Cybersecurity

21.3 The Final Report

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 the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and the defacing of museums 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 aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

After the tip from Tracy's husband, Joe, her phone was seized and an image extracted. The team was provided the image for forensic analysis. The following narrative is supported by the evidence found. Tracy(Coral), who works at the National Gallery, was having money troubles connected to the divorce from Joe. One of these issues was related to her daughter's school tuition which Tracy could not afford. Her daughter, Terry, advised her mom that Joe would pay for school if she was living with him. To avoid that outcome, Tracy contacted her brother Pat(Perry) about organizing the theft after seeing the valuations of the stamps from the insurance documents. When the insurance documents came to Terry's attention, she passed the information on to her brother Pat, a Nat City Police Officer, who, in turn, reached out to King and threatened to put him back in prison if he did not cooperate in organizing the heist. King provided a list of needed materials confirming that he would take part in the heist.

Equipment and Tools

The team used Autopsy, SQLite, and other various tools preinstalled on this version of Kali Linux.

Details of Tracy's iPhone

Name	Findings	Location in Iphone Files
Model	Iphone 1 or 2	tracy-phone-2012-07-15-

Name		final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Host	Tracy Sumtwelves Iphone	tracy-phone-2012-07-15-
OS version	Iphone OS 4.2.1	tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Install time	06/06/2012 19:03:28	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/mobile/Library/Mail/IMAP-tracysumtwelve@gmail.com@imap.gmail.com
Phone Number	+1 (703)-340-9661	./vol_vol5/logs/lockdown.log1
ICCID	89014103255195342366	./vol_vol5/logs/lockdown.log1
IMEI	012021003735398	./vol_vol5/root/library/lockdown/activation_records/wildcard_record.plst
MD5Hash	34c4888f095dc3241330462923f6fea5	
SHA256Hash	71aed05a86a753dec4ef4033ed7f52d6 577ccb534ca0d1e83ffd27683e621607	

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: patsumtwelve@gmail.com
Relationship: Tracy's Brother

Terry:

Phone Number: (703) 829-6071
Email: Unknown
Relationship: Tracy's Daughter

Joe:

Phone Number: Unknown
Email: Unknown
Relationship: Tracy's Ex-Husband

Carry:

Phone Number: (202) 725-2124
Email: carrysum2012@yahoo.com
Relationship: Friend of Tracy

In conclusion, Tracy, Pat, and King conspired to steal valuable stamps from the National Archive. Tracy's motivation was to pay her daughter's tuition so that her daughter would continue to live with her. Pat's motivation was to help his sister. King's motivation was to stay out of prison.

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 came upon the important stamp collection display as appeared in ‘Mailbox Information Structure’. Tracy (Coral) emails Pat (Perry) saying that an interesting foreign exhibit is going to happen and that from assessing the paperwork, she feels that it would be a big deal. Moreover, appears Tracy and Pat are curious about stealing it since it’s small and valuable. Pat tries to get a guy to join in on the heist (King) who has a criminal history and is out on parole. He does this by intimidating him and blackmailing him. King agrees to do the heist and sends out a list of necessities. Pat at that point sends the list to Tracy with instructions on how to access the attachment over SMS. Tracy then emailed the insurance documents of the stamp collection which were marked as confidential to Pat. Tracy’s iPhone has numerous photos of the stamps, which were mentioned in the insurance documents. All these pieces of evidence make it clear that Pat and Tracy were conspiring to steal valuable stamps. 6 images from Tracy’s phone show pictures of the Gallery Stamps that were taken before the heist. The Geo-Location of these images shows they were taken at the Museum, which proves that Tracy took these photos while being there.

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.

