| Cybersecurity |
| --- |
| 21.3 The Final Report |

Case Report

National Gallery DC

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

John Mercer

# Table of Contents

[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)

[Appendix C: Photographic Evidence](#_wayy6bz2ml05)

# 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.

Based on email, SMS, and text information, Tracy Sumtwelve conspired with her brother Pat and an associate of Pat’s known by King to steal rare and valuable stamps from the National Gallery in Washington, D.C.

### Equipment and Tools

Tracy’s iPhone image was captured using Encase and analyzed using Autopsy version 4.10.0. Selected contents were additionally reviewed using SQLiteBrowser version 3.10.1 and Microsoft Excel version 2207 build 16.0.15427.20182.

# Details of Tracy’s iPhone

| **Name** | **Findings** |
| --- | --- |
| Model | iPhone1 or iPhone 2 |
| Host Name | Tracy Sumtwelve’s iPhone |
| OS Version | iPhone OS 4.2.1 (8C148) |
| Install Time | 6/6/2012 12:03:28 -0700 |
| User Emails | [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com) [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  tracy.sumtwelve@nationalgallerydc.org |
| Phone Number | (703) 340-9661 |
| Serial Number | 86004482Y7H |
| ICCID | 89014103255195342366 |
| IMEI | 012021003735389 |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 |

Data obtained from:

1. vol\_vol5/logs/AppleSupport/general.log
2. vol\_vol5/logs/lockdownd.log
3. vol\_vol5/mobile/Library/Mail/Envelope Index
4. vol\_vol5/mobile/Library/Mail
5. vol\_vol5/logs/lockdownd.log
6. vol\_vol5/root/Library/Lockdown/activation\_records/Wildcard\_record.plist

# 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)

coralbluetwo@hotmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused of planning stamp theft

The phone belongs to Tracy and contains an address book, SMS text messages, and an email box for the [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) email address with mail messages. There are also mailboxes for [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org) and [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com), but these contain no relevant email messages.

Pat:

Phone Number: (571) 308-3236

Email: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)

perrypatsum@yahoo.com

Relationship: brother of Tracy, accomplice for planning stamp theft

There is an entry for Pat in the address book, as well as phone calls, SMS messages, and email messages from Pat on the phone.

Terry:

Phone Number: (703) 829-6071

Email:

Relationship: child of Tracy

There is an entry for Terry in the address book as well as SMS text messages.

Joe:

Phone Number:

Email:

Relationship: Spouse of Tracy (divorcing) and father of Terry.

There are references to Joe in SMS messages from Terry, but no direct communications between Joe and Tracy are documented on this phone.

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: acquaintance of Tracy

There is an entry for Carry in the address book as well as SMS text messages.

King:

Phone Number:

Email: [throne1966@hotmail.com](mailto:throne1966@hotmail.com)

Relationship: acquaintance of Pat, accomplice for planning stamp theft

There are email correspondences between Pat and King that are forwarded to Tracy.

Tracy and Joe are separated and in the process of divorce. Their daughter Terry goes to Prufrock school, but it is expensive and Tracy cannot afford it any more. Joe offers to pay for the school but only if Terry lives with him.

Pat is Tracy’s brother.

# 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.

7/6/2012 Tracy asks Pat to call (artifacts 6, 7, 8, & 9). They have a 4 minute & 4 second call (artifact 10). Pat then emails King about a planned heist at the National Gallery (artifact 11).

7/9/2012 Tracy emails (artifact 14) from her personal account to the alias account a document (artifact 15) with the insurance policies (artifacts 16, 17, & 18) for nine of the stamps in the display at the National Gallery totalling $260,000.

7/10/2021 King replies in email (artifact 19) that he will assist in the heist and supplies a list of needed items (artifact 20). Pat forwards this list on to Tracy (artifact 21). Pat texts Tracy (artifact 22) that the list file extension needs to be changed. Tracy replies via text that she will “get on it” (artifact 23).

# 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.

7/5/2012 Tracy and Carry agree to meet at Bubba’s grill (artifacts 4 & 5)

7/11/2012 Tracy and Carry agree to meet “out front” to take the tablet in (artifacts 24 & 25).

7/13/2012 Tracy asks Carry how the flashmob is going (artifact 26).

# Plot Timeline

7/5/2012 Tracy and Carry agree to meet at Bubba’s grill (artifacts 4 & 5)

7/6/2012 Tracy asks Pat to call (artifacts 6, 7, 8, & 9). They have a 4 minute & 4 second call (artifact 10). Pat then emails King about a planned heist at the National Gallery (artifact 11).

7/9/2012 Tracy emails (artifact 14) from her personal account to the alias account a document (artifact 15) with the insurance policies (artifacts 16, 17, & 18) for nine of the stamps in the display at the National Gallery totalling $260,000.

7/10/2021 King replies in email (artifact 19) that he will assist in the heist and supplies a list of needed items (artifact 20). Pat forwards this list on to Tracy (artifact 21). Pat texts Tracy (artifact 22) that the list file extension needs to be changed. Tracy replies via text that she will “get on it” (artifact 23).

7/11/2012 Tracy and Carry agree to meet “out front” to take the tablet in (artifacts 24 & 25).

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy used the alias Coral and had access to the email address [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) on her phone.
* Tracy sent information about the stamps’ value to “Coral” via email.
* Pat used the alias Perry Patsum once in an email, but primarily used the personal email address patsumtwelve@gmail.com.
* Tracy asked Pat for help in planning a heist of the stamps from the museum.
* Pat asked “King” for help in the heist knowing he is on parole and violating his conditions.
* “King” agrees to help and sends a list of equipment he will need.
* Tracy agrees to get the equipment.

# Appendix A: Correspondence Evidence

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

| **Master Timeline of NGDC** | | | | |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Header Information** | **Key Information** | **Evidence Location** |
| 1 | 6/19/2012 14:38 | F: Perry Patsum <[perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)>  T: Coral Bluetwo <[coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)>  S: Crazydave by the VMs | Hey Coral,  Just got your email. That took longer than expected!  Oh well! You've got to check out this new song by the VMs.  I love the base. Tell me what you think!  Perry  attachment: Crazydave1.mp3 | Mailbox data structure |
| 2 | 7/3/2012 13:41 | F: Tracy  T: Terry | Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else? | SMS |
| 3 | 7/3/2012 14:04 | F: Terry  T: Tracy | moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools :( | SMS |
| 4 | 7/5/2012 18:18 | F: Carry  T: Tracy | Sounds good let's shoot for one àt Bubba s grill | SMS |
| 5 | 7/5/2012 18:20 | F: Tracy  T: Carry | Okay that sounds great. See you there | SMS |
| 6 | 7/6/2012 15:02 | F: Tracy  T: Pat | Hey can you give me a call | SMS |
| 7 | 7/6/2012 15:08 | F: Pat  T: Tracy | Sis I'm really busy can we can do this later | SMS |
| 8 | 7/6/2012 15:11 | F: Tracy  T: Pat | No pat this is important I need you to call me soon | SMS |
| 9 | 7/6/2012 15:13 | F: Pat  T: Tracy | Ok ok I'll call in 5 | SMS |
| 10 | 7/6/2012 15:18 | F: Pat  T: Tracy | call, duration 244 seconds (4 minutes, 4 seconds) | Call log |
| 11 | 7/6/2012 15:49 | F: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  T: [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  CC: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  S: can't pass up | King,  Long time no see...I have a juicy proposition for you. Two weeks from now,  me and my associates are planning a heist at the national gallery.  Although, we need a helping hand. I know that you are on parole right now  and are probably hesitant to participate. Me and your parole officer go  years back. He is a very strict fellow. If he were to find out that you  were dealing drugs and shooting dope in your veins every night, i feel he  wouldn’t be too happy. It’s very easy for a person to phone the feds an  anonymous tip that you are on drugs and the location of your stash. All  they have to do is give you a drug test and since you're on parole, the  feds don’t need a search warrant. Well hit me up. You know where to find  me. | Mailbox data structure |
| 12 | 7/6/2012 16:27 | F: Carry  T: Tracy | I have a table inside | SMS |
| 13 | 7/6/2012 16:27 | F: Tracy  T: Carry | Okay brt | SMS |
| 14 | 7/9/2012 10:44 | F: [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  T: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  S: things | no message.  Attachment: documents.zip | Mailbox data structure |
| 15 | 7/9/2012 10:44 | documents.zip | Stamp insurance 1.pdf  Stamp insurance 2.pdf  Stamp insurance 3.pdf | Mailbox data structure |
| 16 | 7/9/2012 10:44 | Stamp insurance 1.pdf | Insurance policy x23654 covering stamps  Lot # 25 Armed Forces Reserve $43,000.00  Lot #26 Stamp of Kazakstan2 $29,000.00  Lot # 27 BradyCo. $12,000.00 | Mailbox data structure |
| 17 | 7/9/2012 10:44 | Stamp insurance 2.pdf | Insurance policy x23654 covering stamps  Lot # 11 Woman’s Profile $31,000.00  Lot # 12 Stamp of Kazakstan $29,000.00  Lot # 13 1929 Napal $27,000.00 | Mailbox data structure |
| 18 | 7/9/2012 10:44 | Stamp insurance 3.pdf | Insurance policy x23654 covering stamps  Lot #1 Douglas MacArther $35,000.00  Lot # 2 Nederland $30,000.00  Lot # 3 Mongolia $24,000.00 | Mailbox data structure |
| 19 | 7/10/2012 11:19 | F: King kthings <[throne1966@hotmail.com](mailto:throne1966@hotmail.com)>  T: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  S: RE: can't pass up | "You're too kind... I got you brotha. I need some tools in order to do this  job for you. Here are some requirements that i will need:  see attachment  attachment: needs.txt" | Mailbox data structure |
| 20 | 7/10/2012 11:19 | Needs.txt [actually a PDF file per artifact 22] | -A rope and javelin (using alternative means to break in)  -tactical turtlenecks ( what i will be wearing)  -spray paint (for the cameras)  -vibram five finger shoes (in order to walk silently)  -pack of smokes (detecting lasers)  -smoke grenades (use as A means of escape if caught) | Mailbox data structure |
| 21 | 7/10/2012 11:24 | F: Pat TeeSumTwelve <[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)>  T: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  S: Fwd: can't pass up | this is what we need to get for the guy thats going to make our job happen  attachment: needs.txt" | Mailbox data structure |
| 22 | 7/10/2012 15:26 | F: Pat  T: Tracy | hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know | SMS |
| 23 | 7/10/2012 15:58 | F: Tracy  T: Pat | Sure thing I'll get on it | SMS |
| 24 | 7/11/2012 12:41 | F: Carry  T: Tracy | I'm almost there where should I meet you? | SMS |
| 25 | 7/11/2012 12:49 | F: Tracy  T: Carry | Just meet me out front, I'll take the tablet in. | SMS |
| 26 | 7/12/2012 17:06 | F: Tracy  T: Carry | How's the flashmob going | SMS |

