



Cybersecurity

21.3 The Final Report

Case Report National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

[Evidence relating to theft of valuable stamps](#)

[Evidence relating to defacement of museum art](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: WiFi and GPS Location Information](#)

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

- Tracy is a suspect in the aforementioned conspiracy.
- As part of the investigation, Tracy'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.

Based on the evidence shown below, it appears that Tracy and her brother Pat conspired with an unknown 3rd party with email address "King kthings throne1966@hotmail.com" to steal stamps from the National Gallery.

Equipment and Tools

Digittech used the following tools:

- Autopsy - which is an open-source forensics tool
- Kali Linux host to analyze an image of Tracy's iPhone.

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone1,2	vol5/logs/AppleSupport/general.log
Host Name	Tracy-Sumtwelve-iPhone	vol5/mobile/preferences/SystemConfiguration
OS Version	iPhone OS 4.2.1 (8C148)	vol5/logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	vol5/logs/AppleSupport/general.log
User Email	IMAP: tracysumtwelve@gmail.com POP: coralbluetwo@hotmail.com	vol5/mobile/Library/Mail/Envelope Index
Phone Number	1 (703) 340-9661	vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log.1
IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	n/a (tracy-phone-2012-07-15-final.E01 image)
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	n/a (tracy-phone-2012-07-15-final.E01 image)

Evidence to Establish Personas

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

Tracy:

Phone Number: (703) 340-9961
 Personal Email: tracysumtwelve@gmail.com
 Work Email: tracy.sumtwelve@nationalgallerydc.org
 Relationship: Accused

Pat:

Phone Number: (571) 308-3236
Email: perrypatsum@yahoo.com/patsumtwelve@gmail.com
Relationship: Tracy's brother

Terry:

Phone Number: (703) 829-6071
Email: unknown
Relationship: Tracy & Joe's daughter

Joe:

Phone Number: unknown
Email: unknown
Relationship: Tracy's ex-husband

Carry:

Phone Number: (202) 725-2124
Email: unknown
Relationship: Tracy's accomplice and friend

We were able to trace Carry and Tracy to find that they were culprits.

Evidence relating to theft of valuable stamps

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

Emails and SMS messages were exchanged between Tracy, Pat, Carry, and an unnamed co-conspirator with email address "King kthings throne1966@hotmail.com" (referenced in Appendix A).

One email from "King kthings" contained an attachment with a list of items needed for the theft.

Figure 1: Email attachment 'needs.jpg' from "King kthings"

