Case Report

National Gallery DC

### Tracy’s iPhone [2012-07-15-National-Gallery]

Table of Contents

1. Executive Summary
2. Equipment and Tools
3. Details of Tracy’s iPhone
4. Evidence to Establish Persons
5. Evidence relating to theft of valuable stamps
6. Evidence relating to defacement of museum art
7. Plot Timeline
8. Conclusion
9. Appendix A: Correspondence Evidence
10. Appendix B: WiFi and GPS Location Information

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 investigation, we can say that Tracy and his brother Pat, with the help of King, stole the stamps from the National Gallery.

### 

Equipment and Tools

We used Autopsy, an open-source forensic tool, which was installed on a Kali Linux VM.

Details of Tracy’s iPhone:

| **Name** | **Findings** | **Location in the iPhone image file** |
| --- | --- | --- |
| Model | 1-2 | vol\_vol5/logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelve’s iPhone | vol\_vol5//$CarvedFiles/f0463080.plist |
| OS Version | iPhone OS 4.2.1 (8C148) | vol\_vol5/logs/AppleSupport/general.log |
| Install Time | 6/6/2012 12:03:28 | vol\_vol5/logs/AppleSupport/general.log |
| User Email | tracysumtwelve@gmail.com, tracysumtwelve@nationalgallergydc.org | vol\_vol5/mobile/Library/Mail |
| Phone Number | +1 (703) 340-9661 | vol\_vol5/logs/lockdownd.log |
| Serial Number | 86004482Y2H | vol\_vol5/logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | vol\_vol5/logs/lockdownd.log |
| IMEI | 012021003735398 | vol\_vol5/root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | n/a |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | n/a |

Evidence to Establish Persons

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy:

Phone Number: +1 (703) 340-9961

Personal Email: tracysumtwelve@gmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused

Pat:

Phone Number: +1 (571) 308-3236

Email: patsumtwelve@gmail.com

perrypatsum@yahoo.com

Relationship: Tracy’s Brother

Terry:

Phone Number: +1 (703) 829-6071

Email: Unknown

Relationship: Tracy’s Daughter

Joe:

Phone Number: unknown

Email: joe.sum.twelve@gmail.com

Relationship: Tracy’s Ex-husband

Carry:

Phone Number: +1 (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Tracy’s Friend/Acquaintance

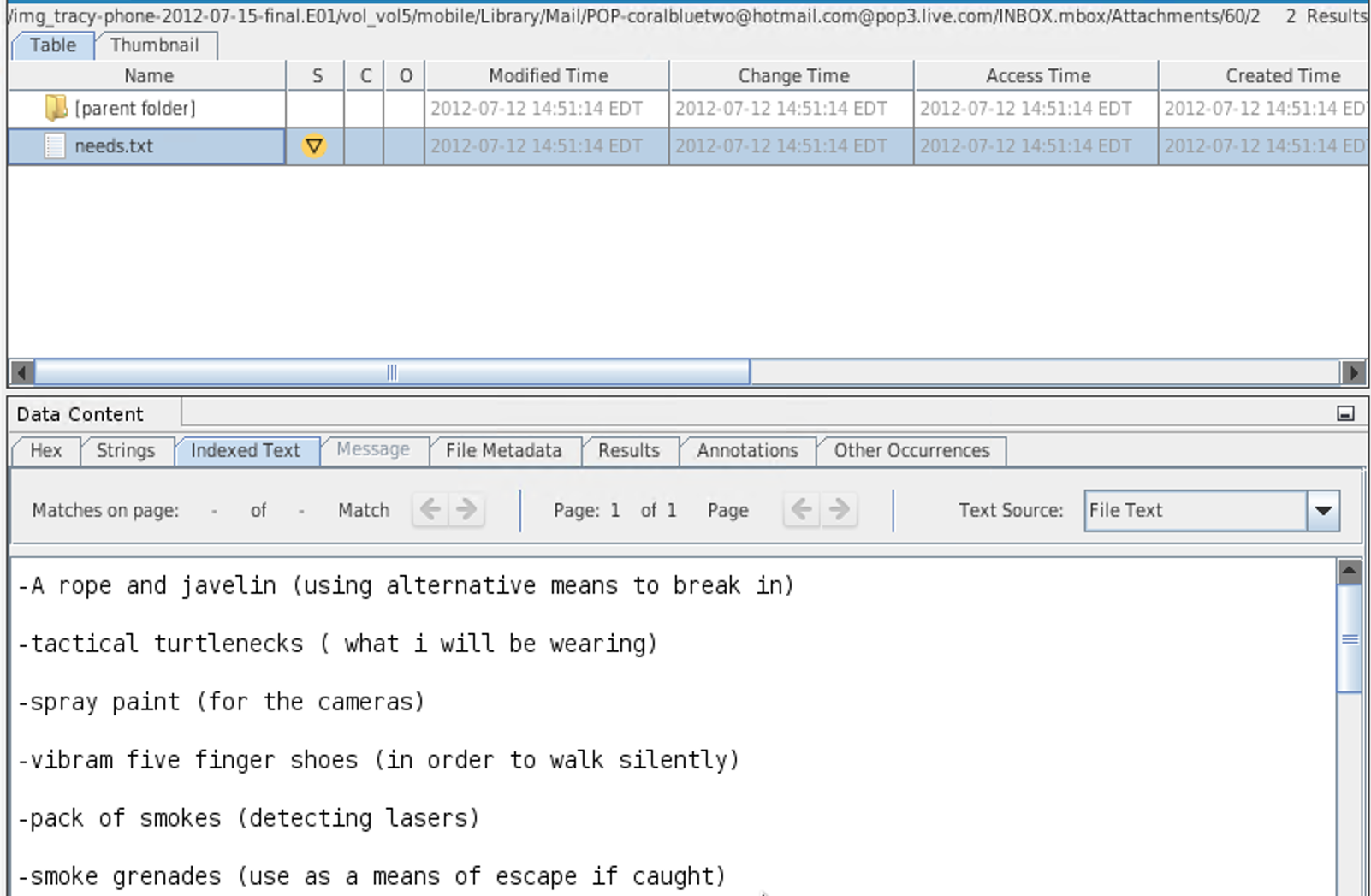
Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

