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.

Based on the information found during our investigation, there is evidence and reason to believe that Tracy and her brother Part conspired with 'King' (unknown 3rd party), to carry out the theft of stamps from the National Gallery, with intent to deface several high value pieces of artwork.

Equipment and Tools

The open-source tool 'Autopsy' was used to carry out our Forensic investigation. Other tools publicly available were also used such as Google Maps.

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone1,2	vol5/logs/AppleSupport/general.log
Host Name	Tracy-Sumtwelves-iPhone	vol5/mobile/preferences/SystemConfiguration
OS Version	4.2.1 (8C148)	vol5/logs/AppleSupport/general.log
Install Time	06/06/2012 12:03:28	vol5/logs/AppleSupport/general.log

User Email	Imap: tracysumtwelve@gmail.com Pop: coralbluetwo@hotmail.com	vol5/mobile/library/Mail/metadata.plist
Phone Number	1-(740)-340-9661	vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log
IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	N/A
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	N/A

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

Terry:

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

Joe:

Phone Number: N/A
Email: N/A
Relationship: Father to Terry, Tracy's ex-husband

Carry:

Phone Number: (202) 725-2124
Email: N/A
Relationship: Tracy's friend

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.

Email messages were found between someone named 'King', Tracy, Pat & Carry.

Within one of those email messages was found to be a list of items that were said to be required to complete the heist. Those items included:

- A rope and javelin
- Tactical turtlenecks (Apparel)
- Spray Paint

- Vibram five finger shoes
- Pack of smokes
- Smoke grenades

Next to each item was also the reasoning behind why each item would be necessary.
The Rope & javelin were a means of breaking in, the tactical turtlenecks was what would be worn, spray paint to block the cameras, Vibram five finger shoes to walk quietly, pack of smokes to evade laser detection, and smoke grenades as a means of escape if they were to have gotten caught.

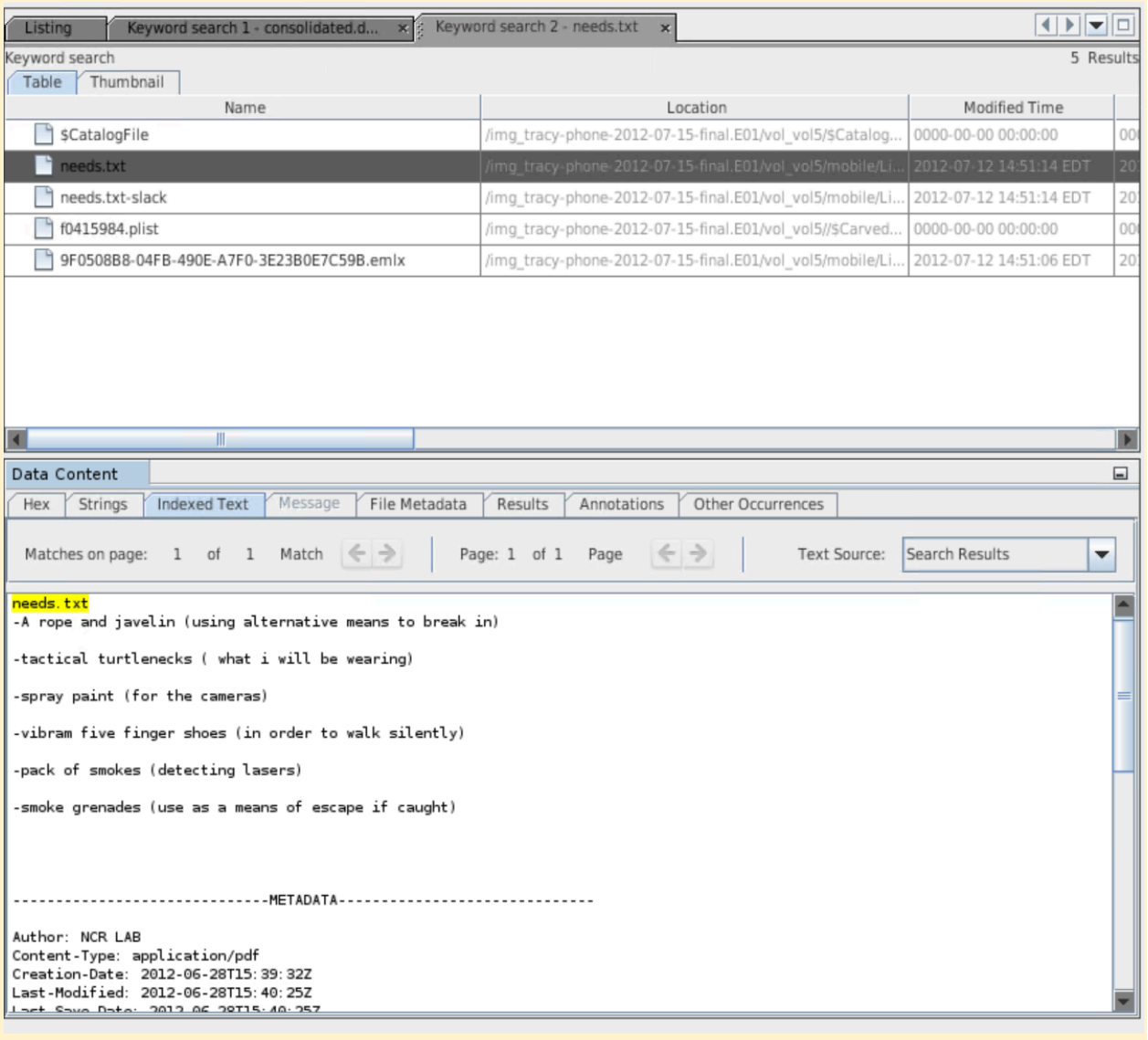
There was also found to be an mp3 file attached to an email that contained instructions on how to install a virtual machine using VirtualBox, which was intended to be used for the crime.

