carry...	NULL	NULL	0
11	18	...	Do you like church?	NULL	NULL	0
12	19	...	No, but I have to go there because I'm...	NULL	NULL	0
13	20	...	What do you work on?	NULL	NULL	0
14	21	...	I study rivers and ecology.	NULL	NULL	0
15	22	...	I study literature.	NULL	NULL	0
16	23	...	Hey Carry...	NULL	NULL	0
17	24	...	Hey...	NULL	NULL	0
18	25	...	Yea sure, that sounds good. See you...	NULL	NULL	0
19	26	NULL	NULL	0
20	27	NULL	NULL	0
21	28	NULL	NULL	0
22	29	NULL	NULL	0
23	30	NULL	NULL	0
24	31	NULL	NULL	0
25	32	NULL	NULL	0
26	33	NULL	NULL	0
27	34	NULL	NULL	0

Go to: 1

Mode: Text

```

34 >>> Hey,
35 >>>
36 >>> I can definitely help get your tablet in. Our security guards can be
37 >>> pretty ridiculous sometimes! When would you want to get in and take a
38 > look
39 >>> around?
40 >>>
41 >>> Tracy
42 >>>
43 >>> On Jul 9, 2012, at 2:18 PM, Carry Sumtweentytwo wrote:
44 >>>
45 >>>
46 >>>
47 >>> Hey I was wondering
48 >>> if there was any way you could help me get my tablet into the gallery.
49 >>> I know security isn't to keen on computers and the like in the gallery,
50 >>> but maybe you could pull some strings and get it in for me? I can make
51 > it
52 >>> worth your while :) But really I would happy to get lunch again or
53 >>> something else for your help. I want to get some pictures for my flash
54 > mob
55 >>> event I told you about. Let me know.
56 >>>
57 >>>
58 >>>
59 >>> -----
60 >>> On Fri, Jul 6, 2012 10:55 AM PDT Tracy Sumtweentytwo wrote:
61 >>>
62 >>> Hey Carry,
63 >>>
64 >>> Just wanted to say thanks for lunch. I had a great time and it was
65 > good
66 >>> catching up with you. We should do lunch more often.

```

Type of data currently in cell: Text / Numeric
2758 characters

3. BitRecover EMLX Viewer:

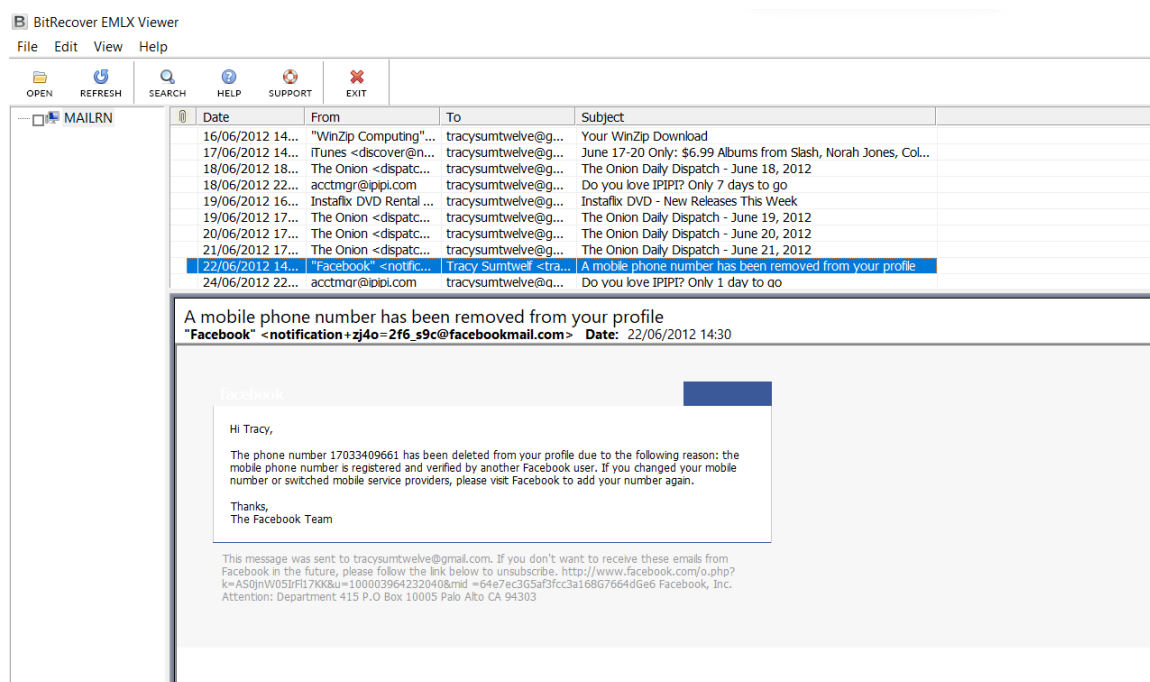
BitRecover EMLX Viewer is a specialized software designed to open and view EMLX files, primarily used in Apple Mail. This tool offers users a convenient way to access and explore the contents of EMLX files without the need for the Apple Mail application.

