Case Report

National Gallery DC

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

**Team Members**:

Chris Duke

Chris Garcia

Donathan Williams

Isidro Collazo

John Elliott

Michael Lynn

Mikhail Erick

Shea Padilla

# 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 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.

Performed a Digital Forensics analysis of Tracy’s phone. Inside was evidence of conspiracy to commit insurance fraud with several other accomplices assisting in the crime.

### **Equipment and Tools**

Programs and tools used were:

* Kali Linux
* Autopsy Digital Forensics
* Sqlite Browser

How Programs and tools were utilized:

* The files needed for providing evidence were extracted from Autopsy and then displayed on the Sqlite Browser for further evidence gathering.

# 

# Details of Tracy’s iPhone

# Case Name: 2012-07-15-National-Gallery

# Case #: 1EZ215-P

## Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone (1-2) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelves iphone | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| OS Version | iPhone OS 4.2.1 (8C148) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Install Time | 6/6/2012 19:03:28 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| User Email | [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  tracysumtwelve@nationalgallergydc.org | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail |
| Phone Number | +1 (703) 340-9661 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Serial Number | 86004482Y7H | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log.1 |
| IMEI | 01202 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | History.plist, under the FILE METADATA |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | History.plist, under the FILE METADATA |

# 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](mailto:tracysumtwelve@gmail.com)

Work Email: [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org)

Relationship: Accused, Alias is Coral

**Pat**:

Phone Number: (571) 308-3236

Email: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com), Alias email [perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)

Relationship: Accomplice, in the SMS.db Pat references Tracy as sis (Brother to the accused)

**Terry**:

Phone Number: (703)829-6071

Email: N/A

Relationship: Accomplice, Tracy’s daughter

**Joe**:

Phone Number: N/A

Email: [joe.sum.twelve@gmail.com](mailto:joe.sum.twelve@gmail.com)

Relationship: Accomplice, Currently in divorce proceedings with Tracy

**Carry**:

Phone Number: (202) 275-2124

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

Relationship: Accomplice, Co-worker in the museum

**King**:

Phone number: N/A

Email: [Throne1966@hotmail.com](mailto:Throne1966@hotmail.com)

Relationship: Acquaintance of Pat and they met in jail and currently being blackmailed

The accused individuals attempted to commit $289k worth of stamp insurance theft fraud.

# 

# **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.

* Path: /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Media/DCIM/100APLE
  + right click on image and open with External Viewer and there are pictures of the stamps that were going to be stolen
* Path:/img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@[pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs](http://pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs)
  + contains 3 Stamp Insurance PDF email file attachments

# **Evidence relating to defacement of museum art**

Path: /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail/IMAP-tracysumtwelve@gmail.com@[irnap.gmail.com/INBOX.irnap.gmail.com/Messages](http://irnap.gmail.com/INBOX.irnap.gmail.com/Messages)

**\*Please refer to the iPhone evidence folder for pictures of stamps to be defaced.**

# **Plot Timeline**

Please reference the worksheet dates and timelines for the order of events which are listed in Appendix A & B.

# **Conclusion**

Evidence found on Tracy’s iPhone indicated the following:

* Tracy used family members to steal expensive stamp collection and collect insurance money to pay for Terry’s(her daughters’) expensive school (Prufrock) tuition.
* Carry bribed Tracy to sneak in a tablet to record and post online a flash mob at the art gallery in hopes to deface and embarrass the Gallery

