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 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:

Evidence was found linking Tracy, also known as "Coral," and her brother Pat, also known as "Perry," to a plot to steal valuable stamps from the National Gallery DC. The evidence includes email correspondence between the siblings containing sensitive information and images of the stamps. Pat also tried to involve a third party named King in the heist. Tracy played a part in facilitating the theft by helping someone named Carry smuggle a tablet into the Gallery and providing them with security shift schedule details.

Details of Tracy's iPhone

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone3G	vol_vol4/Applications/Camera.app/Camera
Host Name	Tracy Sumtwelve's iPhone	lockdownd.log.1
OS Version	Iphone OS 4.2.1 (8C148)	general.log
Install Time	6/6/2012 12:03:28 -0700	general.log
User Email	tracysumtwelve@gmail.com coralbluetwo@hotmail.com	Envelope Index
Phone Number	1 (703) 340-9661	lockdownd.log.1
Serial Number	860044B2Y7H	general.log
ICCID	89014103255195342366	lockdownd.log
IMEI	012021003735398	wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Junior Investigator
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d657 7ccb534ca0d1e83ffd27683e621607	Junior Investigator

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
Relationship: Accused

Pat:

Phone Number: 15713083236
Email: patsumtwelve@gmail.com
Relationship: Brother of the accused

Terry:

Phone Number: (703) 829-6071
Email: Unknown
Relationship: Daughter of the accused and Joe

Joe:

Phone Number: [unknown]
Email: [unknown]
Relationship: Terry's father, currently divorcing the accused

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Acquaintance of Terry

King:

Phone Number:

Email: throne1966@hotmail.com

Relationship: Blackmailed by Pat over his drug abuse into helping them steal the stamps

The information gathered pertains to Tracy's device and reveals that her Apple ID is linked to the email address 'tracysumtwelve@gmail.com'. Additionally, her work email, 'tracy.sumtwelve@nationalgallerydc.org', is configured on the phone, as well as another email address using the pseudonym Coral Blue. Tracy is a supervisor at the NGDC and is involved in a conspiracy with her brother, Pat (Perry), and his partner, King (Kart), to pilfer stamps from the organization. She is also receiving assistance from her co-worker Carry (Cat) at NGDC to obtain images on a tablet.

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 discovered a stamp collection exhibit of considerable value and contacted Pat to inform him of the discovery. Both parties demonstrated a significant interest in the exhibit due to its high value and small size. Pat endeavored to include an individual named King, who had a criminal record and was on parole, in the heist. King agreed to join the conspiracy and provided a list of requirements. Pat shared the list with Tracy and confidential insurance documents related to the stamp exhibit. Tracy, who possessed multiple photographs of the stamps mentioned in the insurance documents on her iPhone, responded to Pat's SMS acknowledging receipt of the attachment. These actions collectively implied Pat and Tracy's mutual intention to engage in a conspiracy to steal the valuable stamps.

There’s also evidence for malign activity, a list of equipment to be supplied and used:

-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)

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.

During a luncheon meeting, Carry requested Tracy's assistance in surreptitiously introducing a tablet into the National Gallery for a planned flash mob event, offering compensation in exchange. Tracy agreed, additionally providing confidential security shift information for further remuneration. Subsequent online interactions, including Carry suggesting connection with another individual, indicate a potentially closer association. However, it remains unclear whether Tracy was fully cognizant of the potential ulterior motives behind the "flash mob," raising questions about her level of complicity or potential exploitation for personal gain.

Plot Timeline

Timestamp	Event
19 Jun 2012 14:38:59	Pat, as Perry, sends Tracy, as Coral, obfuscated information on how to install VirtualBox.
5 Jul 2012 18:18:23	Carry texts Tracy to meet at Bubba's grill.
5 Jul 2012 18:20:26	Tracy confirms meeting.
6 Jul 2012	Carry and Tracy meet at Bubba's grill
9 Jul 2012 10:44:11	Tracy forwards documents containing insured value of stamps to her alias account, coralblue.
9 Jul 2012 18:18	Carry offers Tracy compensation in exchange for sneaking a tablet into a flashmob event they had previously discussed.
10 Jul 2012 11:19	King confirms involvement in heist and sends Pat a list of equipment needed for the job, Pat passes this information on to Tracy.
11 Jul 2012 14:53	Tracy provides guard rotations to Carry in exchange for cash.
11 Jul 2012 22:49:08	Tracy texts Carry with the instruction to meet her out front.

