Case Report
National Gallery DC

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

LaJuan Dover

Table of Contents

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.

Various emails and sms messages have made it evident that arrangements for Tracy Sumtwelve, Pat Sumtwelve, Carry and King to steal stamps from the National Gallery in Washington, DC.Tracy's role in this in this scheme was to provide information to Carry about the National Gallery which would aid Carry in her "flash mob" attack on the gallery with pipe bombs.

Equipment and Tools

On the Kali Linux operating system, forensic images were collected from the iPhone 3G. The image files on *tracy-phone-2012-07-15.final.E01* were analyzed on a forensic tool called Autopsy, where all the evidence of this scheme was gathered. Information from email messages using SQLite browser was later used to gather evidence on the accused. Google maps and Google Earth were used to discover the wifi and GPS locations found within the files.

Details of Tracy's iPhone

Name	Findings	Location in iPhone Image File
Model	Iphone 1,2 3G	/vol_vol5/logs/AppleSupport/general.log
Host Name	"Tracy Sumtwelve's Phone"	/vol5/logs/lockdownd.log1
OS Version	iPhone OS 4.2.1 (8C148)	/vol_vol5/logs/AppleSupport/general.log

Install Time	6/6/2012 12:03:38	/vol_vol5/logs/AppleSupport/general.log
User Email	• tracy.sumtwelve@nationalgallerydc.org • tracysumtwelve@gmail.com • coralbluetwo@hotmail.com	/vol_vol5/mobile/Library/Mail
Phone Number	1(703) 340-9661	/vol5/logs/lockdownd.log1
Serial Number	86004482Y7H	/vol_vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	/vol5/logs/lockdownd.log1
IMEI	012021003735398	/vol_vol5/root/Library/Lockdown/activation_records
MD5 Hash	b8ea5d71a9be40cd760c7b73413aedco	/vol_vol5/logs/AppleSupport/general.log
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
Personal Email:	tracysumtwelve@gmail.com
Work Email:	tracy.sumtwelve@nationalgallerydc.org
Alias Email:	coralbluetwo@hotmail.com
Relationship:	Ex-husband (Joe), Daughter (Terry)
Status:	Accused

Pat:

Phone Number: (571)-308-3236
Email: patsumtwelve@gmail.com
Relationship: Brother (Accomplice)

Terry:

Phone Number: (703)-829-6071
Email: N/A
Relationship: Daughter (Of Tracy and Joe)

Joe:

Phone Number: N/A
Email: joe.sum.twelve@gmail.com
Relationship: Ex-husband (of Tracy), Father (of Terry)

Carry:

Phone Number: (202) 725 - 2124
Email: carrysum2012@yahoo.com
Relationship: Tracy's acquaintance (Accomplice)

Tracy's phone had two associated emails that put this scheme in motion. *tracy.sumtwelve@nationalgallerydc.org* was her professional work email and *coralbluetwo@hotmail.com* is her burner email under the alias of Coral Blue. Since is employed at the NGDC as a supervisor, she was able to pass on information regarding the gallery to her accomplice and colleague, Carry. In return, Carry provided images to Tracy on a tablet. Pat and King were then brought on board to steal the stamps from the Gallery

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.

Tracy, Pat and King have come together and communicated about stealing rare, valuable stamps from the National Gallery in Washington, DC.

Tracy emailed her brother Pat about the foreign exhibit that was coming to the gallery. (*see Appendix A, Artifact 8)*

With Tracy CC'd, Pat emails King about their plan to pull of the stamp heist with the intention to recruit his assistance, (*see Appendix A, Artifact 10 and 11)*

Tracy emails her alias email copies of the insurance documents of the stamps they plan on stealing. (*see Appendix A, Artifact 12)*

King sends an email with an attached document of all the tools he will need to pull off the heist. (*see Appendix A, Artifact 15)*

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.