Pros:

- **Focused Functionality:** Specifically made to open EMLX files used by Apple Mail, ensuring a dedicated and optimized viewer for these files.
- **Ease of Use:** Offers a user-friendly interface, allowing users to navigate through EMLX files intuitively without technical complexities.
- **File Viewing:** Allows users to open and view the content of EMLX files, including email messages, attachments, and metadata.
- **Platform Compatibility:** Designed to work across different operating systems, ensuring accessibility for users on Windows, Linux, and Mac OS.

Cons:

- **Limited to EMLX:** Restriction to only EMLX files might limit its usability for users dealing with different email file formats.
- **Lacks Editing Capabilities:** The tool is focused solely on viewing EMLX files and doesn't offer functionalities for editing or manipulating the content.



Appendix VI - Other Important Listings and Information

6.1 Differences between the sets of the drive images

As far as the image's creation, they seem like they were made through standard procedures. SSL strip tool was utilized to perform a network capturing operation yielding capture files with and without SSL-encrypted traffic.

The differences between different sets of drive images could be due to the file format, imaging method, and nature of the information captured. These formats are different types of extensions such as E01, L01, and TAR in making drive images. The E01 (Expert Witness Format) and L01 (Logical Evidence Format) are proprietary formats, and the TAR (Tape Archive) is a more generic archive. These could also be indicators of different imaging software.

E01 images are produced by Encase Forensic, while L01 images are produced by FTK Imager. However, both formats can produce bit-by-bit images which are important in forensics and possess slack space, metadata, and unallocated space for the investigator to restore the deleted data and for file carving. TAR format can also be used for storing physical images created by Autopsy, Sleuth Kit, and so on. However, logical images do not have any unallocated space nor details about the file system and partitions involved. The images from this study comprised of diverse file formats like E01, L01 and TAR, as well as logical images.

Also, there is the E02 image in the evidence which is produced by Encase. The forensics tools like Encase divide the image into small pieces to make it of small size. It calls these next chunks E01, E02, etc. after imaging it is using Encase.

6.2 Possible Intent or Knowledge of Criminal Activity

In the wake of Joe's submission of the keylogger to law enforcement agencies, there was a revelation of the various conspiracies. As a result, initially Tracy's devices were seized. Analysing the evidence obtained from Tracy's devices enabled the unravelling of other conspiracies. According to the investigation, Tracy and Carry were suspected of participating in two separate conspiracies. Tracy was identified as the primary suspect in the planning and execution of the heist, while Carry was responsible for defacing artworks in the gallery.

It is evident that all the people in both intertwined stories – Tracy, Alex and Carry on for the defacement of art, and Pat and King (again with Tracy) are fully responsible for their actions. Tracy could claim not to be aware of Carry's plan to deface the painting; however, it is still not lawful for her to provide the security rotation of the art gallery (*securityrotation.pdf*) that could be utilized in the planning of illegal activities. Similarly, Carry is not allowed to aid her in taking the tablet into the museum which would have been prevented by the museum security who work against the museum security policies.

Tracy's involvement in the planning of the heist with her brother is a clear indication of possible intent and knowledge of the criminal activity. She willingly sent out the stamp insurance documents to Pat, and both had money problems that they were trying to solve through the planned heist. Here, Tracy or Pat cannot defend themselves with arguments like 'unintentionally committed' or lack of information on the legality of actions.

The evidence also proves that Carry was aware of her actions. She responded to Alex's offer and was proactive with the planning, as indicated by her search history. In addition to this, her email to Alex saying that her plan was ready and that she needed his approval to proceed indicates her intent of the criminal activity.

6.3 Information Relating to Image/Graphic Files

1. Digital Editing Software:

Among the primary tools for image tampering are sophisticated digital editing software like Adobe Photoshop and GIMP. These platforms empower users to manipulate images by altering colors, shapes, and content with a level of precision that challenges the veracity of the original.

2. Copy-Paste Operations:

A prevalent method involves copying portions of one image and seamlessly pasting them onto another. This copy-paste operation allows for the addition or removal of objects, individuals, or elements within an image, altering its overall composition.

