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.

Tracy and her husband Joe have fallen on tough times and are in the middle of splitting up. With the split up Tracy can no longer afford to send their daughter (Terry) to her private school. Because she is unable to afford the school costs Tracy sets up a plan to steal a set of valuable stamps from her work (The National Gallery DC) to try and pay for her daughter's private schooling. She enlisted the help of her brother (Pat/Perry) and acquaintance (Carry) who is a Krovnovian supporter.

### Equipment and Tools

Kali linux box- Used to run the tools

Keylogger- Installed by Joe before the divorce to monitor this wife and daughter.

Autopsy- Used to analyze the captured iphone

Sqlite- Used as a more human friendly display for the data

# Details of Tracy’s iPhone

| **Name** | **Findings** | **Location in iPhone image file** |
| --- | --- | --- |
| Model | Iphone 1 or 2 | /mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelve’s iPhone | /mobile/Library/Logs/AppleSupport/general.log |
| 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, tracysumtwelve@nationalgallergydc.org | vol5/mobile/Library/Mail |
| Phone Number | (703) 340-9661 | vol5/mobile/Library/Mail |
| 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: Brother

Terry:

Phone Number: (703) 829-6071

Email:

Relationship: Daughter

Joe:

Phone Number:

Email: joe.sum.twelve@gmail.com

Relationship: Husband

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Acquaintance

All names, numbers, and email addresses came from sms messages, emails, and address book.

# 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.

In artifact #2 You can see that Pat is blackmailing King into helping with the heist of the stamps and forwarding it on to Tracy. Artifact #3 Tracy emails the insurance documents on the stamps to herself. Artifact #29-30 puts Tracy at The National Gallery.

# 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.

In deleted logs you can see that on google plus Carry suggested Alex as a friend who is a Krovnovian who is set to embarrass the United states and has family ties to Carry. Carry set up the flash mob to act as a distraction form the real crime going on.

# Plot Timeline

See Appendix A for timeline

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy (aka Coral) hit financial troubles with coming divorce
* Tracy enlisted the help of her brother (Pat aka Perry) to help her steal stamps from The National Gallery DC
* Pat blackmailed King into helping with the heist
* Tracy involved her acquaintance Carry in on the plan
* Tracy did not know what Carry and Alex had planned for the same time.