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

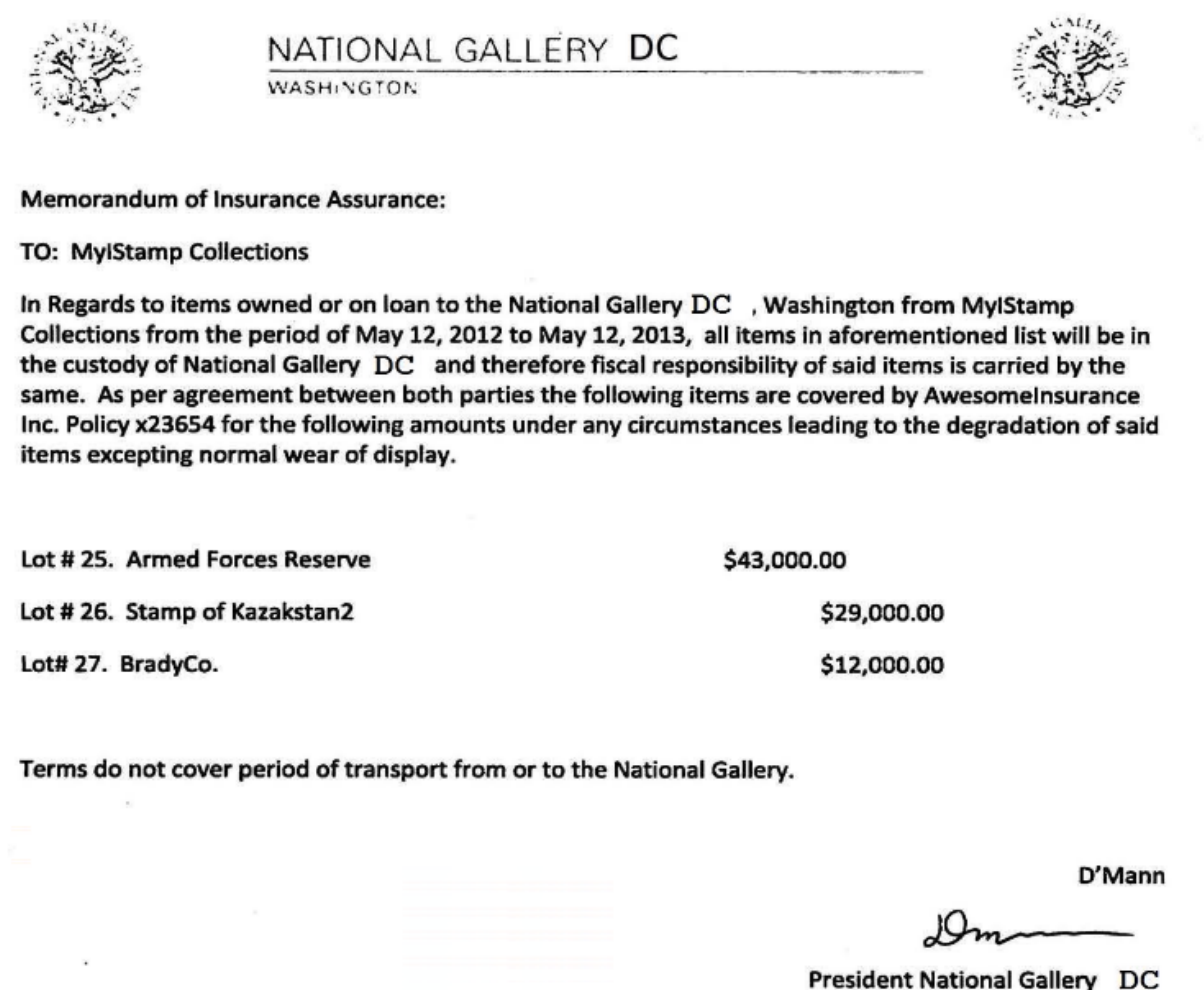
There was also an MP3 audio file attachment (Crazydave1.mp3) with covert instructions on how to install a VirtualBox VM on a host computer, which was to be used for this crime.

There was an SMS message notifying Tracy that she had received a \$1000 Target Giftcard, with instructions to visit a misleadingly named website (www.target.com.trdt.biz) with instructions to entre a numeric code followed by "where to ship it". The website 'trdt.biz' domain is no longer registered by anyone, and it uses 'www.target.com' as a subdomain to hide the fact that it's really a part of 'trdt.biz', and is not affiliated with the Target corporation.

There were 3 .pdf email attachments which were Memoranda of Insurance for various valuable stamps and photos of those stamps in the camera storage location (shown below).

In addition, there were photo images of each of the stamps listed in the insurance documents on the phone.

Figure 2 - Stamp_insurance1.pdf email attachment



- /vol5/mobile/Media/DCIM/100APPLE/IMG_0056.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0051.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0057.JPG

Figure 3 - The three stamps mentioned in Figure 2 above



Figure 4 - Stamp_insurance2.pdf email attachment

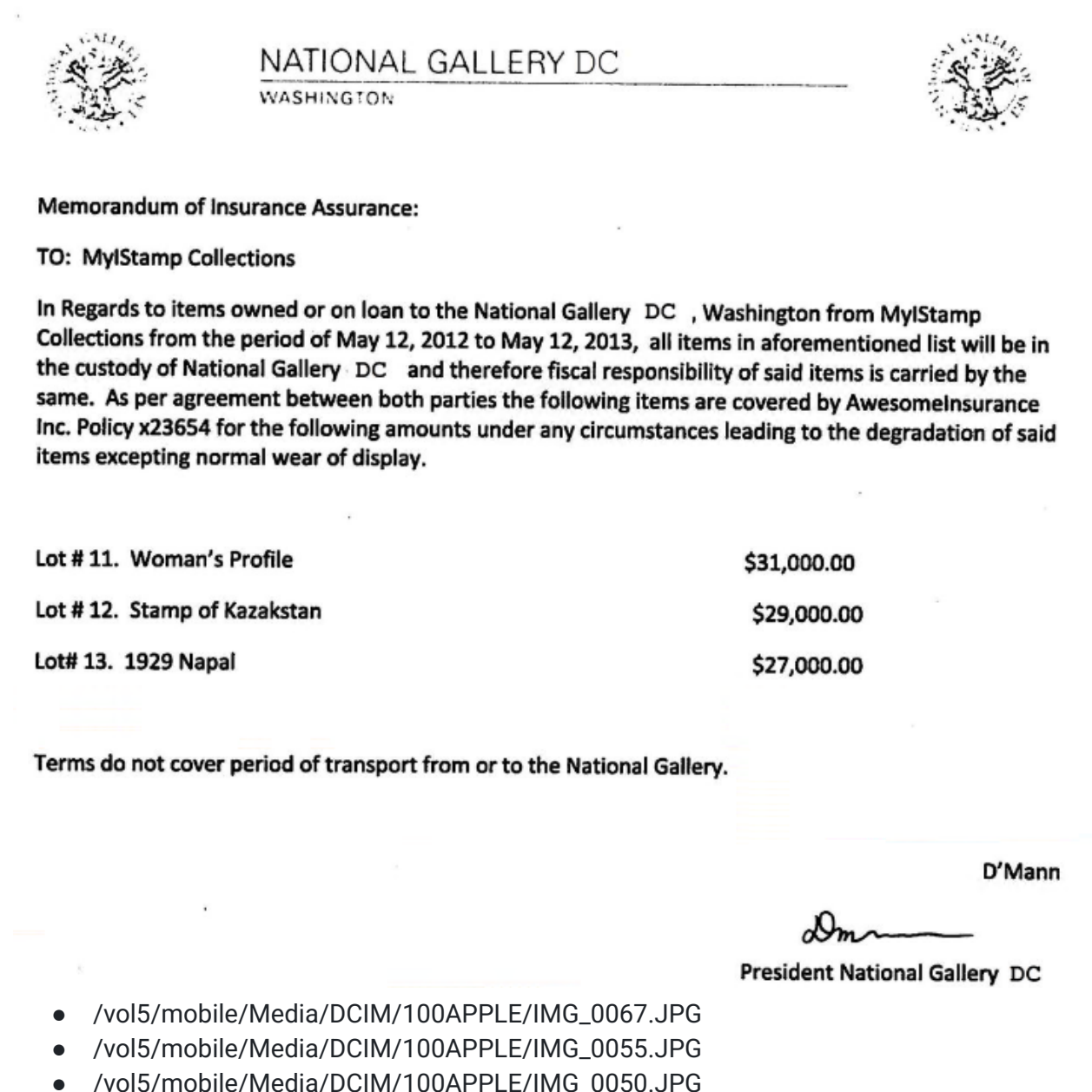


Figure 5 - The three stamps mentioned in Figure 4 above



Figure 6 - Stamp_insurance3.pdf email attachment



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 MacArther	\$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

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0054.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0065.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0071.JPG

