

CASE REPORT

NATIONAL GALLERY DC

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

TABLE OF CONTENTS

<i>Case Report</i>	<i>1</i>
<i>National Gallery DC</i>	<i>1</i>
Executive Summary	3
Details of Tracy's iPhone	3
Relevant Evidence	3
Evidence relating to theft of valuable stamps	6
Evidence relating to Defacement of Museum Art	7
Plot Timeline	8
Email Content	9
SMS Message Content	16
Wi-Fi/GPS location information	17
Conclusion	17

EXECUTIVE SUMMARY

On January 21, 2016, DigiTech Inc. was called in to assist with the National Gallery, Washington DC (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of a museum of art at the NGDC.

- Tracy is a suspect in the above-mentioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- DigiTech Inc. was tasked with investigating evidence relevant to the above-mentioned conspiracy.

As described fully in this report, DigiTech, Inc. made the following findings:

In the following, we discovered messages related to theft from the National Gallery

DETAILS OF TRACY'S IPHONE

Name	Findings	Location in iPhone image file
Model	iPhone 3G	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 19:03:28	/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	vol5/mobile/Library/Mail
Phone #	(703) 340-9661	/logs/lockdownd.log.1
Serial #	86004482Y7H	/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	/logs/lockdownd.log.1
IMEI	012021003735398	/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	

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
Email: tracysumtwelve@gmail.com
Work email: tracy.sumtwelve@nationalgallerydc.org
Secret email: coralbluetwo@hotmail.com
Relationship: Accused

Pat:

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

Terry:

Phone Number: (703) 829-6071
Email: TerryJMcGinnis@gmail.com
Relationship: Tracy's Daughter

Joe:

Phone Number: No phone number available in data
Email: joe.sum.twelve@gmail.com
Relationship: Tracy's soon to be ex-husband

Carry:

Phone Number: (202) 725-2124
Email: carrysum2012@yahoo.com
Relationship: She is acquaintances with Tracy

King (Alias):

Phone Number: No phone number available
Email: throne1966@hotmail.com
Relationship: Associate of Pat

Tracy is the primary suspect in the theft. Pat is Tracy's brother. Joe is Tracy's ex-husband and has a child, Terry, with Tracy. Carry is an acquaintance of Tracy's. King is on parole and recruited for the stamp heist.

