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.

- Tracy was using the alias" Coral"and Pat was using the alias" Perry"
- Tracy is suspected of helping Carry to conduct a flash mob at the museum
- The motivation for the crime is primarily financial gain due to financial hardship
- There are email correspondence between Tracy and Pat containing National Gallery stamps
    - Tracy and Pat are planning to steal stamps from the gallery

Equipment and Tools

- Kali Linux Terminal
- Autopsy
- SQlite Browser
- Nano

Details of Tracy's iPhone

Name	**Findings**	**Location in iPhone image file**
Model	iPhone 1, 2	general.log
Host Name	Tracy Sumtwelve	lockdownd.log.1
OS Version	4.2.1	general.log
Install Time	6/6/2012 12:03	general.log

User Email	tracysumtwelve@gmail.com	addressbook.sqlitedb
Phone Number	703-340-9661	lockdownd.log.1
Serial Number	86004482Y7H	general.log
ICCID	89014103255195342366	lockdownd.log.1
IMEI	012021003735398	wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	

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 (Employed as supervisor at National Gallery)

Since the iPhone belongs to Tracy, her contact information was derived from the primary information stored in the iPhone as well as email and text message communications.

Pat:

Phone Number:	571-308-3236

Email: patsumtwelve@gmail.com
Relationship: Tracy's brother

Pat's contact information was derived from text and email communications between him and Tracy.

Terry:

Phone Number: 703-829-6071
Relationship: Tracy and Joe's teenage daughter

Terry's contact information was retrieved from text messages between her and Tracy.

Joe:

Email: joe.sum.twelve@gmail.com
Relationship: Tracy's ex-husband

Joe's contact information was derived from email communications.

Carry:

Phone Number: 202-725-2124
Email: carrysum2012@yahoo.com
Relationship: Krasnovian supporter

Carry's contact information was derived from email communications.

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.]

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.

[After Carry reached out to Tracy, they met over lunch. Carry also asks Tracy for help sneaking in a tablet into the National Gallery for a flash mob event. Carry also mentions that she would pay Tracy for her help. Tracy agrees and a meeting is set for the hand-off at 9.

Carry asked for information on security shift change from Tracy in exchange for compensation. Tracy, agrees to pass off the security shift information.]

Plot Timeline

Friday, July 6, 2012 - Pat emailed King to help execute a heist at the national gallery. Tracy is copied on this email.
Tuesday, July 10, 2012 - King sent an attachment specifying the tools needed to execute the heist.
Tuesday, July 10, 2012 - Pat forwards King's email to Tracy, noting that King will play a role in the heist.

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 corresponce evidence.

Artifact #	Timestamp	Header Information	Key Information
8A3BD06F	Jul 9 2012 - 7:47	To coralbluetwo@hotmail // from tracysumtwelve@gmail Things	Files attached [documents.zip] txt/plain 7bit encoding charset=us-ascii base 64
01FE9965	Jul 11 2012 11:18	To Coralbluetwo@hotmail - from michrosoft 30 Day Free Trail	Free trial expiration email
3896FC6F	Jun 19 2-12 : 14:39	To perrypatsum@yahoo // from tracysumtwelve@gmail Crazydave VMs	Mp3 files
9F0508B8	Jul 10 2012 // 11:24	To ‘’ // from patsumtwelve@gmail // forwarded from: throne1966@hotmail (king kthings) Needs	Blackmailing king (on parole 4 drugs/still using) - txt files dictating operation needs [needs.txt]
F3F4EB95	Jul 5 2012 // 12:58	To coralbluetwo // from woina.honril@m57.biz Busy	File 000001.doc - “I didnt”

Appendix B: WiFi and GPS Location Information

WI-FI/GPS LOCATION CONTENT

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, Arlington, VA 22203)	Location Data
6/13/2012 19:04:03	WifiLocation	Location: Virginia Tech Research Center -Arlington (900 N Glebe Rd, Arlington, VA 22203)	Location Data
6/23/2012 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	WifiLocation	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	WifiLocation	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