With the evidence that has been gathered, there is proof of Tracy communicating and plotting to assist Carry with her "flash mob" event. "Flash mob" was a cover to deface the art at the National Gallery in Washington, DC. With the sensitive data Tracy provided to Carry upon request, a plan was formed to launch the attack on the gallery.

Email and SMS messages between Tracy and Carry detail a plan for the individuals to meet at Bubba's grill (*see Appendix A, Artifact 9 and 21)*

In a thread email, Tracy and Carry discuss bringing Carry's tablet into the gallery despite security protocol. Tracy cautiously agrees to bring the tablet into the gallery for her. (*see Appendix A, Artifact 13, 14 and 32)*

Tracy messages Carry for a status update on "Flash mob". (*see Appendix A, Artifact 33)*

Carry gives Tracy further details on "Flash mob" through email with the intention of recruiting her assistance. (*see Appendix A, Artifact 16)*

Plot Timeline

Plot Timeline	
Date:	**Information:**
Tuesday, June 19, 2012	Pat sends Tracy Information on a Virtual Machine

Tuesday June 19, 2012	Pat accepts Tray's proposal
Thursday July 5, 2012	Arrangements are made between Tracy and Carry to meet at Bubba's grill
Friday July 6, 2012	Carry and Tracy meet at Bubba's grill
Friday July 6, 2012 - Tuesday July 10, 2012	Pat, Tracy and King discuss the stamp heist
Sunday July 8, 2012	Tracy takes pictures of the targeted stamps
Monday July 9, 2012	Tracy sends herself copies of memos and insurance documents for specific stamps
Wednesday July 11, 2012	Tracy meets up with Carry to take carry's tablet inside the gallery
Thursday July 12, 2012	Tracy asks about "Flash mob" and a status update.

Appendix A: Correspondence Evidence

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

Email Timeline of NGDC Heist				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Evidence Location**
1	Tuesday, June 19, 2012 20:06:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Paris Speak and answer	An email written in french that translates to Pat accepting Tracy's proposal. He asks her to email using her alias for further instructions.	Mailbox Data Structure
2	Tuesday, June 19, 2012 21:38:59	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Perry (Pat) emails Coral (Tracy) with instructions on installing a virtual machine hidden in an audio file.	Mailbox Data Structure

3	Tuesday, June 19, 2012 21:39:34	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: ???	Tracy uses her alias email to message Pat's alias email to confirm if the messages are coming through.	Mailbox Data Structure
4	Thursday, June 28, 2012	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Whats going on	Pat asks Tracy to email using her alias for future messages, as it would be "safer" to email each other with their alias emails. Pat mentions that he would like to engage in riskier, illegal business since both of them are enduring financial hardships. More ideas will be discussed between them via alias emails and virtual machines on ways to make money.	Mailbox Data Structure
5	Friday June 29, 2012 14:21:56	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	Email thread: Tracy decides that she will keep her eyes open for more opportunities. She would like Pat to try to get in on some business soon. Tracy's daughter refuses to change schools, so she is in financial constraint and needs money soon. Tracy claims that she is paying attention to insurance papers so that she could identify larger payout opportunities. Pat reassures her, but he is nervous that IA has been sniffing around.	Mailbox Data Structure
6	Friday Jun 29, 2021 14:31:36	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: hey sis	Perry (Pat) makes the mistake of emailing Tracy and referring to her as "sis". Perry asks about her personal life throughout the email and he apologizes for being busy with Coral. Coral is Tracy's alias, so it is clear that he is misdirecting any possibility of being caught by referring to Coral and a separate person.	Mailbox Data Structure
7	Tuesday July 3, 2012 13:29:37	F: joe.sum.twelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Regarding Terry	Email Thread: Tracy emails Joe about her inability to pay their daughter Terry's tuition. She later asks Joe for monetary	Mailbox Data Structure

