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 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 found that Tracy and several of her accomplices are guilty of theft and vandalism.

Equipment and Tools

I used Autopsy on Kali Linux and Google.

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone1,2	vol5/logs/AppleSuport/general.log
Host Name	Tracy-Sumtwelves-iPhone	vol5/mobile/preferences/SystemConfiguration
OS Version	iPhone OS 4.2.1 (8C148)	vol5/logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	vol5/logs/AppleSupport/general.log
User Email	IMAP: tracysumtwelve@gmail.com POP: coralbluetwo@hotmail.com	vol5/mobile/Library/Mail/Envelope Index
Phone Number	1 (703) 340-9661	vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log.1
IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist

MD5 Hash	34c4888f095dc3241330462923f6fea5	n/a (tracy-phone-2012-07-15-final.E01 image)

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: perrypatsum@yahoo.com/patsuymtwelve@gmail.com
Relationship: Tracy's brother

Terry:

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

Joe:

Phone Number: unknown

Email: unknown
Relationship: Tracy's ex-husband

Carry:
Phone Number: (202) 725-2124
Email: unknown
Relationship: Tracy's friend

All of these contacts were in communication with Tracy.

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.

Emails and text messages between Tracy, Pat, Carry, and King lay out a timeline of the planning and execution of the heist. Appendix A is the display of the timeline. Within the exchange of emails are insurance documents and pictures of the 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.

No direct evidence of defacement of the museum art was found.

Plot Timeline

- June 19: Pat and Tracy communicate, Tracy sets up a VM for communication using aliases.
- June 21: Tracy confirms to Pat that the VM is set up.

- June 28: Pat and Tracy begin communicating using the VM, plotting a way to make money due to financial hardship.
- June 29: Pat and Tracy communicate their worries about IA.
- July 2: Tracy and Pat discuss the foreign exhibit coming to the museum as a possibility for making money.
- July 3: Tracy asks her ex-husband Joe for financial support, to which he declines. This prompts further motivation for her involvement in the heist.
- July 6: Pat and Tracy make contact with King to discuss the heist.
- July 9: Pat and Tracy discuss how to sneak the tablet into the museum.
- July 10: Tracy agrees to carry the tablet in. King agrees to the heist and tells them what equipment he will need.
- July 11: Tracy and Carry discuss the guard shift change. Tracy agrees to send it to her.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

Tracy, Pat, King, and Carry all planned to carry out the heist.

Appendix A: Correspondence Evidence

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

1.	6/19/2012 20:06:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Paris Speak and answer	Pat emailed Tracy to tell her that he has accepted her proposal and tells 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 emailed Tracy to tell her to use 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	Perry emailed Tracy with to install a VM.	Mailbox Data Structure
4.	6/19/2012 21:39:34	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: ???	Pat tells Perry the emails were received.	Mailbox Data Structure
5.	6/21/2012 17:43:15	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Crazydave by the VMs	Tracy confirms the instructions sent helped to install the VM	Mailbox Data Structure
6.	6/28/2012 19:31:33	6/28/2012 19:31:33 F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Whats going on	Pat tells Tracy to communicate using the VM and discusses engaging in illicit behavior due to financial hardship.	Mailbox Data Structure
7.	6/29/2012 14:21:56	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	Pat and Tracy communicate on the VM discussing how to make money. Pat is concerned about IA.	Mailbox Data Structure
8.	6/29/2012 14:31:36	F: perrypatsum@yahoo.com T: tracysumtwelve@gmail.com Subject: hey sis	Pat communicates with Tracy addressing her as ‘sister’ asking about Terry. This was a possible misdirection attempt.	Mailbox Data Structure
9.	6/29/2012 15:21:35	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on	Pat is concerned about IA.	Mailbox Data Structure
10.	7/2/2012 16:13:18	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Tracy contacts Pat about a foreign exhibit and that it may be an opportunity.	Mailbox Data Structure

11.	7/2/2012 20:00:31	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Tacy and Pat further discuss that the exhibit could be worth a lot of money.	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 Joe asking for financial support.	Mailbox Data Structure
13.	7/3/2012 14:53:04	F: perrypatsum@yahoo.com T :coralbluetwo@hotmail.com Subject: Re: Some good news	Tracy and Pat discuss ideas for stealing the stamps.	Mailbox Data Structure
14.	7/5/2012 15:51:31	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Long time no see...	Carry contacts Tracy asking her if they could meet for lunch.	Mailbox Data Structure
15.	7/6/2012 15:27:51	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Tracy talks with Pat saying that she spoke with Coral and that Coral got some great news about her job and suggested that Pat catch up with Coral. Pat says back saying that he knows a guy called King.	Mailbox Data Structure
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 King with Tracy discussing the heist at a national gallery. He also threatens King to help by putting his parole at stake.	Mailbox Data Structure