Email Content

Master Timeline of NGDC				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Evidence Location**
1	19 Jun 2012 14:38:59	F: Perry perrypatsum@yahoo.com" T: Coral coralbluetwo@hotmail.com Subject: Crazydave by the VM's Attach: Crazydave1.mp3	Hey Coral, Just got your email. That took longer than expected! Oh well! You've got to check out this new song by the VMs. I love the base. Tell me what you think! Note: THe mp3 file explains how to install a VirtualBox	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
2	19 Jun 2012 20:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com	Tracy receives an email from Pat informing her that he has agreed to her proposal. He requests her to use her alias to send him further instructions via email.	Mailbox data structure
3	19 Jun 2012 21:38	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com	Pat sends an email to Tracy with an audio file, providing her with guidelines to set up a Virtual Machine.	Mailbox data structure
4	21 Jun 2012, 17:43	F: patsumtwelve@gmail.com	Pat, responds to Tracy in an email conversation regarding the	Mailbox data structure

		T: tracysumtwelve@gmail.com	installation of a Virtual Machine. Pat suggests that Tracy should consider listening to some crazy song na Crazydave1. Tracy confirms in the email thread that the previously sent instructions in the audio file were helpful to her.	
5	29 Jun 2012, 14:21	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com	Pat and Tracy are having a conversation via email. They are discussing different ideas on how to make money. Pat suggests that they utilize Virtual Machines and aliases to stay connected and continue searching for opportunities to earn money.	Mailbox data structure
6	2 July 2012, 12:05	F: coralbluetwo@hotmail.com T: perrypatsum@yahoo.com	Carry tells Perry that there's a foreign exhibit before the official announcement, that it might be useful for their plans.	Protected Index
7	06 Jul 2012, 15:27	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com	Tracy sent an email to Pat informing that she had a conversation with Coral. According to Tracy, Coral received some fantastic news about her work. Tracy recommended that Pat should reconnect with Coral.	Mailbox data structure
8	06 Jul 2012, 17:59	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com	Tracy proposes that they should spend some time together in the near future. (meaning King, Tracy and Pat)	Mailbox data structure

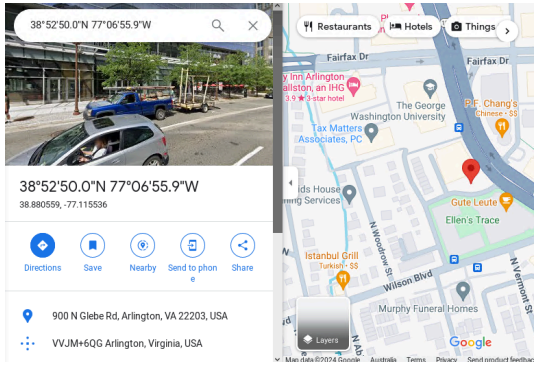
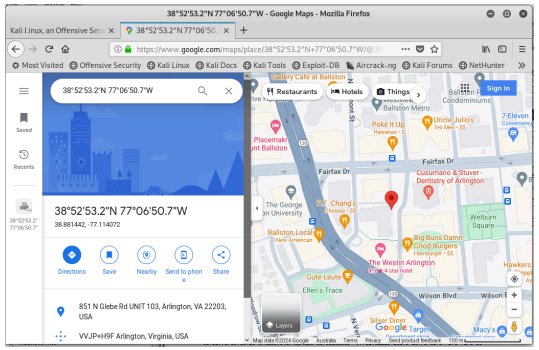
9	09 Jul 2012, 18:18	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com	Carry reached out to Tracy via email, requesting her assistance in sneaking a tablet into a flash mob event they previously discussed. Carry proposed that Tracy would be compensated for her help in some manner.	Mailbox data structure
10	9 Jul 2012 10:44:11	F: Tracysumtwelve@gmail.com T: coralbluetwo@gmail.com	Large base64 encoded attached with message 'somethings'	Mailbox data structure
11	9 Jul 2012 10:44:11	F: Tracysumtwelve@gmail.com T: coralbluetwo@gmail.com	'docs.zip' attachment contains three pdfs outlining the insured value of nine stamps owned by the museum Stamp insurance 1.pdf, Stamp insurance 2.pdf, Stamp insurance 3.pdf	Mailbox data structure
12	10 Jul 2012 11:19AM	F: throne1966@hotmail.com T: patsumtwelve@gmail.com Subject: RE: Can't pass this up Attach: needs.txt Forwarded F: patsumtwelve@gmail.com T: coralbluetwo@gmail.com	Email from contained an attachment with a list of items needed for the theft. Attachment includes: needs.txt -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)	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

