Cybersecurity

21.3 The Final Report

Nickson Njau
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 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.

Evidence was uncovered that Tracy, a supervisor at the National Gallery motivated by financial gain, planned a stamp heist at the National Gallery where she worked due to running into some money troubles. During the investigation, evidence was uncovered that supports the following findings: Tracy was using the alias Coral, and Pat was using the alias Perry. Tracy was motivated by financial gain in planning the stamp heist due to running into some money troubles. Emails originating from Tracy's and Pat's personal email containing details of the National Gallery DC stamp letters. Digitech Inc. found evidence indicating that Tracy was formulating a plan to steal stamps with Pat. Additionally, Digitech Inc. found evidence that indicated Tracy knew that Pat was trying to coerce someone named King to help with the heist. Digitech Inc. found evidence indicating Tracy helped an individual named Carry for financial gain. The evidence included leaked sensitive security rotation information about the National Gallery to Carry. There is also evidence indicating that Tracy helped Carry smuggle a tablet into the National Gallery. Also found in "Notes" under the library, Tracy took note of needing to find "help" for Prufrock, which is the school that the daughter attends. (Note aforementioned financial troubles) Also found a search for "Financial Aid" in Tracy's Safari Cache.

Equipment and Tools

- Autopsy
- Kali Linux
- Sqlite Browser (DB Browser for SQLite)

- Google Maps/Google Earth
- Nano (text edit)
- Note Pad (text edit)

Details of Tracy's iPhone

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone (1–2)	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/mobile/Library/Logs/AppleSupport/general.log
OS Version	iPhone OS 4.2.1 (8C148)	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28	/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com, tracysumtwelve@nationalgallergydc.org	vol5/mobile/Library/Mail
Phone Number	(703) 340-9661	vol5/logs/lockdownd.log.1
Serial Number	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	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd2768	

	3e621607	

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:

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

Terry:

Phone Number: (703) 829-6071
Email: N/A
Relationship: Tracy and Joe's daughter

Joe:

Phone Number: N/A
Email: joe.sum.twelve@gmail.com
Relationship: Terry's father, Tracy's ex-husband

Carry:

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

King:

(Alias: Kart)
Email: throne1966@hotmail.com
Relationship: Acquaintance of Pat

The data collected is from Tracy's phone, and the email associated with the Apple ID is 'tracysumtwelve@gmail.com' Also, her work email 'tracy.sumtwelve@nationalgallerydc.org' was setup on this phone, along with another email address under the alias name Coral Blue. Tracy is a supervisor at the NGDC. She is colluding with her brother, Pat (Perry), and his accomplice, King (Kart), to steal stamps at the NGDC. She is also getting some help from her colleague Carry (Cat) at NGDC to get some pictures on a table

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 across the valuable stamp collection exhibit as shown in 'Mailbox Data Structure'. 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 They also show Tracy and Pat being interested in stealing it since it's small and valuable. Pat tries to enroll a guy called King, who has a criminal history and is currently out on parole, into the heist by intimidation and blackmail. King agrees to be a part of the heist and sends out a list of requirements. Pat then forwards the list to Tracy along with instructions on how to access the attachment over SMS, which Tracy then acknowledges. Tracy also emails the Insurance documents regarding the stamp collection exhibit which were marked as confidential to Pat. Tracy's iPhone also has multiple photos of the stamps 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 photos of Gallery Stamps. These were taken prior to the heist. The Geo-Location of these images shows that they were taken at the Museum, showing that Tracy took them while being there. We think that this is information leading to the accusation that she may have been sending them to people or taking them to show people later on.

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, they met over lunch. In the same email, Carry asks Tracy for help sneaking in a tablet into the National Gallery for a flash mob event she was planning. Carry also mentions that she would compensate Tracy for her help. Tracy agrees to sneak in the tablet and a meeting is set for the hand-off at 9. Also, Carry asked for information on security shift change from Tracy in exchange for compensation. Tracy, agrees to pass off the security shift information. Tracy 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 these notifications was the suggestion to add Alex JFamEleven who was a part of Carry's circles. Tracy messaged carry asking about how the flash mob was going. This message and earlier communication together present a view that Tracy although a part in leaking information and smuggling in the tablet, was not aware of anything more in the plot.