17.	7/6/2012 17:59:24	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Tracy says King, Tracy and Pat should hang out. Pat emailedTracy with account login information for an email. A .zip file with insurance documents was sent.	Mailbox Data Structure
18.	7/9/2012 14:44:11	F: tracysumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: things		/mobile/Librar y/Mail/POP-coralbluetwo @hotmail.com @pop3.live.com/INBOX.mbox/Messages/8A3BD06F-CDB1-4453- 9C69-77E06823F2AE.emlx
19.	7/9/2012 18:18:47	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see..	Carry asks Tracy for help finding a way to get a tablet for a flash mob event in. Carry said she would be paid for the help.	Mailbox Data Structure
20.	7/10/2012 13:48:40	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Tracy agreed to help Carry sneak in the tablet.	Mailbox Data Structure
21	7/10/2012	F: patsumtwelve@gmail.com	King agrees to do the heist and tells	/mobile/Lib

	15:24:57	T: coralbluetwo@hotmail.com Subject: Fwd: can't pass up Attachment: needs.txt	them what equipment he will need.	rary/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E- A7F0-3E23B0E7C59B.emlx
22.	7/11/2012 17:06:19	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Carry asks Tracy to give her information on security guard shift changes and tells he she will be paid and Tracy confirms.	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+	Carry asks 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 Subject: Carry	Tracy sends the security shift details.	Mailbox Data Structure

		Carsumtwotwelve is sharing with you on Google+		
25.	7/12/2012 16:12:07	F: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+	Mailbox Data Structure
26.	7/12/2012 18:03:51	F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Carry discusses a previous typo.	Mailbox Data Structure
27.	Jul 7 2012 07:36:35 P	SMS from 206-910-0932	"Congratulations, your entry in last months drawing won you a FREE $1,000 Target Giftcard! Enter ""703"" at www.target.com.trdt.biz to tell us where to ship it"	sms.db
28.	Jul 11 2012 12:41:45	SMS to Carry	"I'm almost there where should I meet you?"	sms.db
29.	Jul 11 2012 12:49:08	SMS to Carry	"Just meet me out front, I'll take the tablet in."	sms.db
30.	Jul 12 2012 17:06:45	SMS to Carry	"How's the flashmob going"	sms.db

Appendix B: WiFi and GPS Location Information

```
        Timestamp MagneticX MagneticY MagneticZ BiasX BiasY BiasZ Level Magnitude Inclination

WifiLocation

        MAC Timestamp Latitude Longitude HorizontalAccuracy Altitude VerticalAccuracy Speed Course Confidence
        44:1e:a1:f4:d:7f 3.61306882473715E8 38.88055896 -77.11553561 281.0 96.0 19.0 -1.0 -1.0 50
        0:23:5e:b0:6d:f1 3.61306882473715E8 38.88106083 -77.11533838 68.0 113.0 13.0 -1.0 -1.0 50
        0:26:b8:ac:1c:10 3.61306882473715E8 38.88005346 -77.11595332 42.0 103.0 23.0 -1.0 -1.0 50
        c0:c1:c0:15:66:fa 3.61306882473715E8 38.88093715 -77.11640596 42.0 134.0 9.0 -1.0 -1.0 50
        e0:46:9a:3f:1b:a6 3.61306882473715E8 38.87996816 -77.11601394 42.0 104.0 38.0 -1.0 -1.0 50
        54:75:d0:a5:f:a3 3.61306882473715E8 38.88138395 -77.11556851 48.0 133.0 43.0 -1.0 -1.0 50
        54:75:d0:a5:f:a0 3.61306882473715E8 38.88139647 -77.11564362 42.0 111.0 31.0 -1.0 -1.0 50
        0:26:b8:ad:bd:dc 3.61306882473715E8 38.87974703 -77.11598318 42.0 101.0 21.0 -1.0 -1.0 50
        0:26:b8:ac:19:d0 3.61306882473715E8 38.87969022 -77.1154859 42.0 99.0 17.0 -1.0 -1.0 50
        0:26:f3:f8:b8:fb 3.61306882473715E8 38.87970983 -77.11530274 42.0 101.0 18.0 -1.0 -1.0 50
        0:26:f3:f8:b8:f8 3.61306882473715E8 38.87970793 -77.11529815 42.0 101.0 23.0 -1.0 -1.0 50
        0:26:b8:ae:e7:1b 3.61306882473715E8 38.8796842 -77.11539471 42.0 101.0 20.0 -1.0 -1.0 50
        0:26:f3:f8:b8:f9 3.61306882473715E8 38.87969332 -77.11530435 42.0 99.0 20.0 -1.0 -1.0 50
        0:26:b8:ac:6:68 3.61306882473715E8 38.87969988 -77.11591041 42.0 96.0 16.0 -1.0 -1.0 50
        0:24:6c:67:e8:a0 3.61306887017 53E8 0.0 0.0 -1.0 0.0 -1.0 -1.0 -1.0 0
        0:24:6c:67:e6:1 3.6130700024568E8 0.0 0.0 -1.0 0.0 -1.0 -1.0 -1.0 0
        e4:e0:c5:f:29:fa 3.61307043743548E8 38.88143724 -77.11478394 45.0 140.0 25.0 -1.0 -1.0 50
        0:18:1:fb:b2:c3 3.61307043743548E8 38.8815732 -77.11455619 88.0 138.0 45.0 -1.0 -1.0 50
        0:18:f8:1a:69:23 3.61307043743548E8 38.88154673 -77.11469429 44.0 131.0 34.0 -1.0 -1.0 50
        0:26:62:44:d5:4f 3.61307043743548E8 38.88157737 -77.11462634 43.0 130.0 35.0 -1.0 -1.0 50
```