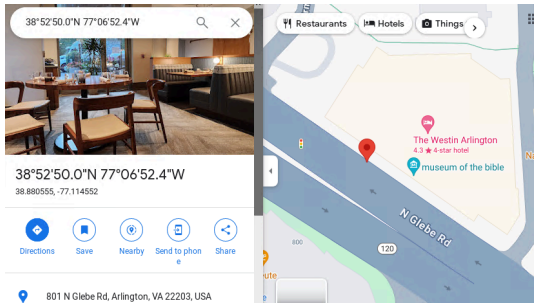
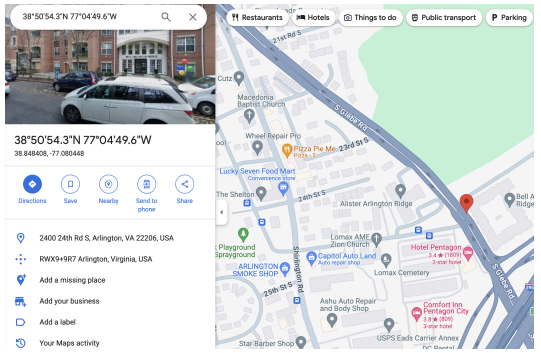
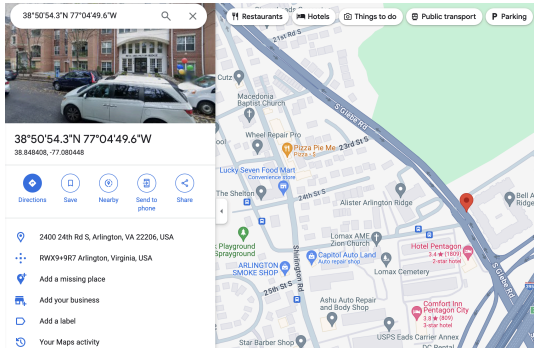
13	10 Jul 2012 08:24:58	F: Patsumtwelve@gmail.com T: coralbluetwo@hotmail.com	Discusses the crime planning, tools needed for the job, forwarded message from King about how he is on drugs and Pat is blackmailing him	Mailbox data structure
14	11 Jul 2012 14:53	F: Tracysumtwelve@gmail.com T: Carrysum2012@yahoo.com	Tracey gives Carry information on guard rotations and security in exchange for cash	Protected Index
15	12 Jul 2012 14:52:41	F: Coral <coralbluewo@hotmail.com> T: Awen.Throsam@m57.biz	Talk about a foreign exhibit that is coming over. Money is rough. Internal Affairs is sniffing around.	

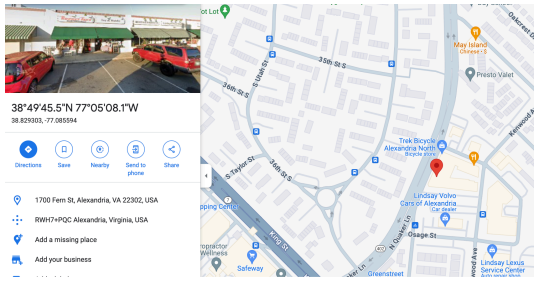
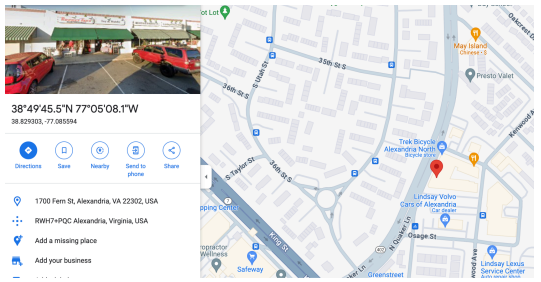
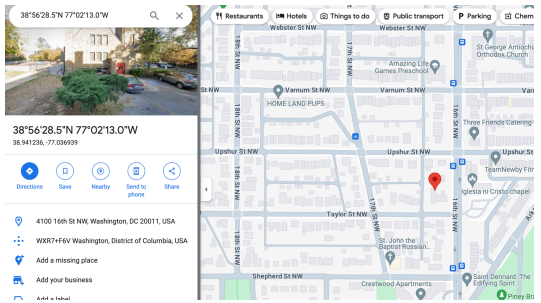
SMS Message Content