From the email and text messages, it can be deduced that she was related to the theft of the valuable stamps. She also depicted in an email about which stamps to steal and sends the insurance documents related to the stamps.

In an email attachment we found needs.txt which lists the necessary things to steal the stamps.

Screenshot of the needs.txt



In an email, Tracy got instructions on how to install a VM on a computer which she used for this heist.

Evidence relating to defacement of museum art

I haven’t found any information about the defacement of museum art from Tracy’s iphone image.

Plot Timeline

| Time | Incident |
| --- | --- |
| Jun 19, 2012 at 14:38 | Pat emails Tracy on how to install VM |
| Jul 5, 2012 at 18:18:23 | Tracy and Carry agree to meet for lunch |
| Jul 9, 2012 at 10:44:11 | Tracy emails on which stamps to steal and insurances related to the stamps. |
| Jul 10, 2012 at 15:24:57 | Pat forwards a list of things necessary for the heist. |
| Jul 11, 2012 at 12:41:45 | Tracy meets Carry and delivers a tablet to Carry. |
| Jul 12 2012 at 17:06:45 | Tracy texts Carry asking how the flashmob is going. |

Conclusion

Tracy and Pat both used alias names, which are Coral and Perry, respectively. The email accounts Tracy and Pat used are coralbluetwo@hotmail.com and perrypatsum@yahoo.com. In order to steal the stamps, Pat contacted a criminal named King to get the necessary things to take with him. Tracy sends herself the insurance documents for the stamps that they want to steal. Carry organized a flash mob to distract the guard while other guys were stealing the stamps.