			assistance with the tuition. Joe refuses to help.	
8	Tuesday July 3, 2012 14:53:04	F: perrypatsum@yahoo.com T :coralbluetwo@hotmail.com Subject: Re: Some good news	Email Thread: Coral (Tracy) sends Perry (Pat) information about a foreign exhibit. She said the exhibit was a ”big deal” due to it’s rare stamp collection. Within the same thread, Tracy mentions that she can scan and verify shipping information.	Mailbox Data Structure
9	Thursday July 5, 2012 15:27:51	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Long time no see...	Carry reaches out to Tracy after discovering that she is struggling financially on Facebook.com. Carry suggests getting together for lunch.	Mailbox Data Structure
10	Friday July 6, 2012 15:49:31	F: patsumtwelve@gmail.com T: throne1966@hotmail.com Cc:coralbluetwo@hotmail.com Subject: can't pass up	Pat messages King and adds Coral as a cc in regards to the heist and the gallery. Pat threatens to put King’s parole in jeopardy if he refuses the offer.	Mailbox Data Structure
11	Friday July 6, 2012 17:59:24	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Tracy suggests that all three participants (meaning King, Tracy and Pat) should meet to discuss further) Pat emails Tracy with account login information for: coralblue@hotmail.com Password: legalBee	Mailbox Data Structure
12	Tuesday July 9, 2012 14:44:11	F: tracysumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: things	Tracy emails herself (coral) documents and insurance forms regarding the stamps Documents.zip: a compressed ZIP folder containing 3 insurance documents related to stamps. Docs.zip: an encrypted ZIP folder containing 3 insurance documents related to stamps.	/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messa

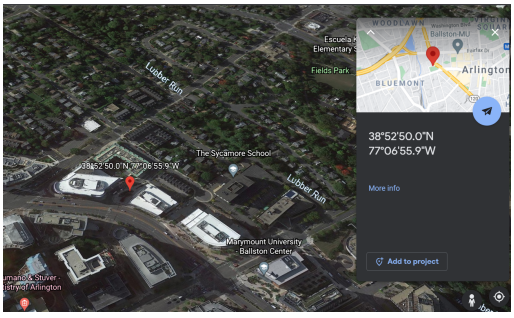
				ges/8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
13	Tuesday July 9, 2012 18:18:47	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see..	Email Thread: Carry emails Tracy in regards to getting her tablet into the gallery despite the security policy being against it. Carry wanted to take images for the “flash mob” event. This event was discussed with Tracy when they met for lunch.	Mailbox Data Structure
14	Tuesday July 10, 2012 13:48:40	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Tracy informs Carry that she can bring her tablet into the gallery	Mailbox Data Structure
15	July 10, 2012 15:24:57	F: patsumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	King agrees to help Pat and claims that he needs tools in order to help him out. King sends a document with equipment required for the job. Pat forwards this email to Tracy (Coral) *needs.txt is a pdf file which was saved with a wrong extension.	Mailbox Data Structure
16	Wednesday July 11, 2012 13:53	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Carry tells Tracy about the event that she wants to host. She tells Tracy that she will be compensated if she decides to help out. Carry asks for the security guards’ shift schedules. Tracy warns Carry to be careful but will help her with the event in exchange for money. Carry wants information regarding	Mailbox Data Structure

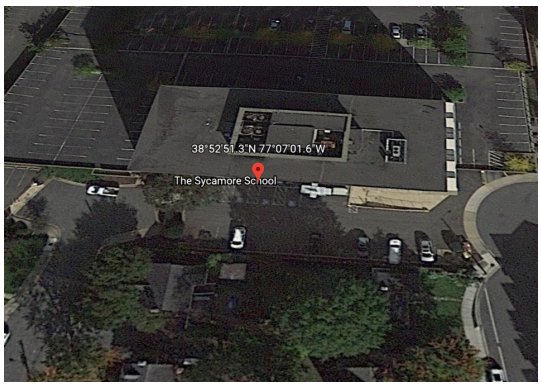
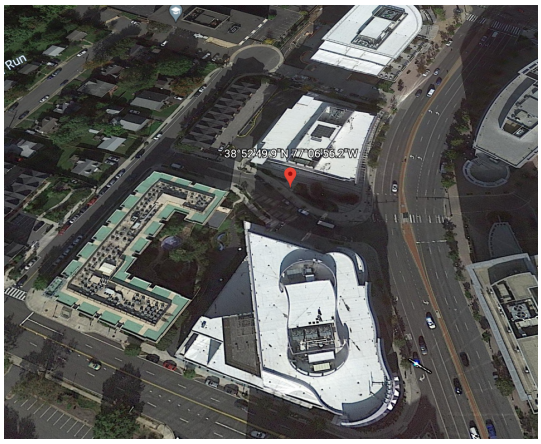
			shift changes of the security guards.	
17	Wednesday July 11, 2012	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Carry Shares images with Tracy on Google+	Mailbox Data Structure
18	Thursday July 12, 2012	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Carry Shares images with Tracy on Google+	Mailbox Data Structure