# 

# Appendix A: Correspondence Evidence

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

**Please reference EMAILS TIMELINE, SMS Timeline and Details of Tracy’s iPhone**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | EMAILS | | | |
| Artifact # | Timestamp | Header Information | | Body | Map Screenshot | |
| E1 |  | From:[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  to:tracysumtwelve@gmail.com  SUB:Paris Speak and Answer | | Email about using Alias’ | Graphical user interface, text, application, email  Description automatically generated |
| E2 |  | From:perrypatsum@yahoo.com  to:coralbluetwo@hotmail.com  SUB:hey sis | | Email about dinner and planning | Graphical user interface, text, application  Description automatically generated | |
| E3 |  | From:perrypatsum@yahoo.com  to:coralbluetwo@hotmail.com  SUB:Whats going on | | Tracy AKA Coral says nothing interesting turned up, but will soon. Pat AKA Perry says they can get the job done | Graphical user interface, text, application, email  Description automatically generated | |
| E4 |  | From:perrypatsum@yahoo.com  to:coralbluetwo@hotmail.com  SUB:some good news | | Tracy tells pat she found a foreign exhibit. She thinks it could be important. Perry replies feeling hopeful about it | Graphical user interface, text, application, email  Description automatically generated | |
| E5 |  | From:perrypatsum@yahoo.com  to:coralbluetwo@hotmail.com  SUB:some good news | | Tracy says the exhibit is worth alot of money, shipping cost is low | Graphical user interface, text, application, email  Description automatically generated | |
| E6 |  | From:perrypatsum@yahoo.com  to:coralbluetwo@hotmail.com  SUB:some good news | | Tracy tells Pat the exhibit is a valuable stamp collection. Pat starts planning heist | Graphical user interface, text, application, email  Description automatically generated | |
| E7 |  | From:carrysum2012@yahoo.com  to:tracysumtwelve@hotmail.com  SUB:Long time no see | | Carry emails Tracy about lunch. Mentions Faebook and hard times | Graphical user interface, text, application, email  Description automatically generated | |
| E8 |  | From:[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  to:tracysumtwelve@gmail.com  SUB:good news | | Tracy emails pat about coral and her job and needs pat to catch up. Pat mentions King | Graphical user interface, text, application  Description automatically generated | |
| E9 |  | From:[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  to:[tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  CC:coralbluetwo@hotmail.com  SUB:cant pass up | | Pat emails King about heist, blackmails with tipping off feds about drugs | Graphical user interface, text, application, email  Description automatically generated | |
| E10 |  | From:[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  to:tracysumtwelve@gmail.com  SUB:good news | | Tracy suggests a meetup with pat and king. Login creds for [coralblue@hotmail.com](mailto:coralblue@hotmail.com)  Password: legalBee | Graphical user interface, text, application, email  Description automatically generated | |
| E11 |  | From:tracysumtwelve@gmail.com  to:coralbluetwo@hotmail.com  SUB:things | | Zip files labelled documents and docs that contain attachments with insurance forms | Graphical user interface, text, application, email  Description automatically generated | |
| E12 |  | From:carrysum2012@yahoo.com  to:tracysumtwelve@hotmail.com  SUB:Long time no see | | Carry asks Tracy about sneaking in a tablet for the flash mob, tracy would be comp’d | Graphical user interface, text, application  Description automatically generated | |
| E13 |  | From:carrysum2012@yahoo.com  to:tracysumtwelve@hotmail.com  SUB:Long time no see | | Tracy agrees to Carry’s request | Graphical user interface, text, application, email  Description automatically generated | |
| E14 |  | From:[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  to:coralbluetwo@hotmail.com  SUB:cant pass up | | King agrees to be part of heist. There is an attachment called needs.txt with a list of tools | Graphical user interface, text, application, email  Description automatically generated | |
| E15 |  | From:carrysum2012@yahoo.com  to:tracysumtwelve@hotmail.com  SUB:Long time no see | | Carry asks about Guard scheduling. Tracy gives Carry info of guards shifts | Graphical user interface, text, application, email  Description automatically generated | |
| E16 |  | From:Google+  to:tracysumtwelve@hotmail.com  SUB:Carry | | Carry adds Tracy to her Google+ circle | Graphical user interface, text, application, email  Description automatically generated | |
| E17 |  | From:Google+  to:tracysumtwelve@hotmail.com  SUB:Carry | | Carry shared an album with Tracy | Graphical user interface, text, application  Description automatically generated | |
| E18 |  | From:carrysum2012@yahoo.com  to:tracysumtwelve@hotmail.com  SUB:Long time no see | | Carry accidentally email Tracy about “it will be gun”. Carry meant “it will be fun” | Graphical user interface, text, application, email  Description automatically generated | |
|  |  |  | |  | **/img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail/Protected Index** | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SMS | | | | |
| Artifact # | Timestamp | Header Information | Body | Map Screenshot |
| SMS1 | 6/12/2012  @ 21:25:04 | From:Pat  To:Tracy | Pat asks Tracy about weekend plans | Graphical user interface, application  Description automatically generated |
| SMS2 | 6/13/2012  @ 17:30:28 | From:Terry  To:Tracy | Terry is telling Tracy about getting pizza with her dad. Tells her to not cook | Graphical user interface, application  Description automatically generated |
| SMS3 | 6/13/2012  @ 18:30:38 | From:Tracy  To:Pat | Tracy tells Pat she has no plans and asks what his plans are | Graphical user interface, application  Description automatically generated |
| SMS4 | 6/13/2012  @ 18:33:46 | From:Tracy  To:Terry | “ Ok, Sounds good. “ | Graphical user interface, application  Description automatically generated |
| SMS5 | 7/3/2012  @ 13:41:51 | From:Tracy  To:Terry | Tracy asks Terry to think about switching schools since Prufrock is too expensive | Graphical user interface, application  Description automatically generated |
| SMS6 | 7/3/2012  @ 14:04:32 | From:Terry  To:Tracy | Terry tells Tracy she wants to stay at Prufrock and wants to stay with her dad | Graphical user interface, application  Description automatically generated |
| SMS7 | 7/5/2012  @ 18:18:23 | From:Carry  To:Tracy | Carry tells Tracy to meet her at Bubba’s grill at 1pm | Graphical user interface, application  Description automatically generated |
| SMS8 | 7/5/2012  @ 18:20:26 | From: Tracy  To:Carry | Confirms meeting | Graphical user interface, application  Description automatically generated |
| SMS9 | 7/6/2012  @ 15:02:19 | From:Tracy  To:Pat | Tracy tells Pat to call her | Graphical user interface, application  Description automatically generated |
| SMS10 | 7/6/2012  @ 15:08:37 | From:Pat  To:Tracy | Pat replies he is busy and will call later | Graphical user interface, application  Description automatically generated |
| SMS11 | 7/6/2012  @ 15:11:54 | From:Tracy  To:Pat | Tracy says to Pat to call her quick, implying urgency | Graphical user interface, application  Description automatically generated |
| SMS12 | 7/6/2012  @ 15:13:31 | From:Pat  To:Tracy | Pat will call Tracy within a 5min time frame | Graphical user interface, application  Description automatically generated |
| SMS13 | 7/6/2012  @ 16:27:16 | From:Carry  To:Tracy | Carry tells Tracy she is inside at a table | Graphical user interface, application  Description automatically generated |
| SMS14 | 7/6/2012  @ 16:27:50 | From:Tracy  To:Carry | Tracy tells Carry she is on her way | Graphical user interface, application  Description automatically generated |
| SMS15 | 7/10/2012  @ 15:26:19 | From:Pat  To:Tracy | Pat Tells Tracy about changing an Attachment to a PDF file format and to also inform Coral | Graphical user interface, application  Description automatically generated |
| SMS16 | 7/10/2012  @ 15:58:04 | From:Tracy  To:Pat | Confirmation from Tracy about Pats text | Graphical user interface, application  Description automatically generated |
| SMS16 | 7/10/2012  @ 16:37:09 | From:Tracy  To:Pat | Failed Location Sharing with MMS | Graphical user interface, application  Description automatically generated |
| SMS18 | 7/10/2012  @ 17:18:38 | From:Tracy  To:Terry | Tracy asks Terry to lunch | Graphical user interface, application  Description automatically generated |
| SMS19 | 7/10/2012  @ 18:19:24 | From:Tracy  To:Terry | Tracy tells Terry she is at work | Graphical user interface, application  Description automatically generated |
| SMS20 | 7/10/2012  @ 18:54:24 | From:Terry  To:Tracy | Terry tells Tracy she is busy and recommends meeting during the weekend | Graphical user interface, application  Description automatically generated |
| SMS21 | 7/11/2012  @ 21:41:45 | From:Carry  To:Tracy | Carry tells Tracy she is close to the National Gallery |  |
| SMS22 | 7/11/2012  @ 21:49:08 | From:Tracy  To:Carry | Tracy tells Carry to meet outside the exchange the tablet |  |
| SMS23 | 7/12/2012  @ 17:06:45 | From:Tracy  To:Carry | Tracy asks Carry about the Flash Mob |  |
| SMS24 | 7/13/2012  @ 13:02:10 | From:Carry  To:Tracy | Terry wants to go to her Fathers (Joe) over the weekend and that Joe will take her shopping for school |  |
| NOTES1 | Opened with sqlitebrowser - notes.sqlite and found under screenshots |  | “ You need to find help for Prufrock “ |  |

