Case Report
National Gallery DC

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

By: Carolina Hernandez

Table of Contents

Executive Summary

On the date of January 21, 2016, DigiTech Inc received a call to assist with the National Gallery in Washington DC (NGDC) for a case involving the conspiracy associated with the theft of valuable stamps and defacing foreign art displayed at the museum of art at the NGDC.

- Tracy is a suspect in the conspiracy.
- As part of the investigation of DigiTech Inc. Tracy's iPhone was taken into custody.
- DigiTech was assigned with investigation of the evidence relevant to the conspiracy.

As described on this report, DigiTech Inc. made the following findings on the conspiracy:

Tracy was using the alias 'Coral' and Pat, her brother using the alias 'Perry'.

Tracy's main motivation to commit the crime:

- Recent financial issues.

Email communication between Tracy and Pat containing National Gallery stamp letters.

Evidence denoting that Tracy worked with her acquaintance Carry to perform the crime.

Equipment and Tools

List of Evidence	Files in Encase
Carry's Tablet	Carry-tablet 2012-07-15-0532.E01
Tracy's iPhone	tracy-phone-2012-07-15-final.E01
Tracy's External Hard Drive	tracy-external-2012-07-16-final.E01

Tracy's Macbook Air	tracy-home-2012-07-16-final.E01
Carry's Phone	carry-phone-2012-07-15-final.zip

Details of Tracy's iPhone

NAME	FINDINGS	LOCATIONS IN IPHONE IMAGE FILE
Model	iPhone 1 or 2 3G	vol5/mobile/Library/Logs/AppleS upport/general.log
Host	Tracy Sumtwelves iPhone	vol5/logs/lockdownd.log.1
Name		vol5/preferences/SystemConfiguration/preferences.plist
Os Version	iPHONE OS 4.2.1 (8C148)	vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Install Time	06/06/2012 19:03:28	vol_vol5/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	vol5/mobile/Library/Mail
Phone Number	+15713083236	vol5/mobile/lockdownd.log1
Serial Number	86004482Y7H	vol5/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/wireless/Library/logs/lockdownd.log.1
IMEI	004999010640000	vol5/root/Library/Lockdown/activ ation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc241334629 23f6fea5	
SHA256 Hash	71aed05a86a753dec4ef40 33ed7f52d6 577ccb534ca0d1e83ffd27 683e621607	

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: N/A
Relationship: Tracy's daughter

Joe:

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

Carry:

Phone Number: 202 725 2124
Email:carrysum2012@yahoo.com

Relationship:Acquaintance of Tracy

Evidence relating to theft of valuable stamps

The section below provides details regarding the evidence found on the device as it relates to the theft of valuable stamps.

Tracy stumbles into the valuable stamp collection exhibit as shown in ‘Mailbox Data Structure’. Coral’s (Tracy’s alias) emails to Perry’s (Pat’s alias) mentioning that some interesting foreign exhibit will be taking place soon and that from evaluating the paperwork, she feels that they are very valuable.

They also demonstrate their interest in stealing it since it's small and valuable.

Pat (Tracy’s brother and corrupt police officer) enrolls a guy that goes by the name King, who he knows has a criminal record and he is currently out on parole. Pat convinced King into the heist by intimidation and blackmail. Kings agree to be part of the heist and send out a list of essentials.

Pat forwards the list of essentials to Tracy along with the instructions on how to access the attachment over SMS, which Tracy then acknowledges.

Tracy also sends the Insurance Documents to Pat through email in regards to the stamp collection exhibit which were labeled as confidential. Moreover, multiple pictures of the stamps mentioned in the insurance documents were found on Tracy’s iPhone. The collection of these pieces of evidence makes it clear that Tracy and Pat were conspiring to steal the valuable stamps from the museum of art at the NGDC.

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.

The section below provides details regarding the evidence found on the device as it relates to the Defacement of foreign art displayed at the Museum of art.

Carry reaches her acquaintance Carry to meet over lunch, on the same email Carry casually asks Tracy for help sneaking in a tablet into the Museum for a flash mob event she was planning. Carry also hints at compensation for her help. Tracy agrees to help Carry to sneak the tablet in the museum and sets up a meeting for hand-off at 9.