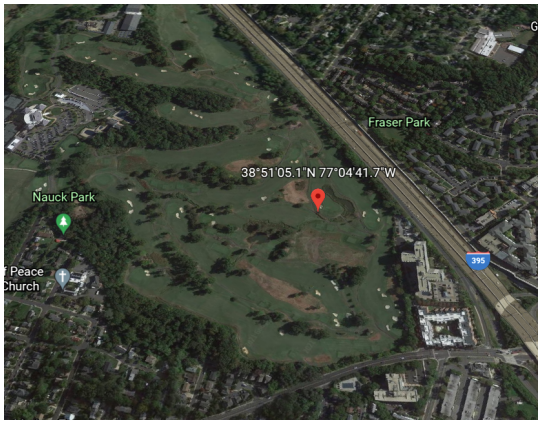
SMS Timeline of NGDC Heist			
Artifact #	**Timestamp**	**Header Information**	**Key Information**
19	Tuesday, July 3, 2012 1:41:51 PM	F:Tracy T:Terry	Tracy messages Terry about possibly switching school due to the financial burden
20	Tuesday, July 3, 2012 2:04:32 PM	F:Terry T:Tracy	Terry does not want to switch schools. She also mentions that she wants to stay with her father in order to attend Prufrock
21	Thursday, July 5, 2012 6:18:23 PM	F:Carry T:Tracy	Carry arranges to meet Tracy at Bubba's grill 1pm
22	Thursday, July 5, 2012 6:20:26 PM	F:Tracy T:Carry	Tracy confirms the meeting's time and location
23	Friday, July 6, 2012 3:02:19 PM	F:Tracy T:Pat	Tracy asks Part to call her
24	Friday, July 6, 2012 3:08:37 PM	F:Pat T:Tracy	Pat claims to be to busy, but he will call her later
25	Friday, July 6, 2012 3:11:54 PM	F:Tracy T:Pat	Tracy insists that calling her is important and wants Pat to call her as soon as possible

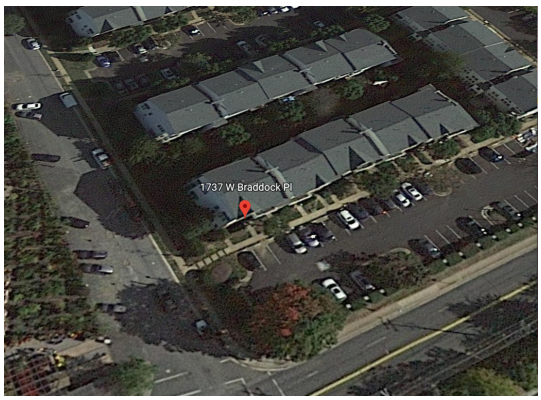
26	Friday, July 6, 2012 3:13:31 PM	F:Pat T:Tracy	Pat says he will call her in 5 minutes.
27	Friday, July 6, 2012 4:27:16 PM	F:Carry T:Tracy	Carry informs Tracy that she is inside Bubba's grill and that she has a table inside the restaurant
28	Tuesday, July 10, 2012 3:26:19 PM	F:Pat T:Tracy	Pat tells Tracy about an email that needs to be changed to PDF and asks her to pass it on to Coral
29	Tuesday, July 10, 2012 3:58:04 PM	F:Tracy T:Pat	Tracy acknowledged the email and the text message
30	Tuesday, July 10, 2012 4:37:09 PM	F:Tracy T:Pat	Tracy tried to send a location to Pat over MMS message, but it failed to send. Location: 2600-2700 24th Rd S, Arlington VA 2206
31	Wednesday, July 11, 2012 12:41:45 PM	F:Carry T:Tracy	Carry informs Tracy that she is almost there (The Gallery)
32	Wednesday, July 11, 2012 12:49:08 PM	F:Tracy T:Carry	Tracy tells Carry to meet her in the front of the building and she will take the tablet inside.
33	Thursday, July 12, 2012 5:06:45 PM	F:Tracy T:Carry	Tracy asks Carry about "Flash mob"

