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

- Tracy is a suspect in the conspiracy above.
- As part of the investigation, Tracy's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the conspiracy above.

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

[Provide a summary of your findings here.]
Pat, known to be Tracy's brother, conspired with this unknown 3rd party with the email address "King Kthings throne1966@hotmail.com" to steal stamps from the National Gallery. One of the emails has an attachment with a list of how the theft will be carried out.

Equipment and Tools

<Briefly summarize the equipment and tools you used to gather and analyze the evidence.>
The equipment and tools used are as follows:

1. Maps.google.com

2. Digitech also used the Autopsy open-source forensics tools on the Kali Linux host to analyze images found on Tracy's phone.

Details of Tracy's iPhone

[Add Tracy's iPhone Details worksheet from Day 2 here.

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)
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	n/a (tracy-phone-2012-07-15-final.E01 image)

Evidence to Establish Personas

This section establishes aliases, phone numbers, and email 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: 703-340-9961

Email: perrypatsum@yahoo.com

Relationship: Tracy's brother

Terry:

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

Joe:

Phone Number: Unknown
Email: Unknown
Relationship: Tracy's ex-husband

Carry:

Phone Number: 202-725-2124
Email: carrysum2012@yahoo.com
Relationship: Tracy's accomplice and friend

[Provide a summary of your conclusions here.]

TRACY

Tracy is a single mother battling for her child's custody. Tracy's daughter attended a private school that is very expensive and puts Tracy where she can no longer afford the fees. The ex-husband offered to pay the school fees to Tracy on the condition that their daughter be with him. Meanwhile, Terry, who is 15 years old, preferred to be with Dad because it would keep her in school since Dad would be paying school fees.

PAT

Pat is Tracy's brother, a police officer of the D.C. Enforcers Bureau. He is a detective close to his sister and niece, Terry. He busted King with some items against his parole, but there was no evidence that King was arrested, only a promise of future favor.

JOE

Joe is Terry's father, who is going through a divorce from Tracy. Joe is financially well-off compared to Tracy. He wants custody of the child because he has the money to pay for the school fees and Terry's upkeep. Joe installed a keylogger on the MacBook Air to keep track of Terry's online behavior and spy on Tracy and Terry's activities.

ALEX

Alex is a foreigner who lives outside the country as a Krasnovian supporter who wishes to embrace the United States. The name of the region where he lives is Krasnovia. Alex knows Carry through extended family connections and contacts her as both have similar family ties and are fellow Krasnovians. His purpose is to deface foreign works on exhibit in the National Gallery of DC. Defacing this artwork will damage the foreign country's reputation with the United States. Some documentation referred to it as 'Majavia,' a second pseudo-nation.

CARRY
Carry was contacted by Alex since both of them share family ties. As a Krasnovian supporter, Carry is occasionally a social media user whom Alex contacts to orchestrate the defacing of the artwork because she is a Krasnovian supporter and has 'connections.' She is also Tracy's friend and accomplice.

TERRY

Terry is the daughter of Tracy and Joe, who attends Prufrock Preparatory School, a private school with expensive school fees that Tracy can no longer afford. Terry prefers to stay in the same school and keep her current friends, so she stays with Dad since Dad Joe can afford to pay the school fees.

Evidence relating to the theft of valuable stamps

This subsection provides details regarding the evidence related to the theft of valuable stamps.

Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your findings.]

In conclusion, it is known that SMS messages were exchanged between Carry, Pat, and Tracy with an unknown co-conspirator with the email address "King Kthings throne1966@hotmail.com" (referenced in Appendix A).

One of the emails from “King Kthings” has an attachment with a list of items needed for the theft. This can be found in needs.txt, which contains the following items:

1. A rope and a Javelin (using alternative means to break in)
2. Tactical Turtlenecks (what I will be wearing)
3. Spray Paint (for the cameras)
4. Vibram's finger shoes (to walk silently)
5. Pack of smokes (detecting lasers)
6. Smoke grenades (used as a means of escape if caught)

There was an MP3 audio file attachment (Crazydave1.mp3) with detailed instructions on installing a VirtualBox VM on a host computer, which was to be used for this crime.

The SMS message was to inform Tracy that she had received a $1000 Target gift card, with instructions to visit a misleading website like www.target.com.trdt.biz and enter a code with instructions on “where to ship it.” This website is deceptive because it does not relate to Target Corporation and is not registered simultaneously.

Photos for all stamps were listed in the insurance documents on that phone. It also has 3 .pdf email attachments, which include the Memoranda of Insurance for different valuable stamps and the pictures of those stamps in the camera storage location. Of the stamps in the camera storage location. Evidence location can be found on:
/vol5/mobile/Media/DCIM/100APPLE/IMG_0056.JPG
/vol5/mobile/Media/DCIM/100APPLE/IMG_0051.JPG
/vol5/mobile/Media/DCIM/100APPLE/IMG_0057.JPG

The above stamps were the stamps used. Stamps 1,2, and the last is stamp 3.