Carry reached out to Tracy and asked to meet for lunch, and they did. In the same email, Carry asks Tracy for assistance to sneak a tablet into the National Gallery for a flash mob event that she was planning, in which she offers her compensation. Tracy agrees to sneak in the tablet in exchange for money and they plan to meet at 9. Also, Carry asked for information regarding the security guard's shift change in exchange for money. Tracy also agrees to give information regarding the security shift changes. Tracy then receives notifications from Google+ informing her that Carry added her to a circle and that she shared something with her on Google+. In one of the notifications from Google+ was a suggestion to add Alex who was a part of Carry’s circle. Tracy then messaged her asking how the flash mob was going. This message, along with all their communication before suggests that even though Tracy gave up valuable information and snuck the tablet in, she was not aware of anything more in the plan.

Plot Timeline

- Email Content: /mobile/Library/Mail/Protected Indexed
- SMS Content: /mobile/Library/SMS/sms.db
- Call Data: /wireless/Library/CallHistory/call_history.db

- Wifi & Cell Location Data: /root/Library/Caches/locationd/consolidated.db

PLOT TIMELINE	
Tuesday, June 19, 2012	Pat sends information about a VM
Thursday, July 5, 2012	Text messages between Tracy and Carry talking about meeting up for lunch
Friday, July 6, 2012	Tracy meets up with Carry for lunch
Friday, July 6, 2012 - Tuesday, July 10, 2012	Communication between Tracy, Pat, and King about the necessities needed for the stamp heist
Sunday, July 08, 2012	Tracy takes photos of the stamps (6) that they are thinking about stealing
Monday, July 09, 2012	Tracy sends herself copies of documents regarding insurance for specific stamps
Wednesday, July 11, 2012	Tracy meets up with Carry again to take Carry's tablet in with her
Thursday, July 12, 2012	Tracy asks Carry about the status of the flash mob

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy used the alias Coral and Pat used the alias Perry
- Tracy's main motivation to give information on the security guard's shifts and sneak in the tablet was financial gain
- Tracy emailed stamp letters to her personal email account and to Pat
- Tracy knew that Pat was trying to talk a guy (King) into helping with the heist.
- Tracy leaked sensitive information over to Carry (Security Guards Shift Changes)
- Tracy helped Carry sneak a tablet into the National Gallery
- Tracy was unaware of the bigger plan

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 emailed Tracy to let her know he had accepted her proposal and asked 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 VM 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 he is 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 VM installation saying that she should also listen to other songs. Also, Tracy confirmed in the email thread that the instructions sent earlier in the audio file helped her.	Mailbox Data Structure

6.	6/28/2012 19:31:33	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: What's going on	Pat (Perry) emailed Tracy (Coral) asking her to communicate using the aliases and the VM setup to keep them safer from here on out. He mentioned that because of their financial situation, they might have to "push the envelope" a bit. He then says he has some friends that he works with who are good at these type of things and wants to discuss more ideas over email.	Mailbox Data Structure
7.	6/29/2012 14:21:56	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: What's going on	This email between Pat (Perry) and Tracy (Coral) is where they discussed ideas for making money. Pat said to use the "new setup" (VM) to communicate. Coral says they need to try to get in on something if something comes up around the office. She mentions her "kiddo" is getting really bent out of shape about possibly having to switch schools, and that she is paying more attention to the papers that come across her desk, particularly insurance documents since they get a bunch of them. She then states she will keep a look out for anything that stands out and let pat know.	Mailbox Data Structure
8.	6/29/2012 14:31:36	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: hey sis	Pat (Perry) emails Tracy calling her "sis" and ask if Terry sorted out the problems she was having in her literature class. She says she has been busy sorting things out with her friend Coral and says they should all go out for dinner sometime.	Mailbox Data Structure
9.	6/29/2012 15:21:35	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	Pat replies to the email thread regarding Coral's concern about people sniffling around and says to not worry, and that if something like they talked about pops up, they will definitely pull something off.	Mailbox Data Structure
10.	7/2/2012 16:13:18	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com	Tracy (Coral) emails Pat (Perry) mentioning everybody at the office	Mailbox Data Structure