Plot Timeline

Date	Information
June 19, 2012 (Tue)	Pat sends Tracy information about a virtual machine.
July 5, 2012 (Thu)	Text messages between Tracy and Carry about meeting up at Bubba's grill.
July 6, 2012 (Fri)	Tracy meets up with Carry at Bubba's grill.
July 6 - July 10, 2012	Correspondence between Tracy, Pat, and King about the tools needed for the stamp heist.
July 08, 2012 (Sun)	Tracy photographs the stamps that they are interested in stealing.
July 09, 2012 (Mon)	Tracy sends herself copies of memos regarding insurance for specific stamps.
July 11, 2012 (Wed)	Tracy meets up with Carry again to take Carry's tablet in with her.
July 12, 2012 (Thu)	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 prime motive was financial gain for planning the stamp heist.
- Tracy emailed National Gallery DC stamp letters to her personal email account and to Pat.
- Tracy formulated a plan with Pat to steal stamps.

- Tracy knew that Pat, was trying to coerce someone named King to help with the heist.
- Tracy helped Carry also, for financial gain.
- Tracy leaked sensitive security rotation information about the National gallery to Carry.
- Tracy helped Carry smuggle a tablet into the Gallery.
- Tracy did not know about the bigger plan that Carry had in mind.

Appendix A: Correspondence Evidence

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

SMS evidence

Artifact #	Timestamp	From	To	Information	Key Information
1	Tuesday, Jun 12, 2012	Pat	Tracy	Pat asks Tracy about her plans for the weekend	
	21:25:04				
2	Wednesday, Jun 13, 2012	Terry	Tracy	I'm going out with dad after school for pizza! Thought I'd let you	
	17:30:28			know if you planned to cook.	

3	Wednesday, Jun 13, 2012	Tracy	Pat	Tracy replies to Pat's message saying that she has no big plans and	
	18:30:38			enquires about his plans.	
4	Wednesday, Jun 13, 2012	Tracy	Terry	Ok, sounds good.	
	18:33:46				
5	Tuesday, Jul 03, 2012	Tracy	Terry	Tracy messages Terry asking about her opinion on switching schools	
	13:41:51			since they can't Prufrock anymore.	
6	Tuesday, Jul 03, 2012	Terry	Tracy	Terry replies back saying that she doesn't want to switch schools	
	14:04:32			and would rather stay with her dad and continue at Prufrock.	

7	Thursday, Jul 05, 2012	Carry	Tracy	Carry sets up the time and location as 1 pm at Bubba's grill for	
	18:18:23			meeting with Tracy	
8	Thursday, Jul 05, 2012	Tracy	Carry	Tracy confirms the meeting time and location	
	18:20:26				
9	Friday, Jul 06, 2012	Tracy	Pat	Tracy asks Pat to give her a call	
	15:02:19				
10	Friday, Jul 06, 2012	Pat	Tracy	Pat says he is busy and suggests calling later	
	15:08:37				
11	Friday, Jul 06, 2012	Tracy	Pat	Tracy says it's important and insists that pat call her soon	

	15:11:54				
12	Friday, Jul 06, 2012	Pat	Tracy	Pat says he will call in 5 min	
	15:13:31				
13	Friday, Jul 06, 2012	Carry	Tracy	Carry messages saying she has a table inside	
	16:27:16				
14	Friday, Jul 06, 2012	Tracy	Carry	Tracy replies back saying that she will be there.	
	16:27:50				
15	Tuesday, Jul 10, 2012	Pat	Tracy	Pat messages Tracy telling her about the email and informing her	The attachment needs to be changed to pdf.
	15:26:19			that the attachment needs to be changed to pdf. He asks Tracy to	Tell this information to Coral.

				tell this information to Coral.	
16	Tuesday, Jul 10, 2012	Tracy	Pat	Tracy acknowledges the email and message.	
	15:58:04				
17	Tuesday, Jul 10, 2012	Tracy	Pat	*Failed	Tracy tried to share the following
	16:37:09				location with Pat over MMS message but it
					failed.
					Location: 2600-2700 24th Rd S, Arlington,
					VA 22206
18	Tuesday, Jul 10, 2012	Tracy	Terry	Tracy messages Terry for Lunch	

	17:18:38				
19	Tuesday, Jul 10, 2012	Tracy	Terry	Tracy messages Terry that she is back at work.	
	18:19:24				
20	Tuesday, Jul 10, 2012	Terry	Tracy	Terry messages Tracy saying she is busy and suggests meeting up	If her dad isn't busy.
	18:58:24			over the weekend if her dad isn't busy.	
21	Wednesday, Jul 11, 2012	Carry	Tracy	Carry messages, Tracy, informing that she is almost there (NGDC)	
	12:41:45				
22	Wednesday, Jul 11, 2012	Tracy	Carry	Tracy replies to Carry asking her to meet out front. She says that	
	12:49:08			she will take the tablet in.	