# Appendix B: WiFi and GPS Location Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location Information | | | | |
| Artifact # | Timestamp | Header Information | Body | Map Screenshot |
| GRID1 | -6/13/2012  @ 19:01:21  -7/2/2012  @ 16:19:24  -7/3/2012  @ 13:42:42  -7/5/2012  @ 16:32:47 | Cell & WIFI location  -root/Library/Caches/locationd/consolidated.db | 900 N Glebe Rd, Arlington, VA 22203 | Graphical user interface, application, map  Description automatically generated |
| GRID2 | 7/10/2012  @ 16:31:10, @ 16:36:51 | Cell & WIFI location  -root/Library/Caches/locationd/consolidated.db | Apartment Building | Graphical user interface, application, map  Description automatically generated |
| GRID3 | 7/10/2012  @ 16:44:59  @ 16:45:01  @ 16:46:29  @ 16:47:12 | Cell & WIFI location  -/img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Maps/Directions.plist | CVS Pharmacy | Graphical user interface, application, map  Description automatically generated |
| GRID4 | See Apple Timestamp Information Below(last Pic) | Cell & WIFI location  -root/Library/Caches/locationd/consolidated.db | Jordan Apartments  801 N Wake St, Arlington, VA 22203 | Graphical user interface, application, map  Description automatically generated |
| GRID5 | See Apple Timestamp Information Below(last Pic) | Cell & WIFI location  -root/Library/Caches/locationd/consolidated.db | Continential at Ballston  851 N Glebe Rd Arlington VA 22203 | Graphical user interface, application, map  Description automatically generated |
| GRID6 | See Apple Timestamp Information Below(last Pic) | Cell & WIFI location  -root/Library/Caches/locationd/consolidated.db | Office Building with multiple businesses  4420 Fairfax Dr, Arlington, VA 22203 | Graphical user interface, application  Description automatically generated |
| GRID7 | See Apple Timestamp Information Below(last Pic) | Cell & WIFI location  -root/Library/Caches/locationd/consolidated.db | The Weston Arlington Gateway  801 N Glebe Rd, Arlington, VA 22203 | Graphical user interface, application, map  Description automatically generated |

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated