Case Report

National Gallery DC

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

# Table of Contents

[Case Report](#_lnxbz9)

[National Gallery DC](#_gjdgxs)

[Tracy’s iPhone [2012-07-15-National-Gallery]](#_30j0zll)

[Table of Contents](#_1fob9te)

[Executive Summary](#_3znysh7)

[Equipment and Tools](#_2et92p0)

[Details of Tracy’s iPhone](#_tyjcwt)

[Evidence to Establish Personas](#_3dy6vkm)

[Evidence relating to theft of valuable stamps](#_1t3h5sf)

[Evidence relating to defacement of museum art](#_4d34og8)

[Plot Timeline](#_2s8eyo1)

[Conclusion](#_17dp8vu)

Appendix A: [Correspondence Evidence](#_3rdcrjn)

Appendix B: [WiFi and GPS Location Information](#_26in1rg)

# 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. After careful analysis of the emails and text messages we were able to ascertain the names and information of everyone that Tracy has been working with, Pat (her brother), often referenced as “Perry”, and someone named Carry, along with her daughter and ex-husband, Joe. On top of this information, 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

The materials include disk images of hard drives and both logical and physical images of mobile devices. Network captures were performed using the SSLstrip tool, allowing for capture files to be available with and without encrypted SSL traffic.

# Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone 3 | /logs/AppleSupport/general.log |
| Host Name | Tracy-Sumtwelves-iPhone | /preferences/SystemConfiguration/preferences.plist |
| OS Version | iPhone OS 4.2.1 | /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](mailto:tracysumtwelve@gmail.com)  [coralbluetwo@hotmail.com](mailto:coralblue2@hotmail.com)  [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org) | /mobile/library/mail |
| Phone Number | 703-340-9661 | /logs/lockdownd.log |
| Serial Number | 86004482Y7H | /logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | /logs/lockdownd.log |
| IMEI | 012012003735398 | /root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | Provided by Junior Investigator |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | Provided by Junior Investigator |

# 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: Divorced Mother

Pat:

Phone Number: (571) 308-3236

Email: perrypatsum@gmail.com

Relationship: Tracy’s brother

Terry:

Phone Number: (703) 829-6071

Email:

Relationship: Daughter of Tracy and Joe

Joe:

Phone Number:

Email: joe.sum.twelve@gmail.com

Relationship: Father of Terry

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Shares family ties with Alex (criminally involved character)

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 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. 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. 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.

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:

To conclude our findings, we discovered that there was malicious activity happening against the National Gallery DC art museum. After seizing devices and going through network logs, we discovered from text messages and email activity that Tracy, who works as a supervisor at the National Gallery was operating under the alias name Coral. Coral also had her own alias email address (coralbluetwo@hotmail.com) to communicate details of the burglary. Another malicious actor was Tracy’s own brother whom she had an ongoing dialog with regarding stealing Stamps from the National Gallery. Pat, Tracy’s brother is a police officer of the D.C. Enforcers Bureau. He is very devoted to his sister and niece Terry, to this point he isn’t an outright criminal, but walks the line very closely. He busted King with some items that were against his parole, but hasn’t arrested him on the promise of a future “favor.” Pat was under the alias name “Perry.”

# Appendix A: Correspondence Evidence

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Master Timeline of NGDC | | | | |
| Artifact # | Timestamp | Header Information | Key Information | Evidence Location |
| 1 | 06-19-2012 14:38:59 (PDT) | **Subject**: Crazydave by the VMs  **From**: Perry Patsum [perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)  **To**: Coral Bluetwo coralbluetwo@hotmail.com | Perry is acknowledging Coral's email and is suggesting her to check out a new song “by the VMs.” MP3 filename crazydave1.mps | NA |
| 2 | 09-09-2012 07:47:58 | **Subject**: things  **From**: Tracy Sumtwelve [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  **To**: coralbluetwo@hotmail.com | There is a zip file called documents.zip in the message contents. | NA |
| 3 | 09-10-2012 08:24:58 | Subject: Fwd: can’t pass up  Original Sender: King kthings throne1966@hotmail.com  From: Pat TeeSumTwelve  [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  To: coralbluetwo@hotmail.com | Plain text: You’re too kind.. I got you brotha. I need some tools in order to do this job. Here are some requirements that I will need: see attachment. Found: need.txt with a list of tools that indicate a burglary. | /mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E..... |
| 4 | NA | Sender #: 2069100932 | This number sent an advertising text message promoting a business. We believe this is the fraudulent number. | sms.db |
| 5 | NA | Sender #: 7038296071 | We discovered Terry’s number since there was a text message indicating that she cannot afford private school anymore. | sms.db |

# Appendix B: WiFi and GPS Location Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location Information | | | | |
| Artifact # | Timestamp | Header Information | Body | Map Screenshot |
| A1 | 08JUL201212:49:37 PM | Butterfly Stamp, Kazakstan | Picture of a Butterfly Stamp from Kazakstan | See A2, A3 |
| B1 | 08JUL201212:49:25 PM | Douglas MacArthur Stamp, USA | Picture of a Douglas MacArthur stamp from the USA. | See B2, B3 |
| C1 | 08JUL201212:49:49 PM | Armed Forces Reserve Stamp, USA | Picture of an Armed Forces Reserve stamp from the USA. | GPS coordinates not captured, see C2 |
| D1 | 08JUL201201:00:07 PM | Blue Stamp, Origin unknown | Stamp depicting a woman’s profile. The stamp is blue in color. | See D2, D3 |