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. | Jun 19, 2012 21:38:59 | F: perrypatsum@yahoo.com (Pat)  T: coralbluetwo@hotmail.com (Tracy)  Subject: Crazydave by the VMs Attachment: Crazydave1.mp3 | Email:  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!  In this email actually Pat gave Tracy instruction on how to install VM on her computer | Mailbox Data Structure |
| 2. | Jul 6, 2012 15:49:31 | F: patsumtwelve@gmail.com  T: throne1966@hotmail.com  Cc:coralbluetwo@hotmail.com  Subject: can't pass up | Emails:  King,  Long time no see...I have a juicy proposition for you. Two weeks from now,  me and my associates are planning a heist at the national gallery.  Although, we need a helping hand. I know that you are on parole right now  and are probably hesitant to participate. Me and your parole officer go  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’s very easy for a person to phone the feds 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. | Mailbox Data Structure |
| 3. | Jul 9, 2012 14:44:11 | F: tracysumtwelve@gmail.com  T: coralbluetwo@hotmail.com  Subject: things | Email:  somethings  In this email attachment contains documents.zip which is encrypted ZIP folder containing 3 insurance documents related to stamps. | /mobile/Librar y/Mail/POP- coralbluetwo @hotmail.com @pop3.live.co m/INBOX.mbo x/Messages/8 A3BD06F- CDB1-4453- 9C69- 77E06823F2A E.emlx |
| 4. | Jul 10, 2012 15:24:57 | F: patsumtwelve@gmail.com  T: coralbluetwo@hotmail.com  Subject: Fwd: can't pass up  Attachment: needs.txt | Email Thread: cant’ pass up  You're too kind... I got you brotha. I need some tools in order to do this  job for you. Here are some requirements that i will need  King agrees to help with the heist and sends in a document with equipment required for it. The attached document is saved as a ‘txt’ file.  Pat forwards that email to Tracy (Coral)  this is what we need to get for the guy thats going to make our job happen  \*needs.txt is a pdf file which was saved with a wrong extension. | /mobile/Librar y/Mail/POP- coralbluetwo @hotmail.com @pop3.live.co m/INBOX.mbo x/Messages/9 F0508B8- 04FB-490E- A7F0- 3E23B0E7C5 9B.emlx |
| 5. | Jun 12, 2012  21:25:04 | F: Pat  T: Tracy | Message: What are you up to this weekend? | sms.db |
| 6. | Jun 13, 2012 17:30:28 | F: Terry  T: Tracy | Message: I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. | sms.db |
| 7. | Jun 13, 2012 18:30:38 | F: Tracy  T: Pat | Message: I don't have any big plans. How about you? | sms.db |
| 8. | Jun 13, 2012 18:33:46 | F: Tracy  T: Terry | Message: Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else? | sms.db |
| 9. | Jul 3, 2012 14:04:32 | F: Terry  T: Tracy | Message: moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools | sms.db |
| 10. | Jul 5, 2012 18:18:23 | F: Carry  T: Tracy | Message: Sounds good let's shoot for one àt Bubba s grill | sms.db |
| 11. | Jul 5, 2012 18:20:26 | F: Tracy  T: Carry | Message: Okay that sounds great. See you there | sms.db |
| 12. | Jul 6, 2012 15:02:19 | F: Tracy  T: Pat | Message: Hey can you give me a call | sms.db |
| 13. | Jul 6, 2012 15:08:37 | F: Pat  T: Tracy | Message: Sis I'm really busy can we can do this later | sms.db |
| 14. | Jul 6, 2012 15:11:54 | F: Tracy  T: Pat | Message: No pat this is important I need you to call me soon | sms.db |
| 15. | Jul 6, 2012 15:13:31 | F: Pat  T: Tracy | Message: Ok ok I'll call in 5 | sms.db |
| 16. | Jul 6, 2012 16:27:16 | F: Carry  T: Tracy | Message: I have a table inside | sms.db |
| 17. | Jul 6, 2012 16:27:50 | F: Tracy  T: Carry | Message: Okay brt | sms.db |
| 18. | Jul 7, 2012  19:36:35 | F: Unknown  T: Tracy | Message: 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 |
| 19. | Jul 10, 2012 15:26:19 | F: Pat  T: Tracy | Message: hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know | sms.db |
| 20. | Jul 10, 2012 15:58:04 | F: Tracy  T: Pat | Message: Sure thing I'll get on it | sms.db |
| 21. | Jul 10, 2012 17:18:38 | F: Tracy  T: Terry | Message: Going to lunch. You want to go????! | sms.db |
| 22. | Jul 10, 2012 18:19:24 | F: Tracy  T: Terry | Message: Back at work | sms.db |
| 23. | Jul 10, 2012 18:58:24 | F: Terry  T: Tracy | Message: I'm busy. Maybe this weekend if dad isn't busy | sms.db |
| 24. | Jul 11, 2012 12:41:45 | F: Carry  T: Tracy | Message: I'm almost there where should I meet you? | sms.db |
| 25. | Jul 11, 2012 12:49:08 | F: Tracy  T: Carry | Message: Just meet me out front, I'll take the tablet in. | sms.db |
| 26. | Jul 12, 2012  17:06:45 | F: Tracy  T: Carry | Message: How's the flashmob going | sms.db |
| 27. | Jul 13, 2012 1:02:10 | F: Terry T: Tracy | Message: I really want to go to Dad's this weekend. He said he'll take me shopping for school | sms.db |

### 

Appendix B: WiFi and GPS Location Information

*WiFi locations gathered from /vol5/root/Library/Caches/locationd/consolidated.db and plotted using maps.google.com*

The csv file of the location data is share [here](https://drive.google.com/file/d/1-LVFN2W2VbDD25HiQ0p2hq9vdndyzynw/view?usp=sharing).

