

Case Report

National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

[Evidence relating to theft of valuable stamps](#)

[Evidence relating to defacement of museum art](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[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 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.

My forensic team collected information from Tracy's iPhone 3 to aid in the case against her involving the National Gallery. The iPhone's data file tracy-phone-2012-07-15-final.E01 was extracted from her device on June 29, 2022, and this report lays out our findings.

Equipment and Tools

- Autopsy 4.19.3 on Windows 10 was used to ingest the phone's data file for examination
- DB Browser (SQLite) 3.12.2 was used to view extracted .db files
- Google Earth used inside Google Chrome was used to find locations of GPS information
- MD5 and SHA-256 hashes were made of the file to protect integrity

Details of Tracy's iPhone

- Device Model: iPhone 1,2 (Potentially iPhone 3G)
- OS Version: iPhone OS 4.2.1 (8C148)
- Serial Number: 86004482Y7H
- Host Name: Tracy Sumtwelve's iPhone
- Install Time: 6/6/2012 19:03:28
- Phone Number: (703) 340-9661
- Email Addresses: tracysumtwelve@gmail.com , tracysumtwelve@nationalgallerydc.org
- IMEI: 012021003735398
- ICCID: 89014103255195342366

This information can be found in the following sections of the extracted data:

- /mobile/Library/Logs/AppleSupport/general.log
- /logs/lockdown.log.1
- /root/Library/Lockdown/activation_records/wildcard_record.plist
- vol5/mobile/Library/Mail

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
Alias Email: coralbluetwo@hotmail.com
Relationship: Accused

Pat (Perry):

Phone Number: (571) 308-32364
Email: perrypatsum@yahoo.com
Relationship: Tracy's brother and Terry's Uncle

Terry:

Phone Number: (703) 829-6071
Relationship: Tracy's Daughter

Joe:


Email: joe.sum.twelve@gmail.com
Relationship: Tracy's Husband (Going through a divorce currently)

Carry:

Phone Number: (202) 725-2124
Email: carriesum2012@yahoo.com
Relationship: Acquaintance of Tracy

Tracy is also Coral. We found this out by finding the discussion between Pat and Tracy. Articles 1-6 show this conversation develop. Those articles also show that Pat's alias is Perry.

These articles refer to this evidence sheet:

 Week 21 HW Chris Rogers - Email + SMS Correspondence Evidence

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.


Article 7 shows that Tracy is going to try and find a way to make some additional money since Terry didn't want to change schools and Tracy can't afford it anymore. Article 10 shows the first sign of something happening for them to put their plan into action. Article 13 confirms it is a valuable stamp collection that will be at the exhibit at the Gallery and there is mention of a heist. In Article 18 Tracy emails her alias email the insurance files on the stamps. These show the stamps' value. Those insurance forms can be seen here:

[Insurance Forms](#)

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.

To pull off the heist they needed a distraction. They are planning a flash mob (Article 19) and are going to get Carry to help sneak in a tablet for it (Article 20). King sends a list of things needed to take on the heist (Article 21). The list can be seen here from the file needs.txt (it needed to be saved as a PDF to view it properly):

 needs.pdf

Images were found on Tracy's iPhone with pictures of the stamps. Those can be viewed here:

[43375-100APPLE](#)

Plot Timeline

- Tracy can't afford private tuition any more and asks her brother Pat for any ideas.
- Aliases and VMs were set up for secrecy. Tracy was Coral and Pat was Perry.
- Tracy discovered that some valuable stamps were coming as an exhibit to the gallery.
- Pat threatened King about his parole so he would help with the heist.
- King sent over a list of needed items for the heist.
- Tracy gained information about the security guard shifts.
- Carry is working with King to deface the art by bringing in a flash mob
- King is planning the flash mob as a distraction while the heist takes place.


Conclusion

Evidence found on Tracy's iPhone indicated the following:

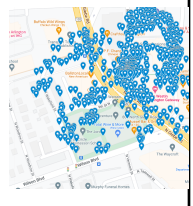
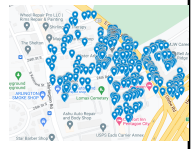
- Photos of stamps (Articles 50-53)
- List of supplies for heist ([needs.pdf](#))
- Stamp insurance PDFs ([Insurance Forms](#))
- Pat suggesting they use aliases and VMs to keep the info secret (Article 6 & 7)
- Emails discussing a heist and talking about the stamps (Article 13)

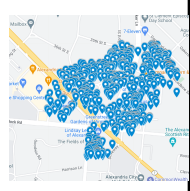
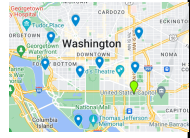
Appendix A: Correspondence Evidence

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

 Week 21 HW Chris Rogers - Email + SMS Correspondence Evidence

Appendix B: WiFi and GPS Location Information

| Location Information | | | | |
|----------------------|-----------|---------------------------------|--|---|
| Artifact # | Timestamp | Header Information | Body | Map Screenshot |
| 1 | | Wifi Coords.csv | Tracy spent time in three main hotspots. This is her wifi tracking location. |  |
| 2 | | | |  |

| | | | | |
|---|--|---------------------------------|--|---|
| 3 | | | |  |
| 4 | | Cell Coords.csv | Cell phone data puts her in these same 3 locations but also all around the gallery. The bright green pin is the gallery's location, and the blue is her cell phone location information. |  |