Figure 7 - The three stamps mentioned in Figure 6 above



Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

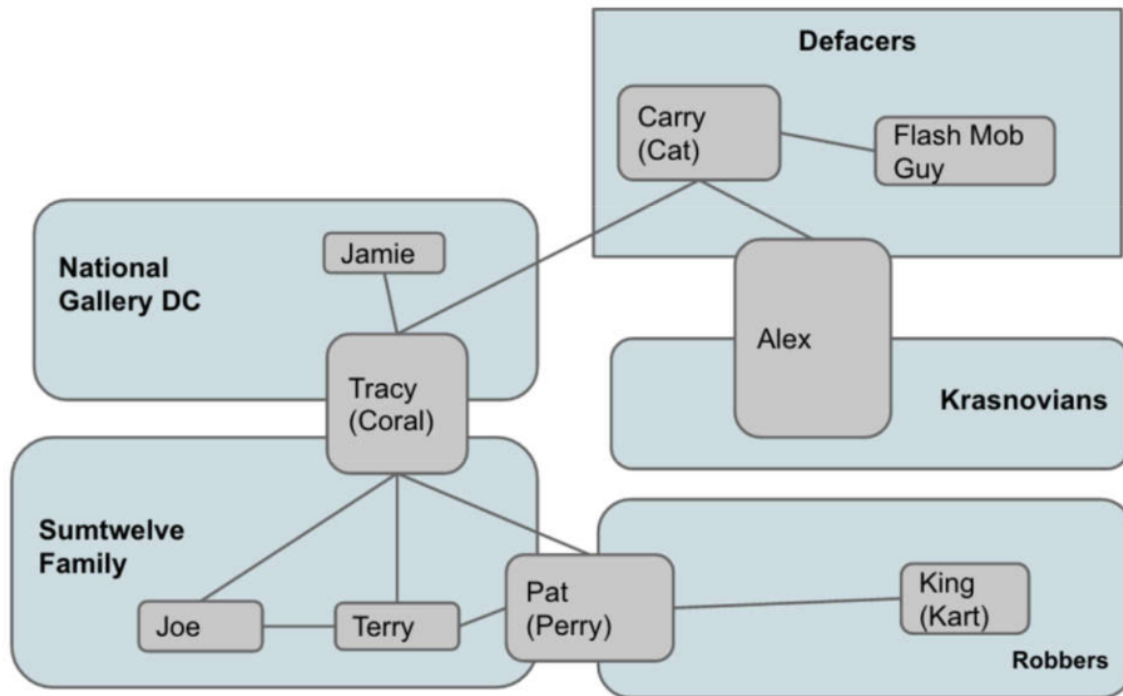
There was no evidence related to defacement of museum art in the iphone image. Only evidence related to the theft of stamps.

Plot Timeline

For details please refer to Appendix A below and the section labeled 'Evidence relating to theft of valuable stamps' above.

- On Tue, Jun 19 2012 at 02:38 PM, Pat (perrypatsum@yahoo.com) emails Tracy (coralbluetwo@hotmail.com) with an MP3 audio recording attachment that contains synthesized voice instructions on how to install a VirtualBox VM on her computer "for later use".
- On Thu, Jul 5 2012 06:18:23 PM Tracy and Carry agree via SMS to meet at Bubba's Grill
- Fri Jul 6 2012 11:49:31 AM Pat arranges via email with subject "can't pass up", a "proposition" with someone who goes by "King" (throne1966@hotmail.com) and Tracy.
- On Fri, Jul 6 2012 04:27:16 PM Tracy and Carry confirm the meeting at Bubba's via SMS.
- On Sat, Jul 7 2012 07:36:35 PM, Tracy receives an SMS from an unknown number that she has received a Target Gift Card worth \$1000 "Congratulations, your entry in last months drawing won you a FREE \$1,000 Target Giftcard! Enter ""703"" at www.target.com.trdt.biz to tell us where to ship it". Note that the URL is faked to look like it's related to Target Corp, but is a subdomain of trdt.biz, for which no registration can be found at this time. Presumably, this payment was received from Alex, but there is no proof.
- Mon, Jul 9 2012 10:44:11 AM Tracy sends herself an email describing which stamps to steal, and how much they are insured for.
- On Mon, Jul 9 2012 10:44:11 AM, Pat and "King" arrange via email a list of things that King will need to do the job.
- Tue, Jul 10 2012 11:24 AM, Pat forwards the list to Tracy.
- On Wed, Jul 11 2012 12:41:45 PM, Carry and Tracy arrange via SMS for Tracy to deliver a tablet to Carry.
- On Thu, Jul 12 2012 05:06:45 PM, Tracy texts Carry to ask how the flashmob is going.

Figure 8 - Persons under investigation



Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy and Pat conspired with each other using email account aliases. Pat used 'patsumtwelve@gmail.com' and Tracy used 'coralbluetwo@hotmail.com'. Pat's usual email address is 'perrypatsum@yahoo.com', and Tracy's normal email address is 'tracysumtwelve@gmail.com'
- Pat coordinated with a known criminal 'King' with email address 'throne1966@hotmail.com' to steal some valuable stamps. Pat knows King's parole officer, so he was able to exert influence on King.
- Tracy conspires with Carry to deliver a notebook with data pertaining to a flashmob that Carry wants to organize. This would help to distract the museum's security guards while King commits the theft.
- Tracy sends herself documents related to the stamps and how much they are insured for.
- Tracy is notified that a 'Gift Card' for \$1000 has been set up for her. This is most likely payment from either Carry via Alex, or directly from Alex. The website URL is purposely

crafted to look like it is from Target, but is actually located in the trdt.biz domain. No information on that URL is available at this time.