3 PDF attachments were found containing important information such as insurance documents, and art intended to be defaced.

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.

Many email messages and SMS messages found contained information that proves there were conspirators to this crime. They used tactful messaging in most of their communications but left behind evidence such as the mp3 file, and PDF files containing information pertaining to this crime, as well as a text file including the necessary items to carry out such a heist.



Plot Timeline

Tue, June 19 2012
Pat emails Tracy with an MP3 audio recording attachment that contains instructions on how to install a VirtualBox VM that is intended to be used later.

Fri, June 29 2012
Pat tells Tracy to use the VM for their future communication since it would be safer.

Mon, July 2 2012
Tracy asks Joe for help financially for Tracy's school tuition and Joe refuses unless Tracy is permitted to live with Joe.

Thu, July 5 2012
Tracy and Carry agree to meet at a restaurant named Bubba's Grill.

Fri July 6 2012
Pat arranges through email a proposition with someone who goes by "King" and Tracy.

Fri, July 6 2012
Tracy and Carry confirm the meeting at Bubba's restaurant over SMS messages again.

Mon, July 9 2012
Tracy sends an email to herself describing what stamps to steal, and how much value they are insured for.

Mon, July 9 2012
"King" sends a list of various items required to complete the heist to Pat.

Tue, July 10 2012
Pat forwards the list of requirements to Tracy.

Wed, July 11 2012
Carry and Tracy plan for Tracy to bring a tablet to Carry.

Thu, July 12 2012
Tracy texts Carry asking how the flashmob is going.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy uses the alias ‘Coral’ in email messaging
- Tracy and Pat conspired to these crimes along with a 3rd party with the name of ‘King’
- Tracy conspired with Carry to deliver a notebook containing data pertaining to a ‘flash mob’ that Carry intended to put together. The flash mob's purpose was to distract museum security while the crime was committed.
- Tracy had sent herself information related to the stamps and the value they are insured for.
- Tracy had snuck in Carry’s laptop, despite museum rules.
- While the flash mob was occurring, ‘King’ committed the theft.

Tracy’s possible motive could be financial since it was clear that Tracy was suffering financial issues in her SMS messages. Joe gave Tracy an ultimatum, either Terry lives with him or he won’t pay for Terry’s schooling, and Terry had made it clear she would prefer to stay with her father, as long as she was able to attend her school.

Appendix A: Correspondence Evidence

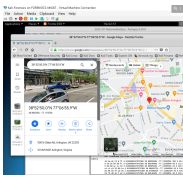
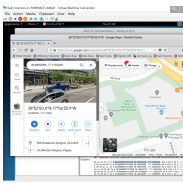
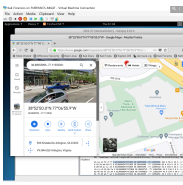
This subsection will provide an amalgamation of the email and SMS correspondence evidence.