# Appendix B: WiFi and GPS Location Information

The Wifi location data on the phone has 2005 data points, but essentially only 5 different timestamps:

6/13/2012 19:01:22

7/3/2012 13:42:43

7/5/2012 16:31:12

7/10/2012 16:31:12

7/12/2012 16:45:02

For each timestamp, there are anywhere from 150 to 650 GPS locations recorded. Samples from each timestamp are shown below.

The Cell tower location data on the phone has 376 data points, but essentially only 5 different timestamps:

6/13/2012 19:01:22

7/2/2012 16:19:23

7/5/2012 16:31:12

7/10/2012 16:31:12

7/12/2012 16:45:02

For each timestamp, there are anywhere from 40 to 120 GPS locations recorded. Samples from each timestamp are shown below.

### 

| **Location Information** | | | | |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Header Information** | **Body** | **Map Screenshot** |
| 1 | 6/13/2012 19:01:22 | Wifi location | 4501-4507 Wilson Blvd, Arlington, VA 22203 |  |
| 2 | 6/13/2012 19:01:22 | Cell location | 509 N Edison St, Arlington, VA 22203 |  |
| 3 | 7/3/2012 13:42:43 | Wifi location | 4501-4507 Wilson Blvd, Arlington, VA 22203 |  |
| 4 | 7/2/2012 16:19:23 | Cell location | 4223 Fairfax Dr, Arlington, VA 22203 |  |
| 5 | 7/5/2012 16:32:48 | Wifi location | 901 N Glebe Rd, Arlington VA 22203 |  |
| 6 | 7/5/2012 16:32:46 | Cell location | 843 N Buchanan St, Arlington, VA 22203 |  |
| 7 | 7/10/2021 16:31:12 | Wifi location | 2691 24th Rd S, Arlington, VA 22206 |  |
| 8 | 7/10/2021 16:31:11 | Cell location | 2915-2923 23rd St S, Arlington, VA 22206 |  |
| 9 | 7/10/2021 16:45:02 | Wifi location | 4110 36th St S, Arlington, VA 22206 |  |
| 10 | 7/10/2021 16:45:00 | Cell location | 1275 Mission Lane, Alexandria, VA 22304 |  |

### 

# Appendix C: Photographic Evidence

There are 30 photographs on the phone, all taken on 7/8/2012 between 12:33 pm and 1:02 pm.

Among them are several of stamps that appear to be the ones mentioned in the insurance documents (artifacts 16, 17, & 18).

| Filename | Timestamp | Photo | Address | Map Screenshot |
| --- | --- | --- | --- | --- |
| IMG\_0049.JPG | 7/8/2012 12:41 |  | National Gallery of Art – Sculpture Garden, Washington, DC 20408 |  |
| IMG\_0050.JPG | 7/8/2012 12:41 |  | National Gallery of Art – Sculpture Garden, Washington, DC 20408 |  |
| IMG\_0051.JPG | 7/8/2012 12:42 |  | National Gallery of Art – Sculpture Garden, Washington, DC 20408 |  |
| IMG\_0054.JPG | 7/8/2012 12:49 |  | National Fire Dog Monument,  600 5th St NW, Washington, DC 20001 |  |
| IMG\_0055.JPG | 7/8/2012 12:49 |  | National Fire Dog Monument,  600 5th St NW, Washington, DC 20001 |  |
| IMG\_0056.JPG | 7/8/2012 12:49 |  | National Fire Dog Monument,  600 5th St NW, Washington, DC 20001 |  |
| IMG\_0057.JPG | 7/8/2012 12:50 |  | National Fire Dog Monument,  600 5th St NW, Washington, DC 20001 |  |