Evidence relating to the defacement of museum art

This subsection provides details regarding the evidence related to the defacement of museum art.

Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your findings.]

No evidence relates to the defacement of museum art in the iPhone image.

Plot Timeline

Provide an outline of the key events in the order in which they occurred. Note the date of each event.]

1. There was a voice instruction on installing a VirtualBox VM on Tracy's computer for later use. This was done by the MP3 audio recording attachment on Tue, Jun 19, 2012, at 02:38 PM. Pat emailed Tracy.
2. There was an agreement between Tracy and Carry through SMS to meet at Bubba's Grill. This occurred on Thu, Jul 5, 2012, 06:18:23 PM.

3. Fri, Jul 6, 2012, 11:49:31 AM There was an email sent by Pat with the subject "can't pass up," a "proposition" with someone who goes by "King."
4. Fri, Jul 6, 2012 04:27:16 PM Tracy and Carry confirmed the meeting at Bubba's through SMS.
5. On Saturday, Jun 7, 2012, at 07:36:35 PM, Tracy received an SMS that said she had a Target Gift Card worth $1000. It goes by, "Congratulations, your entry in last month's drawing won you a free $1,000 Target gift card! Enter " " 703 at www.target.com.trdt.biz to tell us where to ship it." Meanwhile, this fake website looks like Target Corp, and its registration cannot be found. You can see that there is no proof that payment was received from Alex.
6. Mon, Jul 9, 2012, 10:44:11 AM Tracy sends herself an email with a complete description of which stamps to steal and how much it is insured for.
7. On Mon, Jul 9, 2012, 10:44:11 AM, Pat and "King" had an arrangement through email with a list of things that King would need to do the job.
8. On Tue, Jul 10, 2012, 11:24 AM, Pat sends the list to Tracy.
9. On Wed, Jul 11, 2012, 12:12:41:45 PM, Tracy and Carry had an arrangement through SMS for Tracy to get a tablet delivered to Carry.
10. On Thu, Jul 12, 2012, 05:06:45 PM, Tracy texts Carry concerning the flashmob and how the flashmob was going.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- [Summarize your conclusions about the case and Tracy's iPhone here.]
- [For example, Tracy used the alias Coral, and Pat used the alias Perry.]

- Both Tracy and Pat conspired with each other to use email account aliases. We all know that Pat's actual email address is perrypatsum@yahoo.com. Tracy's actual email address is tracysumtwelve@gmail.com. So with this alias account, Pat used patsumtwelve@gmail.com, and Tracy used coralbluetwo@hotmail.com
- Pat collaborated with King Kthings using an email address called "throne1966@hotmail.com" to steal stamps. The influence on King was much easier for him because Pat knew King's parole officer.
- Also, cell location and WiFi indications are linked to all emails, phone calls, and SMS exchanges.
- There is a plan between Tracy and Carry about a flash mob that will help to distract the museum security guards so that King can commit the atrocity.
- There is a document containing stamps with the insured amount, which Tracy sent herself.
- A Gift card for $1000 was set up for Tracy.

Appendix A: Correspondence Evidence

This subsection will amalgamate the correspondence evidence from the email and SMS.
[Paste your Correspondence Evidence Worksheet here.]

Location Information				
Artifact #	**Timestamp**	**Header Information**	**Body**	**Map Screenshot**
1	Tue, June 12	Call from 703-829-6192		vol5/wireless/Library/call

Location Information				
	2012			history/call_history.db
2	Wed, June 13, 2012 4:29:13 pm	Call Pat (571-308-3236)		/vol5/wireless/library/Call_History.db
3	Wed, Jun 13, 2012 5:30:28pm	Message (SMS) Terry 703-829-6071	I'm going out with Dad after school for pizza! I thought I'd let you know if you planned to cook. "Terry".	/vol5/mobile/library/SMS.db
4	Wed, Jun 13, 2012 6:30:38 pm	Message (SMS) To Pat 571-308-3236	" I don't have any big plans. How about you?".	/vol5/mobile/library/SMS.db
5	Wed, Jun 13, 2012 6:33:46 pm	Message (SMS) to Terry on 703-829-6071	"Ok, sounds good."	/vol5/mobile/library/SMS.db
6	Tue, Jun 19, 2012 02:38:59 pm	EMAIL: From: Perry Patsum perrypatsum@yahoo.com To: Coral Blue two coralbluetwo@hotmail.com. Subject: Crazydave by the VMs Attach: Crazydave1.mp3	"Hey, Coral, I just got your email. That took longer than expected! Oh well! You've got to check out this new song by the VMs. I love the base. Tell me what you think! Meanwhile, we noticed that there were voice messages from Perry to Tracy explaining how to install VirtualBox	/vol5/mobile/library/Mail/pop-coralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages /mobile/library/Voicemail/voicemail.db
7	Tue, Jul 3, 2012 01:41:51 pm	Messages (SMS) to Terry on 703-829-6071	"Hey honey, I'm not sure we can afford Prufrock anymore… What do you think about maybe switching somewhere else?	/vol5/mobile/library/SMS.db
8	Tue, Jul 3	Messages	"Moving schools at this point would be the worst! I	/vol5/mobile/