Appendix B: WiFi and GPS Location Information

GPS Evidence of NGDC Heist				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Map Screenshot**
1	Wednesday, June 13, 2012 7:01:22 PM	Cell Location: 38°52'50.0"N 77°06'55.9"W	Virginia Tech Research Centre: 900 N Glebe Rd, Arlington, VA 22203, USA	

2	Monday, July 2, 2012 4:19:23 PM	Cell Location: 38°52'51.3"N 77°07'01.6"W	4600 Fairfax Dr, Arlington, VA 22203, USA	
3	Tuesday, July 3, 2012 1:42:38 PM	Wifi Location: 38°52'50.3"N 77°06'56.1"W	900 N Glebe Rd, Arlington, VA 22203, USA	
4	Thursday, July 5, 2012 4:32:46 PM	Cell Location: 38°52'47.4"N 77°06'51.9"W	4450 Wilson Blvd, Arlington, VA 22203, USA	

5	Sunday July 8, 2012 12:33:36 PM	Cell Location: 38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408, USA	
6	Tuesday, July 10, 2012 4:31:10 PM	Cell Location: 38°51'05.1"N 77°04'41.7"W	1700 Army Navy Dr, Arlington, VA 22202, USA	
7	Tuesday, July 10, 2012 4:31:12 PM	Wifi Location: 38°50'54.0"N 77°04'55.9"W	2693 24th Rd S, Arlington, VA 22206, USA	

8	Tuesday July 10, 2012 4:45:00 PM	Cell Location: 38°49'37.4"N 77°05'10.0"W	1737 W Braddock Pl, Alexandria, VA 22302, USA	
9	Tuesday July 10, 2012 4:45:01 PM	Wifi Location: 38°49'39.5"N 77°05'17.0"W	4104 36th St S, Arlington, VA 22206, USA	

Conclusion

Evidence found on Tracy's iPhone indicated the following:

After a thorough investigation, It can be concluded that Tracy, Pat and King conspired to steal valuable stamps from the National Gallery of Washington, DC. Simultaneously, Tracy partnered with Carry by providing her with sensitive data so that the act of defacing priceless art under the ruse of "Flash mob" could take place.

Stealing Stamps

Through email correspondence, it was discovered that the siblings, Tracy and Pat used alias names and email addresses. Tracy adopted the name "Coral" while Pat took the name "Perry". Out of financial desperation, the two individuals brain-stormed multiple opportunities to make money illegally. It was then that the pair communicated through virtual machines and alias emails before recruiting King onto their team. With King

being experienced in illegal activity, he provided a list of tools that were needed to complete the heist while Tracy gathered images and insurance documents of the stamps they were planning to steal.

Flash Mob

Tracy's financial struggles were made apparent on the social media platform Facebool.com. It was from there that Carry decided to reconnect with Tracy, sensing her desperation. The two met for lunch and later corresponded through SMS and email messages about "Flash mob". Since Carry was offering to compensate Tracy for her co-operation in the attack, Tracy provided Carry with private company data such as security guard shift times and images of art.