3. Splicing:

Splicing is a technique that combines different segments of images to create a cohesive but manipulated whole. For instance, an object or person from one image can be spliced into an entirely different background, creating a convincing yet deceptive narrative.

4. Compression Artifacts:

Compression algorithms, notably employed in JPEG formats, introduce artifacts during the encoding process. Astute manipulators can exploit these artifacts to conceal or fabricate specific features in an image, challenging conventional forensic analysis.

5. Retouching and Airbrushing:

Retouching and airbrushing techniques are applied to enhance or diminish certain features of an image. Frequently used for cosmetic purposes, these methods contribute to the creation of an idealized or altered representation.

6. Metadata Manipulation:

Manipulating metadata embedded within an image file is another strategy employed by those seeking to obscure an image's origin or history. This can include altering timestamps, camera information, or other metadata fields to mislead viewers.

Advancements in Forensic Detection:

In response to the escalating sophistication of image tampering techniques, the scientific community has devised advanced forensic tools and methodologies. The articles you provided discuss cutting-edge methods such as the Earthworm-Rider Optimization Algorithm (EW-ROA) for image tampering detection.

1. Forensic Tools:

Forensic tools, as outlined in the fourth article, are instrumental in the detection process. These tools analyse digital images, generating binary maps that highlight potentially tampered regions. The integration of multiple tools enhances the robustness of the detection process.

2. Earthworm-Rider Optimization Algorithm (EW-ROA):

The EW-ROA, a novel algorithm introduced in the same article, combines the Earthworm Algorithm (EWA) with the Rider Optimization Algorithm (ROA). This integration optimizes the weights of a Deep Belief Neural Network (DBN), offering superior accuracy, sensitivity, and specificity in identifying tampered regions. The algorithm's capacity to balance exploration and exploitation phases contributes to its efficacy.

3. Deep Belief Neural Network (DBN):

DBNs, as part of the proposed method, leverage patterns of data sequences to detect tampered regions in JPEG images. The use of DBNs enhances optimization problem solutions and finds applications in diverse engineering fields, making it a powerful tool for image tampering detection.

Appendix VII – Integrity of Analysed Evidence

The investigation followed proper procedures for hashing the evidence prior to and after investigations. A screenshot of the pre-investigation hash has also been provided below. PowerShell was used for hashing, which enabled a consistent workflow since most of the investigation was carried out on Windows machines, and Windows has PowerShell installed by default.

The Get-FileHash command produces hashes of the specified file. All hashing was done using the SHA256 algorithm.

The post-investigation matched with the earlier hash, which indicated that evidence integrity had been maintained throughout the investigation.

Original Hash of the files before investigating:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\Tracy-phone-logical-2012-07-15-1317.zip"

Algorithm      Hash
-----
SHA256         1E4287DFF75DD2FB84FF46BE3EF5F3152BB894B64030831B442776E522D30329    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-phone-2012-07-15-final.tar"

Algorithm      Hash
-----
SHA256         B209E812AEEAB7B6234F8F6D16BE6B63027E02D667D8882104BD52B3AEA204A1    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-phone-2012-07-15-final.E01"

Algorithm      Hash
-----
SHA256         71AED05A86A753DEC4EF4033ED7F52D6577CCB534CA0D1E83FFD27683E621607    C:\Users\zaina\Desktop\378 fi...
```

```
PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\email.zip"

Algorithm      Hash
-----
SHA256         D1C4470E9E058F83798B6C0C2856E85DF8747783F2105F8C354F366D30A85505    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-phone-2012-07-15-final.zip"

Algorithm      Hash
-----
SHA256         5CFECE099E70529072B6934C6F98F97492985E5A48DAEB64549F96719792D9E    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-phone-logical-2012-07-15-0618.zip"

Algorithm      Hash
-----
SHA256         CBCEE1CB354884EBFA302AD5A6E41C9980FC3BA252B2F74E732B2162540F7357    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-tablet-2012-07-16-final.E01"

Algorithm      Hash
-----
SHA256         26A6EA3049C06AFDD34862C453FC272A5AB4C64954AE51D23CF9DF688473A448    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-tablet-2012-07-16-final.tar"

Algorithm      Hash
-----
SHA256         C70762E49DB8F95CFD11246A3E84D1FCA8A20D7182D1525B462638A28331793F    C:\Users\zaina\Desktop\378 files\carry-tablet-2012-07-16-final.tar

PS C:\Users\zaina>
```

```
PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\Tracy-phone-2012-07-15-1316.L01"