	2012 02:04:32 pm	(SMS) from Terry on 703-829-6071	would rather live with Dad and stay at Prufrock than change schools:"	library/SMS.db
9	Thu, Jul 5, 2012 06:18:23 pm	Message (SMS) from Carry 202-7252124	"Sounds good. Let's shoot for one at Bubba's grill."	/vol5/mobile/library/SMS/sms.db

10	Thu, Jul 5 2012 06:20:2	Messages (SMS) to Carry 202-725-2124	"Okay, that sounds great. See you there".	/vol5/mobile/library/SMS/sms.
11	Fri, Jul 6, 2012 11:49:31 AM	EMAIL: From patsumtwelve@gmail.com To: throne1966@hotmail.com Cc: coralbluetwo@hotmail.com Subject: can't pass up	King, Long time no see.. I have a juicy proposition for you. Two weeks from now, my associates and I are planning a heist at the National Gallery. However, we need a helping hand. You are on parole right now and are probably hesitant to participate. Your parole officer and I went years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, I feel he wouldn't be too happy. It is very easy for a person to phone the feds with an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test, and since you're on parole, the feds don't need a search warrant. Well, hit me up. You know where to find me.	/vol5/mobile/library/Mail/ /vol5/mobile/library/Mail/POP-coralbluetwo@hotmail.com/INBOX.MBOX/Messages/
12	Fri, Jul 6, 2012 04:27:16 pm	SMS from 202-725-2124 - Carry	" I have a table inside."	/vol5/mobile/library/SMS/sms.db
13	Fri, Jul 6, 2012 04:27:50 pm	SMS to 202-725-2124 - Carry	"Okay, but"	/vol5/mobile/library/SMS.sms.db
14	Sat, Jul 7, 201,2 07 36:35 pm	SMS from Unknown On 206-910-0932	"Congratulations, your entry in last month's drawing won you a free $1,000 Target Gift Card! Enter `` " 703" " at www.target.com.trdt.biz to tell us where to ship it."	/vol5/mobile/library/SMS/sms.db