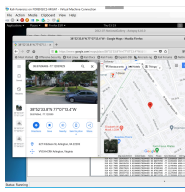
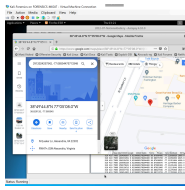
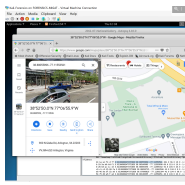
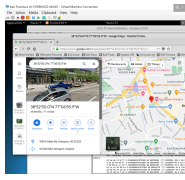
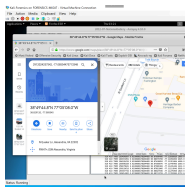
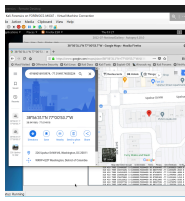
Master Timeline of NGDC				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Evidence Location**
1	Tue, 10 Jul 2012 11:24:57	F:patsumtwelve@gmail.com T:coralbluetwo@hotmail.com	Email agreeing to help carry out the heist, and what requirements they need in order to do so. Attached is a zip document containing the requirements.	Email Message
2	Fri, Jul 6 2012 11:49:31	F: patsumtwelve@gmail.com T: throne1966@hotmail.com CC: coralbluetwo@hotmail.com	Email describing the plan to commit a heist at the national gallery. ‘King’ is seemingly being blackmailed to help carry out the plan or the sender will tell King’s parole officer they have been dealing and doing drugs at work.	Email Message
3	N/A	Picture Attachment containing sensitive information	Important information pertaining to the cost of degrading specific pieces of art.	Email Attachment

4	N/A	Pat Phone Number: 1-571-308-3236	Pat texted Tracy to inform Coral to change the attachment sent to her to a PDF.	SMS
5	2012-07-10 11:19	F: throne1966@hotmail.com T: patsumtwelve@gmail.com Text File containing different items	'King' sends Pat a text file attachment including different items needed to complete the heist including: A rope & javelin, tactical turtlenecks, spray paint, vibram five finger shoes, pack of smokes, smoke grenades.	Email Attatchment
6	2012-07-10 08:24:58 -0700	F: patsumtwelve@gmail.com T: coralbluetwo@hotmail.com	Pat forwards the list that was sent from Tracy to Coral and informs her that those are the tools that will be required to complete the heist.	Email Message/Attachment
7	2012-06-19 21:38:59	F: perrypatsum@yahoo.com T:coralbluetwo@hotmail.com	"Hey Coral, 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! Perry Attachment: Crazydave1.mp3" **Mp3 is found to be modified and has instructions on how to install virtual machines.**	Email Message/ Attachment
8	2012-06-29 19:31:33	F: perrypatsum@yahoo.com T:coralbluetwo@hotmail.com	"Coral, Great, now that we have everything set up it would be better to do most of our communication here and on your new 'setup'. This might keep us a little bit safer. I know money is rough for both of us, so we may have to 'push the envelope' a bit. A few friends from around the office are really good about these types of things. If I find out anything interesting I will shoot you an email. In the meantime let's try to shoot some ideas and back and forth. Your friend, Perry"	Email Message
9	2012-07-02 16:13:18	F: coralbluetwo@hotmail.com T: perrypatsum@yahoo.com	"Perry, I think I may have come across something interesting. Everybody around the office seems to be buzzed about a foreign exhibit that	Email Message

			is supposed to be coming over. There hasn't been any official release in writing but we have been going through quite an ordeal with all this paperwork. From what I can tell, this exhibit has to be a big deal. I'll let you know if I found out anything else. Coral”	

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact #	**Timestamp**	**Header Information**	**Body**	**Map Screenshot**
1	06/13/2012 19:01:22	WifiLocation	Location: Virginia Tech Research Center (900 N Glebe Rd, Arlington VA, 22203)	
2	06/13/2012 19:04:03	WifiLocation	Location: Virginia Tech Research Center (900 N Glebe Rd, Arlington VA, 22203)	
3	07/02/2012 16:19:24	WifiLocation	Location: Virginia Tech Research Center (900 N Glebe Rd, Arlington VA, 22203)	

4	07/07/2012 16:31:27	WifiLocation	Location: Residential home (627 N Edison St, Arlington, VA 22203)	
5	07/10/2012 16:44:59	WifiLocation	Location: Pharmacy (1521 N Quaker Ln, Alexandria, VA 22302)	
6	06/13/2012 19:01:21	CellLocation	Location: Virginia Tech Research Center (900 N Glebe Rd, Arlington VA, 22203)	
7	07/02/2012	CellLocation	Location: Virginia Tech Research Center (900 N Glebe Rd, Arlington VA, 22203)	
8	07/10/2012 16:44:59	CellLocation	Location: Pharmacy (1521 N Quaker Ln, Alexandria, VA 22302)	
9	07/05/2012	CellLocationLocal	Location: 226 Upshur St NW #6, Washington, DC 20011	
10	07/08/2012	CellLocationLocal	Location: National Gallery of Art Sculpture Garden (7th St NW, Washington, DC 20004)