- There are three clusters of WiFi and Cell location info, but it's not clear what the significance is. Further analysis would be needed to correlate the location info and timing with the email and SMS exchanges.

Appendix A: Correspondence Evidence

This subsection will provide an amalgamation of the email and SMS correspondence evidence.

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1.	6/19/2012 20:06:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Paris Speak and answer	Pat emails Tracy letting her know that he has accepted her proposal and asks her to email using her alias for further instructions.	Mailbox Data Structure
2.	6/19/2012 20:26:47	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: Look me up sometime	Pat (Perry) emails Tracy to ask her to communicate using her alias.	Mailbox Data Structure
3.	6/19/2012 21:38:59	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.co	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Mailbox Data Structure

		m Subject: Crazydave by the VMs Attachment: Crazydave1.mp3		
4.	6/19/2012 21:39:34	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: ???	Pat (Perry) replies to Tracy (Coral) confirming that he was getting her emails.	Mailbox Data Structure
5.	6/21/2012 17:43:15	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Crazydave by the VMs	Pat (Perry) replies to Tracy (Coral) on an email thread about Virtual Machine installation saying that she should listen to some other songs as well. In the email thread, Tracy (Coral) confirms that the instructions sent earlier in the audio file helped her.	Mailbox Data Structure
6.	6/28/2012 19:31:33	6/28/2012 19:31:33 F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Whats going on	Pat (Perry) emails Tracy (Coral) asking her to henceforth communicate using the aliases and the Virtual Machine setup to keep them safer. He also indicates that they might have to get into riskier/illegal business since both of them were facing financial hardships. He tells her that few of his workplace friends were good at these businesses and that he will inform her should something pop up; in the meantime they should keep discussing some ideas for the same.	Mailbox Data Structure
7.	6/29/2012 14:21:56	F: perrypatsum@yahoo.com T:	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some	Mailbox Data Structure

		coralbluetwo@hotmail.com Subject: Re: Whats going on	money. To Pat's suggestion that they use the Virtual Machines and aliases to communicate and keep looking for ways to make money, Tracy replies that she will keep her eyes open for opportunities and insists that Pat try to get in on some business soon, since her kid didn't want to change schools. She also indicates that she is paying attention to documents especially insurance papers so that she could identify something of potential. Pat assures that he will make something happen although he is nervous because IA has been sniffing around.	
8.	6/29/2012 14:31:36	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: hey sis	Pat (Perry) emails Tracy addressing her as 'sister' and enquires about Terry. Asks her to check in with Coral with whom he has been planning some things. He also suggests all of them going together for dinner as friends. He asks Tracy to check in with Coral. Possible misdirection attempted by referring to Coral as a third person in the narrative.	Mailbox Data Structure
9.	6/29/2012 15:21:35	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	Pat (Perry) replies to the email thread allaying Tracy's (Coral) concern about IA sniffing around him. Tracy in her earlier email in the thread says that although nothing interesting has turned up yet she expects something soon. Pat in his email mentions that they can certainly get the job done if something like what they had earlier discussed pops up.	Mailbox Data Structure

10.	7/2/2012 16:13:18	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	Mailbox Data Structure
11.	7/2/2012 20:00:31	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Email thread: Some good news Following up on the earlier email about the exhibit, Tracy (Coral) mentions going through documents related to the exhibit from which she found that the exhibit is worth a lot of money but the shipping cost is very low comparatively. Pat (Perry) emails back saying that such a thing may mean that the exhibit is something small which would be a very good thing for them.	Mailbox Data Structure
12.	7/3/2012 13:29:37	F: joe.sum.twelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Regarding Terry	Email Thread: Regarding Terry Tracy emails Joe asking whether he could help her with Terry's tuition this year since it is becoming too expensive for her. Joe replies back saying that he won't be paying Terry's tuition if she is not living with him.	Mailbox Data Structure
13.	7/3/2012 14:53:04	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) saying that the exhibit is rare and highly valuable stamp collection and that may be this is their opportunity. Pat (Perry) replies to Tracy (Coral)	Mailbox Data Structure