23	Thursday, Jul 12, 2012	Tracy	Carry	Tracy messages Carry asking her about the flash mob	
	17:06:45				

Email evidence

Artifact #	Timestamp	Header	Information	Key Information	Evidence
1	Tuesday, Jun 19, 2012, 20:06:33	F: Pat, T: patsumtwelve@gmail.com	Pat emails Tracy letting her know that he has accepted her proposal and asks her to email using her alias for further instructions.	Subject: Paris Speak and answer	Mailbox
2	Tuesday, Jun 19, 2012, 20:26:47	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) emails Tracy to ask her to communicate using her alias.	Subject: Look me up sometime	Mailbox

3	Tuesday, Jun 19, 2012, 21:38:59	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Mailbox
4	Tuesday, Jun 19, 2012, 21:39:34	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) replies to Tracy (Coral) confirming that he was getting her emails.	Subject: Re: ???	Mailbox
5	Thursday, Jun 21, 2012, 17:43:15	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) replies to Tracy (Coral) on an email thread about VM installation, suggesting she listen to some songs as well.	Subject: Re: Crazydave by the VMs	Mailbox

6	Thursday, Jun 28, 2012, 19:31:33	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) emails Tracy (Coral) asking her to communicate using aliases and the Virtual Machine setup to keep them safer.	Subject: Whats going on	Mailbox
7	Friday, Jun 29, 2012, 14:21:56	F: Pat, T: perrypatsum@yahoo.com	Email thread between Pat and Tracy (Coral) discussing ideas for making money.	Subject: Re: Whats going on	Mailbox
8	Friday, Jun 29, 2012, 14:31:36	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) emails Tracy, addressing her as ‘sister’, and enquires about Terry.	Subject: hey sis	Mailbox

9	Friday, Jun 29, 2012, 15:21:35	F: Pat (Perry), T: perrypatsum@yahoo.com	Pat (Perry) replies to Tracy (Coral) allaying her concern about IA sniffing around.	Subject: Re: Whats going on	Mailbox
10	Monday, Jul 02, 2012, 16:13:18	F: Tracy (Coral), T: tracysumtwelve@gmail.com	Tracy emails Pat (Perry) mentioning some interesting foreign exhibit and assessing it as a potential opportunity.	Subject: Re: Some good news	Mailbox
11	Monday, Jul 02, 2012, 20:00:31	F: Tracy (Coral), T: tracysumtwelve@gmail.com	Following up on earlier email, Tracy (Coral) mentions the exhibit is worth a lot of money but the shipping cost is low.	Subject: Re: Some good news	Mailbox

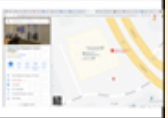
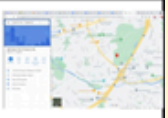
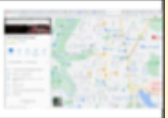
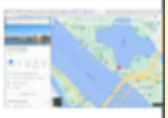
12	Tuesday, Jul 03, 2012, 13:29:37	F: Tracy, T: tracysumtwelve@gmail.com	Tracy emails Joe asking whether he could help her with Terry's tuition since it is becoming too expensive for her.	Subject: Re: Regarding Terry	Mailbox
13	Tuesday, Jul 03, 2012, 14:53:04	F: Tracy (Coral), T: tracysumtwelve@gmail.com	Tracy (Coral) emails Pat (Perry) saying the exhibit is a rare and valuable stamp collection, possibly their opportunity.	Subject: Re: Some good news	Mailbox
14	Thursday, Jul 05, 2012, 15:51:31	F: Carry, T: carrysum2012@yahoo.com	Carry reaches out to Tracy asking to meet for lunch and realizes Tracy is having a hard time recently.	Subject: Long time no see…	Mailbox