Algorithm      Hash
-----
SHA256         A14525B7ECE67131D5943E1DB5847CBB51513E384B49B7FA9921480530223F52    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-home-2012-07-16-final.E02"

Algorithm      Hash
-----
SHA256         41ABC88804FEF9DF6630059CA728F3F1F29A7ED69690073CBCDC980131AAF922    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-home-2012-07-16-final.E01"

Algorithm      Hash
-----
SHA256         26218DD0553A5F22CD11E98AAE42E7B89C9739BBA87EE8B1DE5CD43A069EF17C    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-external-2012-07-16-final.E01"

Algorithm      Hash
-----
SHA256         BFFF9410215485BE97D57ED7064C576319CAFACC4BFEAD179E070AF77C5B6078    C:\Users\zaina\Desktop\378 fi...
```

Hashes of the files after investigating:

```
PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\Tracy-phone-logical-2012-07-15-1317.zip"

Algorithm      Hash
-----
SHA256         1E4287DFF75DD2FB84FF46BE3EF5F3152BB894B64030831B442776E522D30329    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-phone-2012-07-15-final.tar"

Algorithm      Hash
-----
SHA256         B209E812AEAB7B6234F8F6D16BE6B63027E02D667D8882104BD52B3AEA204A1    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-phone-2012-07-15-final.E01"

Algorithm      Hash
-----
SHA256         71AED05A86A753DEC4EF4033ED7F52D6577CCB534CA0D1E83FFD27683E621607    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\Tracy-phone-2012-07-15-1316.L01"

Algorithm      Hash
-----
SHA256         A1452587ECE67131D5943E1DB5847CBB51513E384B49B7FA9921480530223F52    C:\Users\zaina\Desktop\378 fi...
```

```
PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-tablet-2012-07-16-final.E01"

Algorithm      Hash
-----
SHA256         266AE3A049C06AFDD34862C453FC272A5AB4C64954AE51D23CF9DF688473A448    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-tablet-2012-07-16-final.tar"

Algorithm      Hash
-----
SHA256         C70762E490B8F95CFD11246A3E84D1FCA8A20D7182D1525B462638A28331793F    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-phone-logical-2012-07-15-0618.zip"

Algorithm      Hash
-----
SHA256         CBCEE1CB354884EBFA302AD5A6E41C9980FC3BA252B2F74E732B2162540F7357    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\carry-phone-2012-07-15-final.zip"

Algorithm      Hash
-----
SHA256         5CFEC4E099E70529072B6934C6F98F97492985E5A48DAEB64549F96719792D9E    C:\Users\zaina\Desktop\378 fi...
```

```
PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-home-2012-07-16-final.E02"

Algorithm      Hash
-----
SHA256         41ABC88804FEF9DF6630059CA728F3F1F29A7ED69690073CBCDC980131AAF922    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-home-2012-07-16-final.E01"

Algorithm      Hash
-----
SHA256         26218DD00553A5F22CD11E98AAE42E7B89C9739BBA87EE8B1DE5CD43A069EF17C    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\tracy-external-2012-07-16-final.E01"

Algorithm      Hash
-----
SHA256         BFFF9410215485BE97D57ED7064C576319CAFAACC48FEAD179E070AF77C5B6078    C:\Users\zaina\Desktop\378 fi...

PS C:\Users\zaina> Get-FileHash "C:\Users\zaina\Desktop\378 files\email.zip"

Algorithm      Hash
-----
SHA256         D1C4470E9E058F83798B6C0C2856E85DF8747783F2105F8C354F366D30AB5505    C:\Users\zaina\Desktop\378 fi...
```

REFERENCES

[1] H. Munawer Al-Otum and A. A. Ali Ellubani, ‘Secure and effective color image tampering detection and self restoration using a dual watermarking approach’ ScienceDirect Volume 262, July 2022,

<https://www.sciencedirect.com/science/article/abs/pii/S0030402622006155?via%3Dihub>

[2] X. Yuan, X Li and Tong Liu, ‘Gauss–Jordan elimination-based image tampering detection and self-recovery’, ScienceDirect Volume 90, January 2021,

<https://www.sciencedirect.com/science/article/abs/pii/S0923596520301855?via%3Dihub>

[3] L. Zheng, Y. Zhana and V. L. L. Thing, ‘A survey on image tampering and its detection in real-world photos’, ScienceDirect Volume 58, January 2019, Pages 380-399,

<https://www.sciencedirect.com/science/article/abs/pii/S104732031830350X>

[4] R. Cristin, S. P. Premnath and J. P. Ananth, ‘Image tampering detection in image forensics using earthworm-rider optimization’, Wiley Online Library 28 August 2022,

<https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.7293>