		news	asking her to collect as much information as possible about the stamp exhibit and that in the meantime he would look into options for pulling off the heist.	
14.	7/5/2012 15:51:31	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Long time no see...	Carry reaches out to Tracy asking her if they could meet-up for lunch and suggests this Friday. She also mentions that through Facebook she realized that Tracy was having a hard time recently.	Mailbox Data Structure
15.	7/6/2012 15:27:51	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy emailed Pat saying that she spoke with Coral and that Coral got some great news about her job and suggested that Pat catch up with Coral. Pat replied back saying that he knows a guy called King.	Mailbox Data Structure
16.	7/6/2012 15:49:31	F: patsumtwelve@gmail.com T: throne1966@hotmail.com Cc: coralbluetwo@hotmail.com Subject: can't pass up	Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at national gallery. He also threatens King to comply or else he would put King's parole in jeopardy.	Mailbox Data Structure
17.	7/6/2012 17:59:24	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy suggests they (meaning King, Tracy and Pat) should hang out sometime. Pat emails Tracy with account login information for:	Mailbox Data Structure

			coralblue@hotmail.com Password: legalBee	
18.	7/9/2012 14:44:11	F: tracysumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: things	documents.zip is a compressed ZIP folder containing 3 insurance documents related to stamps. docs.zip is an encrypted ZIP folder containing 3 insurance documents related to stamps.	/mobile/Library/Mail/POP - coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Message s/8 A3BD06F-CDB1-4453 - 9C69-77E06823F2A E.emlx
19.	7/9/2012 18:18:47	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see..	Email Thread: Long time no see... Tracy thanked Carry for the lunch. Carry emails Tracy asking for help sneaking in a tablet for a flash mob event they had spoken earlier about. Carry suggests that Tracy would be compensated in some way for the help.	Mailbox Data Structure
20.	7/10/2012 13:48:40	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Email Thread: Long time no see... Tracy agrees to help Carry sneak in the tablet and asks when Carry would like to get in to take a look around the gallery. Carry replies saying that this would be a big help and asks if she could come around 9 tomorrow.	Mailbox Data Structure
21	7/10/2012	F: patsumtwelve@gmail.com	Email Thread: cant' pass up King agrees to help with the heist	/mobile/Library

	15:24:57	T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	and sends in a document with equipment required for it. The attached document is saved as a 'txt' file. Pat forwards that email to Tracy (Coral) *needs.txt is a pdf file which was saved with a wrong extension.	y/Mail/POP - coralbluetwo@hotmail.com @pop3.live.com/INBOX.mbox/Message s/9 F0508B8-04FB-490E-A7F0-3E23B0E7C5 9B.emlx
22.	7/11/2012 17:06:19	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Email Thread: Long time no see Tracy confirms the meet at 9 tomorrow. Carry wants Tracy to pass her information regarding shift changes of security. She suggests that Tracy would be well compensated for the information. Tracy confirms that she will give the security shift information Carry requested in exchange for money but asks Carry to be careful with it. Carry replies asking Tracy not to worry and says "It will be gun".	Mailbox Data Structure
23.	7/11/2012 19:28:53	F: "Google+" <noreply-5dd47ca1@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve added you on Google+	Email Thread: Long time no see Previous email from the thread from Carry asking for the security shift details from Tracy.	Mailbox Data Structure

24.	7/11/2012 23:22:03	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+ informing Tracy that Carry had shared an album.	Mailbox Data Structure
25.	7/12/2012 16:12:07	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+ informing Tracy that Carry had shared an album.	Mailbox Data Structure
26.	7/12/2012 18:03:51	F: carriesum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Email Thread: Long time no see... Tracy emailed Carry asking her what she meant by "It will be gun". Carry replies saying that it was a typographical error and she meant "It will be fun".	Mailbox Data Structure

Appendix B: WiFi and GPS Location Information

WiFi locations gathered from /vol5/root/Library/Caches/locationd/consolidated.db and plotted using maps.google.com.

Figure B1 - National Gallery with green marker vs. iPhone GPS Lat / Lon tracking coordin

