Case Report

National Gallery DC

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

# Table of Contents

[Case Report](#_8mjg1w2w81ai)

[National Gallery DC](#_lrib8gqk2z7b)

[Tracy’s iPhone [2012-07-15-National-Gallery]](#_219o4hryceis)

[Table of Contents](#_786gzvga2e8h)

[Executive Summary](#_ccs3x82xm1tu)

[Equipment and Tools](#_hw4rzs3hh4tn)

[Details of Tracy’s iPhone](#_ebsdggfieq5h)

[Evidence to Establish Personas](#_qixiazcd0tiw)

[Evidence relating to theft of valuable stamps](#_5ri2s3hfb3bw)

[Evidence relating to defacement of museum art](#_kt32233q8aao)

[Plot Timeline](#_nz1crxu2ypd4)

[Conclusion](#_m5r3zcqmj9ou)

Appendix A: [Correspondence Evidence](#_w4pkinqwxqi8)

Appendix B: [WiFi and GPS Location Information](#_f8fx30pgaw29)

# 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.

* Using Tracy’s phone image we were able to find various different logs from text messages, emails, GPS locations, WiFi information, and several other pieces of information that prove relevant to this case.
* Tracy has been having an ongoing communication with her brother Pat, Carry and King.
* SMS messages between Tracy, Carry, Pat and King revealed the conspiracy.
* IP address information that indicates GPS location data.
* Emails and email addresses that contain incriminating evidence.
* analyzing Tracy’s GPS coordinates and WiFi information revealed that she has been going around and stealing valuable stamps from various different locations, as well as evidence of the defacement of museum art.

### Equipment and Tools

| **Name** | **Description** | **Version** |
| --- | --- | --- |
| Autopsy Digital Forensics | End-to-end open-source digital forensics suite: features web artifact analysis, disk image analysis, hash filtering, data carving, IoC scan media devices using STIX | 4.17.0  (Release) |
| DB Browser for SQLite | Is an extension that loads databases to be viewed, browsed, edited and rendered. | 3.12.1 |
| Free EMLX Viewer | Built-in viewer suite that previews all EMLX files. Preview emails and its associated attachments types. ie: **.ppt, images, .docs etc**. |  |
| Microsoft Office (Excel) | Used to import/export data into spreadsheets or worksheets for further analysis and results | 2102 (Build 13801.20266) |
| Nano Text Editor | Linux text editor utility to open, read and edit basic and configuration text files | 5.6.1 |
| iPhone Forensic Image: Important Databases and Files | Document list of common devices of directories |  |
| Windows Media Player | Media player and media library used for playing audio, video and viewing images | 12.0.19041.844 |

# Details of Tracy’s iPhone

| **Name** | **Findings** | **Location in iPhone image file** |
| --- | --- | --- |
| Model | iPhone 3G | /mobile/Library/logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelve’s iPhone | /logs/lockdownd.log.1 |
| OS Version | iPhone OS. 4.2.1(8C148) | /mobile/Library/Logs/AppleSupport/general.log |
| Install Time | 6/6/2012 19:03:28 | /mobile/Library/Logs/AppleSupport/general.log |
| User Email | tracysumtwelve@gmail.com | vol5/mobile/Library/Mail |
| Phone Number | (703)340-9661 | /logs/lockdownd.log.1 |
| Serial Number | 86004482Y7H | /mobile/Library/Logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | /logs/lockdownd.log.1 |
| IMEI | 012021003735398 | /root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | |

# 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

Relationship: Tracy’s Brother

Terry:

Phone Number: (703)8296071

Email:

Relationship: Daughter

Joe:

Phone Number:

Email: joe.sum.twelve@gmail.com

Relationship: Ex-Husband

Carry:

Phone Number: (202)7252124

Email: [carrysum2012@yahoo.com](mailto:carrysum2012@yahoo.com)

Relationship: Hired by Tracy to deface artifacts in the Museum

Tracy works as a supervisor at the National Gallery and is an acquaintance of Carry. Carry contacts Tracy and starts communicating small data as a back and forth under the auspices that Carry wants to organize a Flash mob at the gallery and needs a little help. Carry will give money to Tracy for this help. Items transferred are suspicious in nature but not outright illegal. Tracy’s money troubles help her overlook the suspicious nature of the requests. Tracy has been having an ongoing dialog with her brother about stealing stamps from the National Gallery.

# 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.

Based on our findings from running Autopsy against the devices, we discovered a need.txt file (AppendixA:artifact#21) with a list of tools needed to conduct the burglary. This email was sent from Pat to Tracy’s “Coral Blue” alias account.

Furthermore, there was another email sent from Tracy’s gmail account to her alias again containing a documents.zip file which contained malicious information related to the burglary (AppendixA:artifact#18 ).

Lastly, another email sent from Perry to Tracy’s alias email containing an mp3 file which we believe was an external form of communication regarding the burglary (AppendixA:artifact #3 ).

There are pictures of the stamps targeted for the heist on Tracey’s phone. Essentially, we looked very closely into Tracy’s alias account because we believe the masked account played an essential role in organizing the burglary.

# 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.

The Appendix A (Artifact 19, 20, 23) reveals involvement of Carry in accessing the Museum and its security details.

The Appendix A ( Artifacts 21,22, ) give the information about a need.txt document which is actually a pdf file with evidence relating to possible defacement of the museum art which was communicated between Tracy and Carry.

Tracy has access to her work computer, personal phone, and home computer which will relate to the conspiracy of the stolen stamps. Carry is technically savvy in that she knows about steganography tools and encryption. She hides many of her correspondence in steg files and encrypted files. She purchases a tablet computer and sets it up to use her catsumtwelve email account dealings with Alex, setting up the flash mob, Carry is interested in security, schedules, events, and locations where art will be displayed. Unfortunately for everyone involved, Joe, Tracy’s ex-husband, installed a keylogger onto her computer prior to the divorce to monitor Terry, discovers the conspiracy to commit theft and turns her into the police. This reveals the contact between Tracy and Carry leading to Carry’s Tablet and phone being seized as well revealing the separate defacing plot.

# Plot Timeline

Friday 6 JUL 2012 @ 11:49:31-Pat sent an email (patsumtwelve@gmail.com) to King (throne1966@hotmail.com), recruiting King for the heist. Tracy is cc’d as coralbluetwo@hotmail.com.

Sunday 8 JUL 2012-Tracy takes pictures of Stamps at the National Gallery for possible reconnaissance.

Tuesday 10 JUL 2012 @ 11:19AM- King agrees to take part in the heist and sends Pat a list of tools needed for the job.

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy used the alias Coral and Pat used the alias Perry.
* Tracy was in financial hardships.
* She had ongoing dialouge between Pat (Brother), Carry ( Ties with Alex) regarding theft of valuable and defacement of museum art.
* Tracy shared security info to carry.
* Tracy was communicating with King for helping the theft and defacement plan.

# Appendix A: Correspondence Evidence

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

Go to the link below:

<https://docs.google.com/document/d/194CMxRJLR7rPGMD9QPS14ZCSOqTLCSMR8VF3j1_vgk4/edit?usp=sharing>

# Appendix B: WiFi and GPS Location Information

<https://docs.google.com/document/d/1W3yoAZv-h-8cYKxA0RvY544dymP2xWIYPD3cmj2e1PY/edit?usp=sharing>