Case Report

National Gallery DC

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

Table of Contents

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 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:

From the gathered evidence, the information collected shows the connection between Tracy, Pat, and King, the accomplices in a scheme to steal stamps. Also, that Tracy provided information about NGDC to Carry to assist with the "flash-mod" that ended up being a scheme to vandalize artwork.

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone1,2 3G	tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Host Name	tracyphone	tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log

Install Time	6/6/2012 12:03:28	tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0431720.plist, or in the Envelope Index
Phone Number	1 (703) 340-9661	tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
IMEI	004999010640000	tracy-phone-2012-07-15-final.E01/vol_vol5/wireless/Library/logs/lockdown.log.1
MD5 Hash	34c4888f095dc3241330462923f6fea5	/corpus folder
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	/corpus folder

Evidence to establish Personas

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

Tracy: Alias (Coral Blue)

Phone Number:	(703) 340-9961
Email:	tracysumtwelve@gmail.com /coralbluetwo@hotmail.com
Work email:	tracy.sumtwelve@nationalgallerydc.org
Relationship:	Brother: Pat(Perry) Ex-husband: Joe Daughter: Terry
Status:	Accused

Pat: Alias (Perry)

Phone Number: 1 (571) 308-3236

Email: perrypatsum@yahoo.com

Relationship: Brother of Tracy

Terry:

Phone Number: 1 (703) 829-6071

Email: N/A

Relationship: Daughter of Tracy/Joe and the niece of Pat

Joe:

Phone Number: N/A

Email: joe.sum.twelve@gmail.com

Relationship: Tracy's ex husband, father of Terry

Carry:

Phone Number: +1 (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Acquaintance of Tracy

King:

Phone Number: N/A

Email: throne1966@hotmail.com

Relationship: ex-con that Pat tries to enroll into the heist

Provide a brief summary of your conclusions here.>

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 hears of a stamp collection that's valuable that will be coming through the museum.

Tracy emails her brother Pat and both of them show interest in stealing it because it's all together a small object that would be easy to get their hands on.

Pat ropes an ex-con with the Alias “King” into helping with the heist by blackmailing him. King agrees and sends Pat a list of what they would need for the job.

Pat forwards this list to Tracy

Tracy emails insurance documents for the stamp collection to Pat. All this dialogue between them in email/sms makes it pretty clear of their intent to steal the collection.

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.

<Provide a brief summary of your conclusions here.>

Carry reached out to Tracy meeting over lunch.

In an email Carry asked Tracy to get a tablet into the National Gallery for a flash mob event she wanted to plan; while mentioning that she would compensate her.

Tracy agreed to sneak in the tablet and a hand off time was set for 9 for the handoff.

Carry had also asked for information on shift change for security; and Tracy had agreed to provide that information as well.

Tracy started receiving notifications on Google+ related to Carry, for instance her getting added to her circle and sharing something with her.

Tracy had followed up with Carry to ask about the flash mob.

Plot Timeline

Phone calls: found at /wireless/Library/CallHistory/call_history.db

Txt Messages: /mobile.Library/SMS/sms.db

GPS location information: /root/Library/Caches/locationd/consolidated.db

Email Content

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	F: perrypatsum@yahoo.com	Pat (Perry) emails Tracy to ask her to	Mailbox Data

	20:26:47	T: tracysumtwelve@gmail.com Subject: Look me up sometime	communicate using her alias.	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 a 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: coralbluetwo@hotmail.com	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money.	Mailbox Data Structure

		Subject: Re: Whats going on	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	Mailbox Data Structure

			feels that it would be a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	
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. 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.	Mailbox Data Structure
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	Mailbox Data Structure

			that Tracy was having a hard time recently.	
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: 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-

				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 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	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.	Mailbox Data Structure

