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.

Based on the evidence shown below, it appears that Tracy and her brother Pat conspired with an unknown 3rd party with email address “King kthings [throne1966@hotmail.com](mailto:throne1966@hotmail.com)” to steal stamps from the National Gallery.

### Equipment and Tools

Digitech used the Autopsy open-source forensics tool on a Kali Linux host to analyze an image of Tracy’s iphone. Other websites and tools were also used (e.g. maps.google.com, etc.).

# Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone1,2 | vol5/logs/AppleSuport/general.log |
| Host Name | Tracy-Sumtwelves-iPhone | vol5/mobile/preferences/SystemConfiguration |
| OS Version | iPhone OS 4.2.1 (8C148) | vol5/logs/AppleSupport/general.log |
| Install Time | 6/6/2012 12:03:28 -0700 | vol5/logs/AppleSupport/general.log |
| User Email | IMAP: [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com) POP: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | vol5/mobile/Library/Mail/Envelope Index |
| Phone Number | 1 (703) 340-9661 | vol5/logs/lockdownd.log.1 |
| Serial Number | 86004482Y7H | vol5/logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | vol5/logs/lockdownd.log.1 |
| IMEI | 012021003735398 | vol5/root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | n/a (tracy-phone-2012-07-15-final.E01 image) |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | n/a (tracy-phone-2012-07-15-final.E01 image) |

# 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](mailto:perrypatsum@yahoo.com)  
 [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)

Relationship: Tracy’s brother

Terry:

Phone Number: (703) 829-6071

Email: unknown

Relationship: Tracy & Joe’s daughter

Joe:

Phone Number: unknown

Email: unknown

Relationship: Tracy’s ex-husband

Carry:

Phone Number: (202) 725-2124

Email: unknown

Relationship: Tracy’s accomplice and friend

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.

Emails and SMS messages were exchanged between Tracy, Pat, Carry, and an unnamed co-conspirator with email address “King kthings [throne1966@hotmail.com](mailto:throne1966@hotmail.com)” (referenced in Appendix A).

One email from “King kthings” contained an attachment with a list of items needed for the theft.

Graphical user interface, text, application

Description automatically generated

There was also an MP3 audio file attachment (Crazydave1.mp3) with covert instructions on how to install a VirtualBox VM on a host computer, which was to be used for this crime.

There was an SMS message notifying Tracy that she had received a $1000 Target Giftcard, with instructions to visit a misleadingly named website ([www.target.com**.trdt.biz**](http://www.target.com.trdt.biz)) with instructions to entre a numeric code followed by “where to ship it”. The website ‘trdt.biz’ domain is no longer registered by anyone, and it uses ‘www.target.com’ as a subdomain to hide the fact that it’s really a part of ‘trdt.biz’, and is not affiliated with the Target corporation.

There were 3 .pdf email attachments which were Memoranda of Insurance for various valuable stamps and photos of those stamps in the camera storage location (shown below).

In addition, there were photo images of each of the stamps listed in the insurance documents on the phone.

Stamp\_insurance1.pdf email attachment

Text, letter

Description automatically generated

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0056.JPG

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0051.JPG

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0057.JPG

A picture containing text, picture frame

Description automatically generatedA picture containing text, picture frame

Description automatically generatedA picture containing text, sign

Description automatically generated

Stamp\_insurance2.pdf email attachment

Text, letter

Description automatically generated

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0067.JPG

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0055.JPG

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0050.JPG

A picture containing text

Description automatically generatedA picture containing text, book

Description automatically generatedA picture containing text, rug

Description automatically generated

Stamp\_insurance3.pdf email attachment

Text, letter

Description automatically generated

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0054.JPG

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0065.JPG

/vol5/mobile/Media/DCIM/100APPLE/IMG\_0071.JPG

A picture containing text

Description automatically generatedA picture containing text

Description automatically generatedA picture containing text, old, stone

Description automatically generated

# 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.

**There was no evidence related to defacement of museum art in the iphone image**. Only evidence related to the theft of stamps.

# Plot Timeline

**For details please refer to Appendix A below and the section labelled ‘Evidence relating to theft of valuable stamps” above.**

* On Tue, Jun 19 2012 at 02:38 PM, Pat ([perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)) emails Tracy (coralbluetwo@hotmail.com) with an MP3 audio recording attachment that contains synthesized voice instructions on how to install a VirtualBox VM on her computer “for later use”.
* On Thu, Jul 5 2012 06:18:23 PM Tracy and Carry agree via SMS to meet at Bubba’s Grill
* Fri Jul 6 2012 11:49:31 AM Pat arranges via email with subject “can’t pass up”, a “proposition” with someone who goes by “King” ([throne1966@hotmail.com](mailto:throne1966@hotmail.com)) and Tracy.
* On Fri, Jul 6 2012 04:27:16 PM Tracy and Carry confirm the meeting at Bubba’s via SMS.
* On Sat, Jul 7 2012 07:36:35 PM, Tracy receives an SMS from an unknown number that she has received a Target Gift Card worth $1000 "Congratulations, your entry in last months drawing won you a FREE $1,000 Target Giftcard! Enter ""703"" at www.target.com.trdt.biz to tell us where to ship it". Note that the URL is faked to look like it’s related to Target Corp, but is a subdomain of trdt.biz, for which no registration can be found at this time. Presumably, this payment was received from Alex, but there is no proof.
* Mon, Jul 9 2012 10:44:11 AM Tracy sends herself an email describing which stamps to steal, and how much they are insured for.
* On Mon, Jul 9 2012 10:44:11 AM, Pat and “King” arrange via email a list of things that King will need to do the job.
* Tue, Jul 10 2012 11:24 AM, Pat forwards the list to Tracy.
* On Wed, Jul 11 2012 12:41:45 PM, Carry and Tracy arrange via SMS for Tracy to deliver a tablet to Carry.
* On Thu, Jul 12 2012 05:06:45 PM, Tracy texts Carry to ask how the flashmob is going.