		Subject: Re: Some good news	seems to be buzzed about a foreign exhibit that is supposed to be coming over. Tracy says there hasn't been any official release in writing but that they have been going through quite an ordeal with all the paperwork and says the exhibit seems to be a bid deal and will let her know if anything else is found.	
11.	7/2/2012 20:00:31	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Pat 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	Tracy emails 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	Coral emails Perry saying that the exhibit is rare and a highly valuable stamp collection and this may be their opportunity. Perry replies to Coral asking her to collect as much information as possible abou 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 reached out to Tracy asking her if they could meet up for lunch asking if Friday would work. She also mentions that she realized Tracy was having a hard time recently by Facebook.	Mailbox Data Structure
15.	7/6/2012 15:27:51	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com	Tracy emailed Pat saying she spoke with Coral and that Coral got some great news about her job and	Mailbox Data Structure

		Subject: Re: Good News	suggested that Pat Catch up with Coral. Pat replied back saying he knows a guy called named King.	
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 the guy (King) and cc Tracy (Coral) in it saying that he has a lucrative proposition, a heist at a 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	Tracy suggests that King, Tracy, and Pat should hang out sometimes. Pat emails Tracy with the 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.emix
19.	7/9/2012 18:18:47	F:carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see	Carry emailed Tracy asking for help to sneak 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	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 then replies and says that this would be a big help and asks	Mailbox Data Structure

		Subject: Re: Long time no see	if she could come around 9.	
21.	7/10/2012 15:24:57	F: patsumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	King agrees to help out with the heist and sends in a document with equipment required for it. The attached document is saved as a 'txt' file. Pat then forwards that email to Tracy (Coral) *needs.txt is a pdf file which was saved with the wrong extension.	/mobile/Library/Mail/POP-coralbluetwo Corres… @pop3.live.com/INBOX.mbox/Messages/9F0508D8-04FB-490E-A7F0-3E23B0E7C59B.emix
22.	7/11/2012 17:06:19	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see	Tracy confirms that meeting at 9 is ok for tomorrow. Carry wants Tracy to pass her information regarding shift changes of the security. She suggests that Tracy would be well paid for giving the information. Tracy confirms that she will give up the information regarding the Shift information that Carry asked for in exchange for money. Carry tells Tracy not to worry and says it will be fine.	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+	The 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	Notification from Google+ informing Tracy that Carry had shared an album.	Mailbox Data Structure

		Subject Carry Carsumtwotwelve is sharing with you on Google+		
25.	7/12/2012 16:12:07	F: Carry Carsumtwotwelve 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	Tracy emailed Carry to ask her what she meant by saying “It will begun” and Carry replied by saying she made a typing error and meant to say “It will be fun”	Mailbox Data Structure

Appendix B: WiFi and GPS Location Information

Timestamp	Header Information	Summary	Evidence Location
6/13/2012 19:01:21	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
6/13/2012 19:01:22	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd,	Location Data

		Arlington, VA 22203)	
6/13/2012 19:04:03	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
6/13/2012 17:12:16	CellLocationLocal	Location: 22 West A Condominium 1177 22nd St NW Washington, DC 20037	Location Data
7/2/2012 16:19:23	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
7/2/2012 16:19:24	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
7/3/2012 13:42:42	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Mailbox Data Structure
7/5/2012 16:32:46	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
7/5/2012 16:32:47	WifiLocationl	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
7/5/2012 16:42:27	CellLocationLocal	226 Upshur St NW Washington, DC 20011	Location Data

7/8/2012 16:34:40	CellLocationLocal	Location: National Gallery of Art Sculpture Garden	Location Data
7/8/2012 16:39:10	CellLocationLocal	Location: National Gallery of Art Sculpture Garden	Location Data
7/10/2012 16:31:10	CellLocation	Location 2600-2700 24th Rd S, Arlington, VA 22206	Location Data
7/10/2012 16:31:12	WifiLocation	Location 2600-2700 24th Rd S, Arlington, VA 22206	Location Data
7/10/2012 16:44:59	CellLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	Location Data
7/10/2012 16:45:01	WifiLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	Location Data
7/10/2012 16:46:29	WifilLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	Location Data
7/10/2012 16:47:12	CellLocationLocal	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	Location Data