Evidence relating to theft of valuable stamps

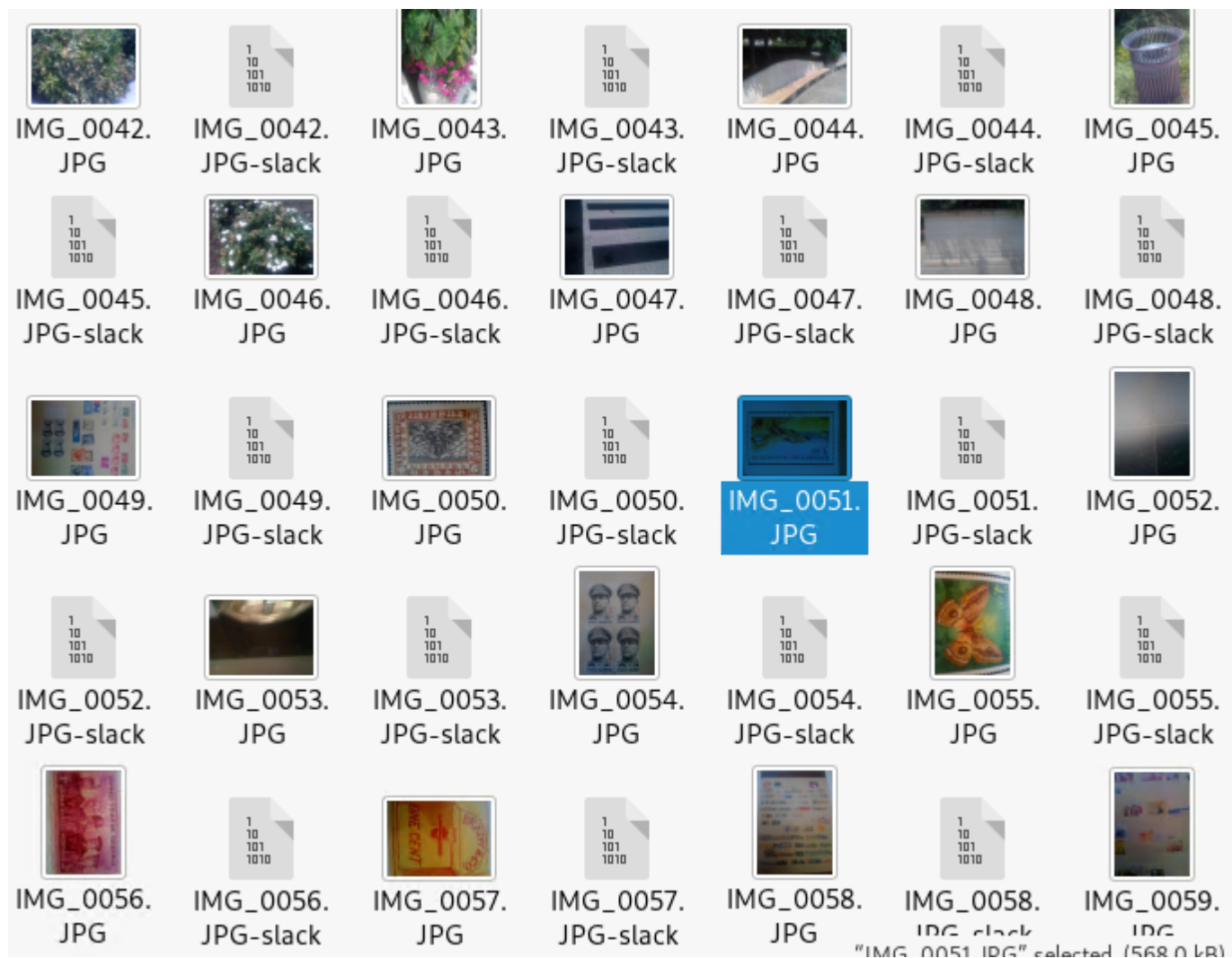
This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

In Tracy's email there is an email to King giving details about the theft at the National Gallery. Also several files discussing the values of the stamps, which could be the motive for the crime.