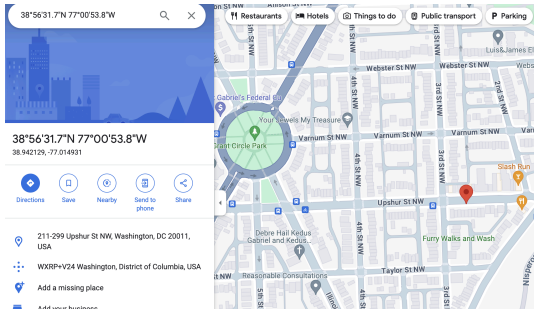
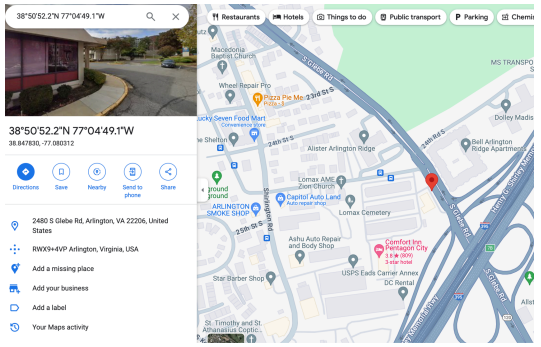
1	6 Jul 2012 16:27	F/T: Carry T/F: Tracy	Carry and Tracy exchange messages confirming meeting at Bubba's grill	sms.db
2	10 Jul 2012 08:26:19	F: 15713083236 (Pat) T: 1 (703) 340-9661 (Tracy)	Text message informing tracy that her 'friend' coral received an email with an attachment that needs to be changed to a pdf [Article 9].	sms.db
3	10 Jul 2012 15:26	F:15713083236 (Pat) T: (703) 340-9661 (Tracy)	Pat told Tracy to convert the email attachment to PDF and inform Coral about it.	sms.db
4	11 Jul 2012 22:49:08	F: 1 (703) 340-9661 (Tracy) T: (202) 725-2124 Carry	Tracy sends text message instructing recipient to meet her out the front.	sms.db
5	12 Jul 2012 05:06 PM	F: (703) 340-9661 (Tracy) T: (202) 725-2124 Carry	Tracy messages Carry asking her about the flash mob.	sms.db

Wi-Fi/GPS Location Information

Location Information				
Artifact #	**Timestamp**	**Header Information**	**Body**	**Map Screenshot**
	June 13, 2012 15:01:22	**Wifi Location**	**Location: 900 N Glebe Rd, Arlington, VA**	
		851 N Glebe Rd Arlington Virginia, USA		

	July 10, 2012 12:46:29	**Wifi Location**	**Location: 801 N Glebe Rd, Arlington, VA**	
4	**Jul, 10 2012 16:31**	**Wifi Location**	**2400 24th Rd S, Arlington, VA 22206, USA**	
5	**Jul, 10 2012 16:31**	**Cell Location**	**2400 24th Rd S, Arlington, VA 22206, USA**	

6	Jul, 10 2012 16:45	Wifi Location	1700 Fern St, Alexandria, VA 22302, USA	
7	Jul, 10 2012 16:45	Cell Location	1700 Fern St, Alexandria, VA 22302, USA	
8	Jul, 5 2012 09:31 PM	Cell Location	4100 16th St NW, Washington, DC 20011, USA	

9	**Jul, 5 2012 04:42 PM**	**Cell Location**	**211-299 Upshur St NW, Washington, DC 20011, USA**	
10	**Jul, 10 2012 09:21 PM**	**Wifi Location**	**2480 S Glebe Rd, Arlington, VA 22206, United States**	

Conclusion

Evidence found on Tracy’s iPhone indicated the following:

- Tracy used the alias "Coral," while Pat used the alias "Perry."
- Their use of aliases, VPNs, hidden messages in MP3s implies they knew they were doing something wrong
- Tracy's main motivation was financial gain for orchestrating the stamp heist.
- Tracy sent National Gallery DC stamp letters to her personal email and to Pat.
- Tracy and Pat collaborated on a plan to steal stamps.
- Tracy was aware that Pat was attempting to pressure someone named King into aiding in the heist.
- Tracy assisted Carry, also for financial gain.
- Tracy disclosed sensitive security rotation details about the National Gallery to Carry.
- Tracy aided Carry in smuggling a tablet into the Gallery.
- Tracy was unaware of Carry's larger scheme.