# 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 | 6/19/2012 21:38:59 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Crazydave by the VMs Attachment: Crazydave1.mp3 | Pat emailed Tracy an .mp3 file instructing her to check out the base also indicating that it is not an average .mp3 file. | Messages/3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx |
| 2 | 7/6/2012 15:49:31 | F: patsumtwelve@gmail.com  T: throne1966@hotmail.com  Cc:coralbluetwo@hotmail.com  Subject: can't pass up | Pat emails King blackmailing him into the heist using his parole and drugs as leverage | Messages/9 F0508B8- 04FB-490E- A7F0- 3E23B0E7C5 9B.emlx |
| 3 | 7/9/2012 14:44:11 | F: tracysumtwelve@gmail.com  T: coralbluetwo@hotmail.com  Subject: things  Attachment: documents.zp | Tracy sent a zip file containing insurance documents about the stamps. | Messages/8 A3BD06F- CDB1-4453- 9C69- 77E06823F2A E.emlx |
| 4 | 7/10/2012 15:24:57 | F: patsumtwelve@gmail.com  T: throne1966@hotmail.com  Subject: Fwd: can't pass up  Attachment: needs.txt | King agrees and sends “needs.txt” which is a list of tools needed. | Messages/9 F0508B8- 04FB-490E- A7F0- 3E23B0E7C5 9B.emlx |
| 5 | 6/12/2012 21:25:04 | F: Pat  T: Tracy | Pat asks Tracy about her plans for the weekend | SMS |
| 6 | 6/13/2012 17:30:28 | F: Terry  T: Tracy | I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. T | SMS |
| 7 | 6/13/2012 18:30:38 | F: Tracy  T: Pat | Tracy replies to Pats message saying that she has no big plans and enquires about his plans. | SMS |
| 8 | 6/13/2012 18:33:46 | F: Tracy  T: Terry | Ok, sounds good. | SMS |
| 9 | 7/3/2012 14:04:32 | F: Terry T: Tracy | Terry replies back saying that she doesn’t want to switch schools and would rather stay with her dad and continue at Prufrock | SMS |
| 10 | 7/5/2012 18:18:23 | F: Carry T: Tracy | Carry sets up the time and location as 1pm at Bubba’s grill for meeting with Tracy | SMS |
| 11 | 7/5/2012 18:20:26 | F: Tracy T: Carry | Tracy confirms the meeting time and location | SMS |
| 12 | 7/6/2012 15:02:19 | F: Tracy T: Pat | Tracy asks Pat to give her a call | SMS |
| 13 | 7/6/2012 15:08:37 | F: Pat T: Tracy | Pat says he is busy and suggests calling later | SMS |
| 14 | 7/6/2012 15:11:54 | F: Tracy T: Pat | Tracy says its important and insists that pat call her soon | SMS |
| 15 | 7/6/2012 15:13:31 | F: Pat T: Tracy | Pat says he will call in 5 min | SMS |
| 16 | 7/6/2012 15:18:50 | F: Pat T: Tracy | Pat calls Tracy and they speak for 4 min 4 secs. | SMS |
| 17 | 7/6/2012 16:27:16 | F: Carry  T: Tracy | Carry messages saying she has a table inside | SMS |
| 18 | 7/6/2012 16:27:50 | F: Tracy  T: Carry | Tracy replies back saying that she will be there. | SMS |
| 19 | 7/10/2012 15:26:19 | F: Pat  T: Tracy | Pat messages Tracy telling her about the email and informing that the attachment needs to be changed to pdf. He asks Tracy to tell this information to Coral. | SMS |
| 20 | 7/10/2012 15:58:04 | F: Tracy  T: Pat | Tracy acknowledges the email and message. | SMS |
| 21 | 7/10/2012 16:37:09 | F: Tracy T: Pat \*Failed | Tracy tried to share the following location with Pat over MMS message but it failed. Location: 2600-2700 24th Rd S, Arlington, VA 22206 | SMS |
| 22 | 7/10/2012 17:18:38 | F: Tracy T: Terry | Tracy messages Terry for Lunch | SMS |
| 23 | 7/10/2012 18:19:24 | F: Tracy T: Terry | Tracy messages Terry that she is back at work. | SMS |
| 24 | 7/10/2012 18:58:24 | F: Terry T: Tracy | Terry messages Tracy saying she is busy and suggests meeting up over the weekend if her dad isn’t busy. | SMS |
| 25 | 7/11/2012 12:41:45 | F: Carry T: Tracy | Carry messages Tracy informing that she is almost there (National Gallery) | SMS |
| 26 | 7/11/2012 12:49:08 | F: Tracy T: Carry | Tracy replies to Carry asking her to meet out front. She says that she will take the tablet in. | SMS |
| 27 | 7/13/2012 1:02:10 | F: Terry T: Tracy | I really want to go to Dad's this weekend. He said he'll take me shopping for school | SMS |

### 

### 

# Appendix B: WiFi and GPS Location Information

### 

| Location Information | | | |
| --- | --- | --- | --- |
| Artifact # | Timestamp | Body | Map Screenshot |
| 28 | 2012-06-23 17:12:16 | 38.904866342, -77.04837378 |  |
| 29 | 2012-07-08 16:34:40 | 38.89174787, -77.02346272 |  |
| 30 | 2012-07-08 16:39:10 | 38.89089193, -77.02163135 |  |
| 31 | 2012-07-10 16:47:12 | 38.82876277, -77.08593607 |  |

### 