NATIONAL GALLERY DC WASHINGTON		NATIONAL GALLERY DC WASHINGTON		NATIONAL GALLERY DC WASHINGTON																			
<p>Memorandum of Insurance Assurance:</p> <p>TO: MyStamp Collections</p> <p>In Regards to items owned or on loan to the National Gallery DC, Washington from MyStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned lot 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 Aesom Insurance Inc. Policy #23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.</p> <table border="0"> <tr> <td>Lot # 25. Armed Forces Reserve</td> <td>\$43,000.00</td> </tr> <tr> <td>Lot # 26. Stamp of Kazakhstan</td> <td>\$29,000.00</td> </tr> <tr> <td>Lot # 27. BradyCo.</td> <td>\$12,000.00</td> </tr> </table> <p>Terms do not cover period of transport from or to the National Gallery.</p> <p style="text-align: right;">D'Mann President National Gallery DC</p>		Lot # 25. Armed Forces Reserve	\$43,000.00	Lot # 26. Stamp of Kazakhstan	\$29,000.00	Lot # 27. BradyCo.	\$12,000.00	<p>Memorandum of Insurance Assurance:</p> <p>TO: MyStamp Collections</p> <p>In Regards to items owned or on loan to the National Gallery DC, Washington from MyStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned lot 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 Aesom Insurance Inc. Policy #23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.</p> <table border="0"> <tr> <td>Lot # 11. Woman's Profile</td> <td>\$31,000.00</td> </tr> <tr> <td>Lot # 12. Stamp of Kazakhstan</td> <td>\$29,000.00</td> </tr> <tr> <td>Lot # 13. 1929 Nepal</td> <td>\$27,000.00</td> </tr> </table> <p>Terms do not cover period of transport from or to the National Gallery.</p> <p style="text-align: right;">D'Mann President National Gallery DC</p>		Lot # 11. Woman's Profile	\$31,000.00	Lot # 12. Stamp of Kazakhstan	\$29,000.00	Lot # 13. 1929 Nepal	\$27,000.00	<p>Memorandum of Insurance Assurance:</p> <p>TO: MyStamp Collections</p> <p>In Regards to items owned or on loan to the National Gallery of Art, Washington from MyStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned lot 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 Aesom Insurance Inc. Policy #23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.</p> <table border="0"> <tr> <td>Lot # 1. Douglas MacArthur</td> <td>\$35,000.00</td> </tr> <tr> <td>Lot # 2. Neerland</td> <td>\$30,000.00</td> </tr> <tr> <td>Lot # 3. Mongolia</td> <td>\$24,000.00</td> </tr> </table> <p>Terms do not cover period of transport from or to the National Gallery.</p> <p style="text-align: right;">D'Mann President National Gallery DC</p>		Lot # 1. Douglas MacArthur	\$35,000.00	Lot # 2. Neerland	\$30,000.00	Lot # 3. Mongolia	\$24,000.00
Lot # 25. Armed Forces Reserve	\$43,000.00																						
Lot # 26. Stamp of Kazakhstan	\$29,000.00																						
Lot # 27. BradyCo.	\$12,000.00																						
Lot # 11. Woman's Profile	\$31,000.00																						
Lot # 12. Stamp of Kazakhstan	\$29,000.00																						
Lot # 13. 1929 Nepal	\$27,000.00																						
Lot # 1. Douglas MacArthur	\$35,000.00																						
Lot # 2. Neerland	\$30,000.00																						
Lot # 3. Mongolia	\$24,000.00																						

From: [redacted]
 To: throne1966@hotmail.com
 CC: coralbluetwo@hotmail.com
 King,

Long time no see... I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole officer go years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, i feel he wouldnt be too happy. It=92s very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don=92t need a search warrant. Well hit me up. You know where to find --f46d0447963147823804c47b5550



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.

Through evidence found from Tracy's Phone we can link her SMS messaging, emails, and geolocation along with timestamps that place Tracy and Carry at the time of the incident. Below

is a timeline of the incidents collected from the device, along with detailed tables regarding her SMS, emails, and geolocation.

PLOT TIMELINE

- June
 - Pat (Perry) and Tracy (Coral) are both struggling financially and want to find a way to make some quick money.
 - Tracy needs money to pay for her daughter's (Terry) private school since she doesn't want to change.
 - Pat and Tracy establish aliases, secret email addresses, and VMs to begin working on plans to make some quick money.
- July
 - Tracy finds information about a stamp exhibit coming to the museum and starts gathering information.
 - Carry reaches out to Tracy to try and meet up to catch up and possibly help Tracy out since she has been having a hard time lately.
 - Tracy (Coral) emails Pat (Perry) telling him to catch up with Coral because she got some news on a new job.
 - Pat replies back that he knows someone that can help named King.
 - Pat emails King (CC to Coral) telling him about the heist and threatens King to help or he would put King's parole in jeopardy.
 - King replies saying he will help and gives them a list of supplies he will need to help with the heist.
 - Tracy finds the insurance information on the stamps for the exhibit and emails them to her alias (Coral).

- Carry emails Tracy asking her for help getting a tablet into the museum for a flash mob event. Carry indicated she would be willing to compensate Tracy for the help
 - Tracy confirms that she will help Carry get the tablet into the exhibit in exchange for money, but wants Carry to be careful with the tablet.
- The day the flash mob is scheduled, Carry texts Tracy to meet her so Tracy can get the tablet and sneak it into the gallery.
- The day after Carry gets the

EMAIL CONTENT

Email Information				
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.com Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Mailbox Data Structure

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 communicate using the aliases and the Virtual Machine setup to keep them safer. He indicates 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: coralbluetwo@hotmail.com Subject: Re: Whats going on	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money. To Pat's suggestion that they use the Virtual Machines and aliases	Mailbox Data Structure