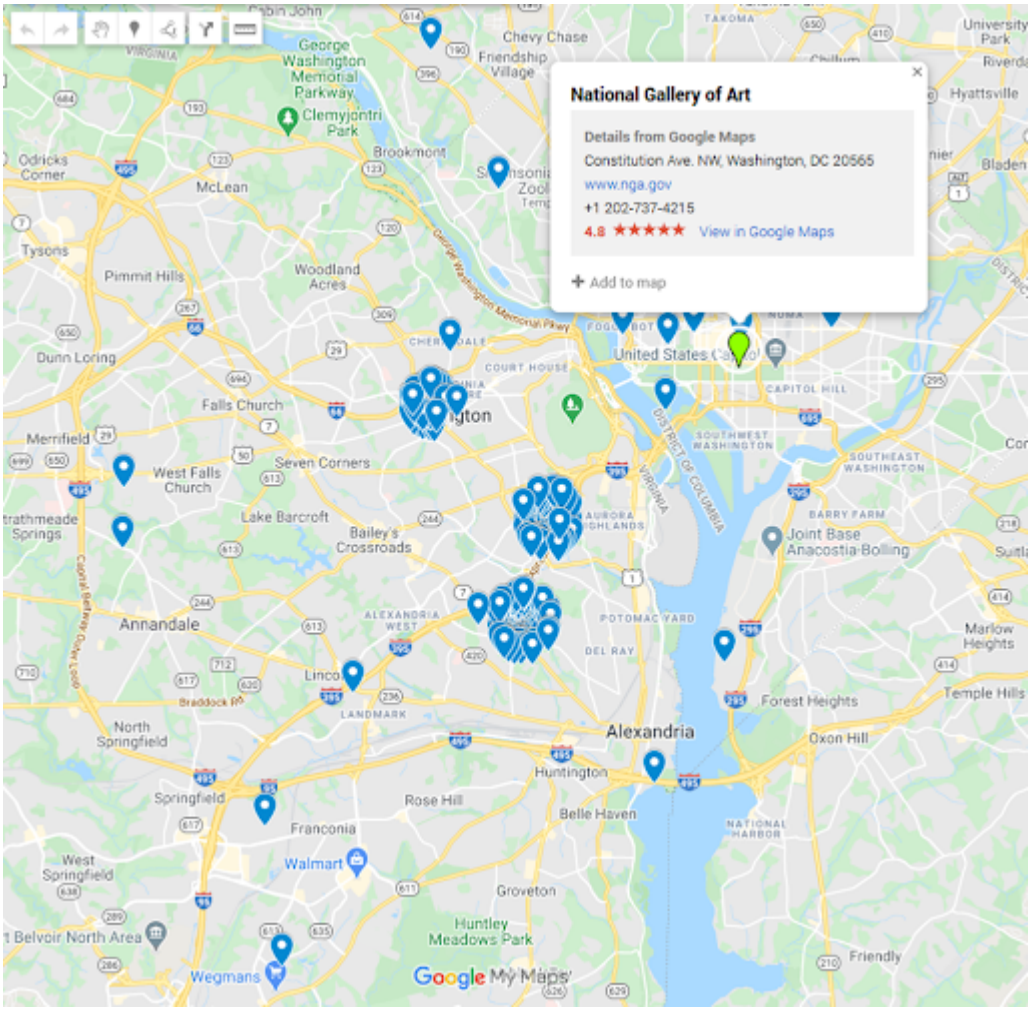
			Tracy confirms that she will give the security shift information Carry requested in exchange for money but asks Carry to be careful with it. Carry replies asking Tracy not to worry and says “It will be gun”.	
23.	7/11/2012 19:28:53	F: "Google+" <noreply-5dd47ca1@plus.google.com> T: tracysumtwelve@gmail.com 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: carrysum2012@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

SMS Message Content

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
27.	6/12/2012 21:25:04	F: Pat T: Tracy	Pat asks Tracy about her plans for the weekend	SMS
28.	6/13/2012 17:30:28	F: Terry T: Tracy	I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. T	SMS
29.	6/13/2012 18:30:38	F: Tracy T: Pat	Tracy replies to Pats message saying that she has no big plans and enquires about his plans.	SMS
30.	6/13/2012 18:33:46	F: Tracy T: Terry	Ok, sounds good.	SMS
31.	7/3/2012 14:04:32	F: Terry T: Tracy	Terry replies back saying that she doesn't want to switch schools and would rather stay with her dad and continue at Prufrock	SMS
32.	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
33.	7/5/2012 18:20:26	F: Tracy T: Carry	Tracy confirms the meeting time and location	SMS
34.	7/6/2012 15:02:19	F: Tracy T: Pat	Tracy asks Pat to give her a call	SMS
35.	7/6/2012 15:08:37	F: Pat T: Tracy	Pat says he is busy and suggests calling later	SMS
36.	7/6/2012 15:11:54	F: Tracy T: Pat	Tracy says its important and insists that pat call her soon	SMS
37.	7/6/2012	F: Pat T: Tracy	Pat says he will call in 5 min	SMS

	15:13:31			
38.	7/6/2012 15:18:50	F: Pat T: Tracy	Pat calls Tracy and they speak for 4 min 4 secs.	SMS
39.	7/6/2012 16:27:16	F: Carry T: Tracy	Carry messages saying she has a table inside	SMS
40.	7/6/2012 16:27:50	F: Tracy T: Carry	Tracy replies back saying that she will be there.	SMS
41.	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
42.	7/10/2012 15:58:04	F: Tracy T: Pat	Tracy acknowledges the email and message.	SMS
43.	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

Wi-Fi/GPS location information



Conclusion

Evidence was found and compiled from using Tracy's iPhone and systems/programs such as: Kali Linux, autopsy, sqlite

- Tracy used the alias Coral and Pat used the alias Perry.
- Tracy knew that King was being involved for the stamp job
- Tracy had emailed letters about the stamps to her own email and to Pat's

- Tracy had made the plan involving Pat to steal the stamps
- Her main motive was for financial gain
- Financial gain was also why she was helping Carry
- Though she did not know the real plan that Carry had formulated
- Tracy had smuggled a tablet into the Gallery for Carry
- She had also supplied her with information about the security shift changes