15	Friday, Jul 06, 2012, 15:27:51	F: Tracy, T: tracysumtwelve@gmail.com	Tracy emails Pat saying she spoke with Coral and Coral got some great news about her job, suggesting Pat catch up with Coral.	Subject: Re: Good News	Mailbox
16	Friday, Jul 06, 2012, 15:49:31	F: Pat, Cc: Tracy, T: throne1966@hotmail.com	Pat emails King with Tracy (Coral) in cc, proposing a lucrative heist at the national gallery and threatening King to comply.	Subject: can't pass up	Mailbox
17	Friday, Jul 06, 2012, 17:59:24	F: Tracy, T: tracysumtwelve@gmail.com	Tracy suggests Pat, Tracy, and King should hang out sometime.	Subject: Re: Good News	Mailbox

18	Monday, Jul 09, 2012, 18:18:47	F: Carry, T: tracysumtwelve@gmail.com	Carry thanks Tracy for lunch and asks for help sneaking in a tablet for a flash mob event.	Subject: Re: Long time no see…	Mailbox
19	Tuesday, Jul 10, 2012, 13:48:40	F: Carry, T: tracysumtwelve@gmail.com	Tracy agrees to help Carry sneak in the tablet and asks when Carry would like to meet to take a look around the gallery.	Subject: Re: Long time no see…	Mailbox
20	Wednesday, Jul 11, 2012, 17:06:19	F: Carry, T: tracysumtwelve@gmail.com	Tracy confirms the meeting with Carry at 9 the next day.	Subject: Re: Long time no see…	Mailbox
21	Wednesday, Jul 11, 2012, 19:28:53	F: "Google+", T: noreply5dd47ca1@plus.google.com	Previous email from Carry asking for security shift details from Tracy.	Subject: Carry added you on Google+	Mailbox

22	Wednesday, Jul 11, 2012, 23:22:03	F: "Carry (Google+)", T: 748d3d22@plus.google.com	Notification from Google+ informing Tracy that Carry has shared an album.	Subject: Carry is sharing with you on Google+	Mailbox
23	Thursday, Jul 12, 2012, 16:12:07	F: "Carry (Google+)", T: 748d3d22@plus.google.com	Another notification from Google+ informing Tracy that Carry has shared an album.	Subject: Carry is sharing with you on Google+	Mailbox
24	Thursday, Jul 12, 2012, 18:03:51	F: Tracy, T: tracysumtwelve@gmail.com	Tracy emails Carry asking what she meant by “It will be a gun”.	Subject: Re: Long time no see…	Mailbox

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	6/13/2012 12:01:22 PT	WifiLocation	Location: Virginia Tech Research Center - 900 N Glebe Rd, Arlington, VA 22203	
2	7/10/2012 9:31:12 PT	WifiLocation	Location: Near Phillipine Embassy/Hotel Pentagon/Army Navy Country Club - 2480 S Glebe Rd, Arlington, VA 22206	
3	7/10/2012 9:45:01 PT	WifiLocation	Location: Near Citizens Bank (also near a FedEx Dropbox) - 3500 King St, Alexandria, VA 22302	
4	6/13/2012 12:01:21 PT	CellLocation	Location: Virginia Tech Research Center - 900 N Glebe Rd, Arlington, VA 22203	
5	7/5/2012 9:32:46 PT	CellLocation	Location: Near Northwest Community Church - 4100 16th St NW, Washington, DC 20011	
6	7/10/2012 9:31:10 PT	CellLocation	Location: Near Phillipine Embassy/Hotel Pentagon/Army Navy Country Club - 2480 S Glebe Rd, Arlington, VA 22206	
7	7/10/2012 9:44:59 PT	CellLocation	Location: Near Citizens Bank (also near a FedEx Dropbox) - 3500 King St, Alexandria, VA 22302	
8	7/5/2012 9:32:46 PT	CellLocation	Location: Near M & S Grocery and liquor- 213 Upshur St NW, Washington, DC 20011	
9	7/10/2012 9:44:59 PT	CellLocation	Location: Near Ohio Drive Bridge (Near The Whitehouse)- Ohio Dr SW, Washington, DC 20024	
10	7/10/2012	CellLocation	Location: Near Friendship United Methodist Church