			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 news	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.	Mailbox Data Structure

			Pat (Perry) replies to Tracy (Coral) 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 the 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: coralblue@hotmail.com Password: legalBee	Mailbox Data Structure

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/Messages/8A3BD06F-CDB1-4453-9C69-77E06823F2AE.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 15:24:57	F: patsumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	Email Thread: cant' pass up King agrees to help with the heist 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.	/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

22.	7/11/2012 17:06:19	<p>F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com</p> <p>Subject: Re: Long time no see...</p>	<p>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.</p> <p>Tracy confirms that she will give the security shift information Carry requested in exchange for money but asks Carry to be careful with it.</p> <p>Carry replies asking Tracy not to worry and says "It will be gun".</p>	Mailbox Data Structure
23.	7/11/2012 19:28:53	<p>F: "Google+" <noreply-5dd47ca1@plus.google.com> T: tracysumtwelve@gmail.com</p> <p>Subject: Carry Carsumtwotwelve added you on Google+</p>	<p>Email Thread: Long time no see Previous email from the thread from Carry asking for the security shift details from Tracy.</p>	Mailbox Data Structure
24.	7/11/2012 23:22:03	<p>F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com</p> <p>Subject: Carry Carsumtwotwelve is sharing with you on Google+</p>	<p>Notification from Google+ informing Tracy that Carry had shared an album.</p>	Mailbox Data Structure
25.	7/12/2012 16:12:07	<p>F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com></p>	<p>Notification from Google+ informing Tracy that Carry had shared an album.</p>	Mailbox Data Structure

		T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+		
--	--	--	--	--

SMS MESSAGE CONTENT

1.	7/5/2012 18:18:23	F: Carry T: Tracy	Carry sets up the time and location as 1pm at Bubba's grill for meeting with Tracy	SMS
2.	7/5/2012 18:20:26	F: Tracy T: Carry	Tracy confirms the meeting time and location	SMS
3.	7/6/2012 16:27:16	F: Carry T: Tracy	Carry messages saying she has a table inside	SMS
4.	7/6/2012 16:27:50	F: Tracy T: Carry	Tracy replies back saying that she will be there.	SMS
5.	7/10/2012 15:26:19	F: Pat T: Tracy	Pat messages Tracy telling her about the email and informing that the attachment needs to be changed to pdf. He asks Tracy to tell this information to Coral.	SMS
6.	7/10/2012 15:58:04	F: Tracy T: Pat	Tracy acknowledges the email and message.	SMS
7.	7/10/2012 16:37:09	F: Tracy T: Pat *Failed	Tracy tried to share the following location with Pat over MMS message but it failed. Location: 2600-2700 24th Rd S, Arlington, VA 22206	SMS
8.	7/11/2012 12:41:45	F: Carry T: Tracy	Carry messages Tracy informing that she is almost there (National Gallery)	SMS
8.	7/11/2012 12:49:08	F: Tracy T: Carry	Tracy replies to Carry asking her to meet out front. She says that she will take the tablet in.	SMS

Wi-Fi/GPS LOCATION INFORMATION

Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	61306882473715E8	consolidated.db	900 N Glebe Rd, Arlington, VA 22203	
2	61306882473715E8	consolidated.db	N Glebe Rd, Arlington, VA 22203	
3	61306882473715E8	consolidated.db	801 N Wakefield St, Arlington, VA 22203	
4	61306882473715E8	consolidated.db	Bluemont, Arlington, VA 22203	

CONCLUSION

We found evidence through Tracy's phone indicating involvement in the theft of the stamps from the National Art Gallery. Some, but not all, of the evidence include EXIF data pulled from photos taken giving GPS coordinates, correspondence (email and text messages) between Tracy and other accomplices, and various phone logs at the time of the theft. The images located on the phone are the same ones stolen. Tracy (alias: "Coral") and Pat (alias: "Perry") were in need of money and thought this theft would be an easy payday. The timeline and GPS locations give authorities the information they need to bring a solid case forward.