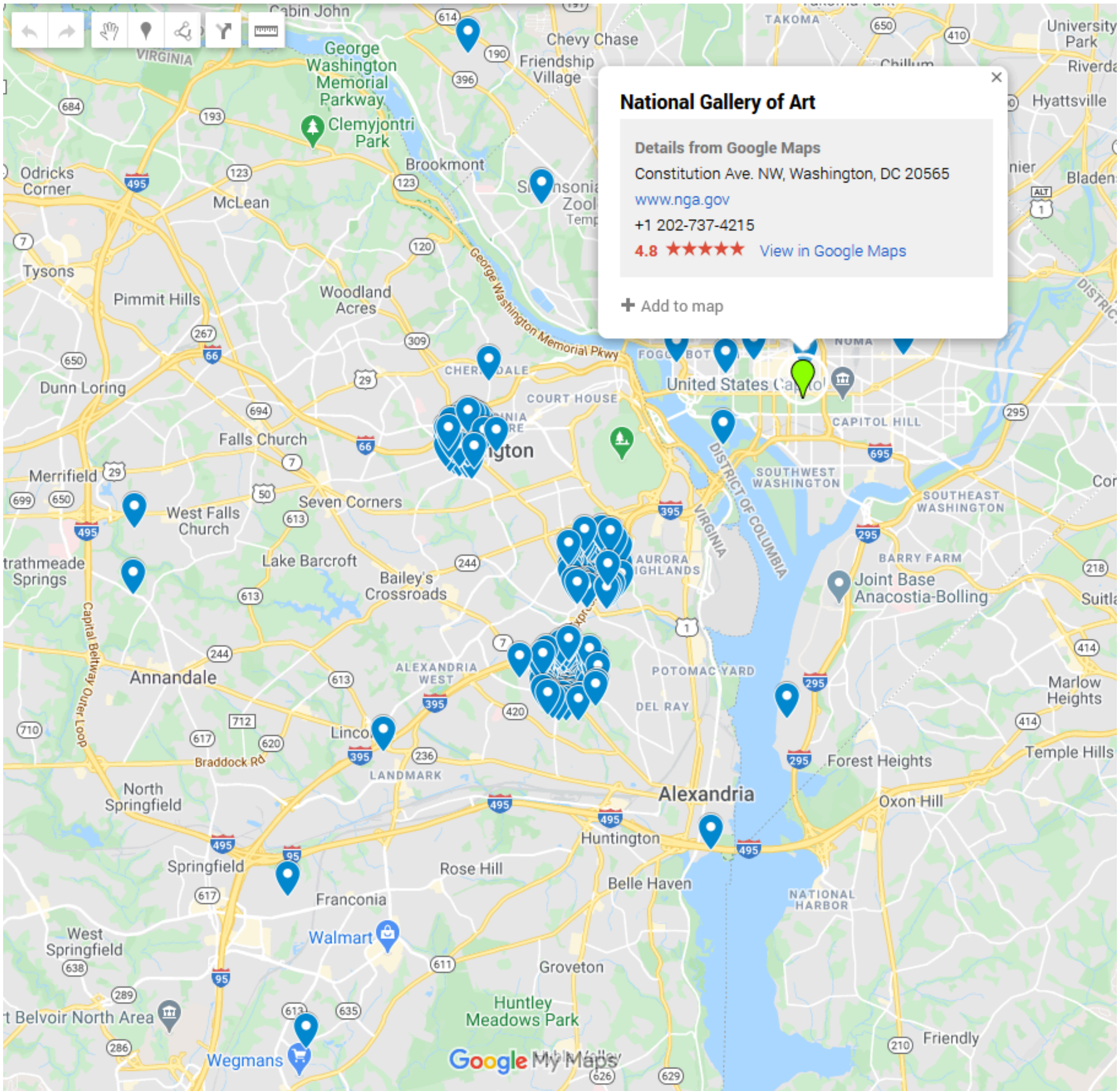
15	Tue, Jul 10 2012 11:19 AM	EMAIL: From: King Kthings throne1966@hotmail.com To: patsumtwelve@gmail.com Subject: RE: can't pass up Attach: needs.txt	You are too kind … I got you, brotha. I need some tools to do this job for you. Here are some requirements that I will need: See attachment The attachment contains the following: A rope and a Javelin (using alternative means to break in) Tactical turtlenecks (what I will be wearing) Spray paint (for the cameras) Vibram's finger shoes (to walk silently) Pack of smokes (detecting lasers) Smoke grenades (used as a means of escape if caught)	/vol5/mobile/library/Mail/POP
16	Tue, Jul 10 2012 11:24 AM	EMAIL: From: TeeSumTwelve patsumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: FWD: can't pass up	" This is what we need to get for the guy that will make our job happen."	/vol5/mobile/library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.MBOX
17	Tue, Jul 10, 2012 03:26:19 pm	SMS from 571-308-3236 Pat	" Hey, sis, your friend Coral got an email. The attachment needs to be changed to PDF. Let her know."	/vol5/mobile/library/SMS/sms.db
18	Tue, Jul 10, 2012	SMS to 571-308-3236 Pat	" Sure thing, I'll get on it."	/vol5/mobile/library/SMS/sms.db

19	Tue Jul 10 2012 05:18:38 PM	SMS to 703-829-6071 Terry	"Going to lunch. You want to go???!?!"	/vol5/mobile/library/SMS/sms.db

20	Tue, Jul 10, 2012 06:19:24 PM	SMS to 703-829-6071 Terry	“Back at work”	/vol5/mobile/library/SMS/sms.db

Appendix B: WiFi and GPS Location Information

[Paste your GPS Evidence Worksheet here.]


National Gallery of Art
Details from Google Maps
Constitution Ave. NW, Washington, DC 20565
www.nga.gov
+1 202-737-4215
4.8 ★★★★★ View in Google Maps
Add to map
Chevy Chase
Friendship Village
George Washington Memorial Parkway
Clemyjontri Park
Brookmont
McLean
Tysons
Pimmit Hills
Woodland Acres
Dunn Loring
Falls Church
Merrifield
West Falls Church
Seven Corners
Lake Barcroft
Bailey's Crossroads
Annandale
North Springfield
Springfield
Franconia
Rose Hill
Alexandria
Huntington
Belle Haven
Groveton
Huntley Meadows Park
West Springfield
Walmart
Wegmans
United States Capitol
Capitol Hill
Southwest Washington
Southeast Washington
Joint Base Anacostia-Bolling
Forest Heights
Oxon Hill
Temple Hills
Marlow Heights
Friendly
Hyattsville
National Harbor
Potomac Yard
Del Ray
Aurora Highlands
Court House
Landmark
Alexandria West
Odricks Corner
Google My Maps