In addition to the initial request, Carry asked for information regarding security shift change in exchange for compensation. Tracy, agrees to share the security shift information. Moreover, Tracy receives a notification from Google+ informing her that she has been added to Carry's circle and that she shares something with her on Google+. In one of these notifications was the suggestion of adding Alex JFamEleven who was part of Carry's Google+ circle. Tracy also sends a message to Carry asking how the flash mob was going.

Although Tracy took part in the information leaking and smuggling in the tablet. The earlier communication and the last message between them present a view that Tracy was not aware of anything more in the final plot.

Plot Timeline

Call information about call history was found at "/wireless/library/callHistory?call_history.db"

SMS: Information on SMS conversions recorded on the phone was found at "/mobile/Library/SMS/sms.db"

Wifi/GPS location Data: Found at "/root/Library/Caches/locationd/consolidated.db"

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Everyone in the group uses an alias to not be reconoced, for example in Trayc's iPhone we can detect that Tracy used the alias ``Coral" and Pat used the alias ``Perry".
- One of the reasons that motives Tracy to gain for planning the stamp heist was financial problems.
- Tracy works as a supervisor and emailed National Gallery DC stamp letters to her personal email account and to Pat.

- The Plan to steal the stamps was by Tracy and Pat.
- Tracy knew that Carry have “connections”, and knew that Pat was trying to coerce someone named King to help with the heist
- Tracy helped Carry also, for financial gain.
- Tracy helped Carry smuggle a tablet into the Gallery, because both are technologically savvy, know steganography tools and encryption.
- Tracy did not know about the bigger plan that Carry had in mind.

Appendix A: Correspondence Evidence

Email and SMS Information			
Timestamp	**Header Information**	**Summary**	**Evidence Location**
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
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.	
6/19/2012 21:38:59	F: perrypatsum@yahoo.com T:coralbluetwo@hotmail.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		
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.	
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 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.	
6/28/2012 19:31:33	F: perrypatsum@yahoo.com T:coralbluetwo@hotmail.com Subject: What's 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	
6/29/2012 14:21:56	F: perrypatsum@yahoo.com T:coralbluetwo@hotmail.com Subject: Re: What's going on	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money. 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.	
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 checking 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.	
6/29/2012 15:21:35	F: perrypatsum@yahoo.com T:coralbluetwo@hotmail.com Subject: Re: What's 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	

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

Appendix B: Wi-Fi and GPS Location Information

Group members:

Location Information				
Artifact #	**Timestamp**	**Header Information**	**Body**	**Map Screenshot**
	6/13/2012 19:01:21	CellLocation	Location: Virginia Tech Research Center -Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	6/13/2012 19:01:22	WifiLocation	Location: Virginia Tech Research Center -Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	6/13/2012 19:04:03	WifiLocation	Location: Virginia Tech Research Center -Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	6/23/2012 17:12:16	CellLocationLocal	Location: 22 West A Condominium 1177 22nd St NW Washington, DC 20037	IMAGES
	7/2/2012 16:19:23	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES

	7/2/2012 16:19:24	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	7/3/2012 13:42:42	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	7/5/2012 16:32:46	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	7/5/2012 16:32:47	CellLocationLocal	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	IMAGES
	7/5/2012 16:42:27	CellLocationLocal	226 Upshur St NW Washington, DC 20011	IMAGES
	7/8/2012 16:34:40	CellLocationLocal	Location: National Gallery of Art Sculpture Garden	IMAGES
	7/8/2012 16:39:10	CellLocationLocal	Location: National Gallery of Art Sculpture Garden	IMAGES
	7/10/2012 16:31:10	CellLocation	Location: 2600-2700 24th Rd S, Arlington, VA 22206	IMAGES

	7/10/2012 16:31:12	WifiLocation	Location: 2600-2700 24th Rd S, Arlington, VA 22206	IMAGES
	7/10/2012 16:44:59	CellLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	IMAGES
	7/10/2012 16:45:01	WifiLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	IMAGES
	7/10/2012 16:46:29	WifiLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	IMAGES
	7/10/2012 16:47:12	CellLocationLocal	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	IMAGES