Diagram

Description automatically generated

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy and Pat conspired with each other using email account aliases. Pat used ‘patsumtwelve@gmail.com’ and Tracy used ‘[coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)’. Pat’s usual email address is ‘[perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)’, and Tracy’s normal email address is ‘tracysumtwelve@gmail.com’
* Pat coordinated with a known criminal ‘King’ with email address ‘[throne1966@hotmail.com](mailto:throne1966@hotmail.com)’ to steal some valuable stamps. Pat knows King’s parole officer, so he was able to exert influence on King.
* Tracy conspires with Carry to deliver a notebook with data pertaining to a flashmob that Carry wants to organize. This would help to distract the museum’s security guards while King commits the theft.
* Tracy sends herself documents related to the stamps and how much they are insured for.
* Tracy is notified that a ‘Gift Card’ for $1000 has been set up for her. This is most likely payment from either Carry via Alex, or directly from Alex. The website URL is purposely crafted to look like it is from Target, but is actually located in the trdt.biz domain. No information on that URL is available at this time.
* There are three clusters of WiFi and Cell location info, but it’s not clear what the significance is. Further analysis would be needed to correlate the location info and timing with the email and SMS exchanges.

# Appendix A: Correspondence Evidence

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Master Timeline of NGDC | | | | |
| Artifact # | Timestamp (all GMT) | Header Information | Key Information | Evidence Location |
| 1 | Tue, Jun 12, 2012 9:25:04 PM | SMS from 571-308-3236 (Pat) | "What are you up to this weekend? " | /vol5/mobile/Library/SMS/sms.db |
| 2 | Tue, Jun 12, 2012 8:04:50 PM | Call from 650-887-0260 |  | /vol5/wireless/Library/CallHistory/call\_history.db |
| 3 | Tue, Jun 12, 2012 8:52:14 PM | Call from 703-829-6192 |  | /vol5/wireless/Library/CallHistory/call\_history.db |
| 4 | Wed, Jun 13, 2012 4:29:13 PM | Call to 571-308-3236 (Pat) |  | /vol5/wireless/Library/CallHistory/call\_history.db |
| 5 | Wed, Jun 13, 2012 5:30:28 PM | SMS from 703-829-6071 (Terry) | "I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook.  T" | /vol5/mobile/Library/SMS/sms.db |
| 6 | Wed, Jun 13, 2012 6:30:38 PM | SMS to 571-308-3236 (Pat) | "I don't have any big plans. How about you?" | /vol5/mobile/Library/SMS/sms.db |
| 7 | Wed, Jun 13, 2012 6:33:46 PM | SMS to 703-829-6071 (Terry) | "Ok, sounds good." | /vol5/mobile/Library/SMS/sms.db |
| 8 | Tue, Jun 19, 2012 02:38:59 PM | Email  F: Perry Patsum [perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)  T: Coral Bluetwo [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: Crazydave by the VMs  Attach: Crazydave1.mp3 | “Hey Coral, Just got your email. That took longer than expectd! Oh well! You’ve got to check out this new song by the VMs. I love the base. Tell me what you think!  **NOTE: from 1:21 to 2:34 in the mp3 file, there is a synthesized voice message from Perry to Tracy explaining how to install VirtualBox** | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/3896FC6F-A083-4D38-B0A2-CE68368D44CA.emlx |
| 9 | Fri, Jun 22, 2012 5:34:26 PM | Call to 571-245-8517 |  | /vol5/wireless/Library/CallHistory/call\_history.db |
| 10 | Tue, Jul 3 2012 01:41:51 PM | SMS to 703-829-6071 (Terry) | "Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?" | /vol5/mobile/Library/SMS/sms.db |
| 11 | Tue, Jul 3 2012 02:04:32 PM | SMS from 703-829-6071 (Terry) | "moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools :(" | /vol5/mobile/Library/SMS/sms.db |
| 12 | Thu, Jul 5 2012 06:18:23 P | SMS from 202-725-2124 (Carry) | "Sounds good let's shoot for one àt Bubba s grill" | /vol5/mobile/Library/SMS/sms.db |
| 13 | Thu, Jul 5 2012 06:20:26 PM | SMS to 202-725-2124 (Carry) | "Okay that sounds great. See you there" | /vol5/mobile/Library/SMS/sms.db |
| 14 | Thu, Jul 5 2012 12:58:41 PM | Email  F: [Woina.Honril@m57.biz](mailto:Woina.Honril@m57.biz)  T: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subj: Busy  Attach: 000001.doc  Attach: 000002.doc | “I didn’t”  **NOTE: The two attachments appear to be official government documents from the FCC and USDA** | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx |
| 15 | Fri, Jul 6 2012 03:02:19 PM | SMS to 571-308-3236 (Pat) | "Hey can you give me a call" | /vol5/mobile/Library/SMS/sms.db |
| 16 | Fri, Jul 6 2012 03:08:37 PM | SMS from 571-308-3236 (Pat) | "Sis I'm really busy can we can do this later" | /vol5/mobile/Library/SMS/sms.db |
| 17 | Fri, Jul 6 2012 03:11:54 PM | SMS to 571-308-3236 (Pat) | "  No pat this is important I need you to call me soon" | /vol5/mobile/Library/SMS/sms.db |
| 18 | Fri, Jul 6 2012 03:13:31 PM | SMS from 571-308-3236 (Pat) | "Ok ok I'll call in 5" | /vol5/mobile/Library/SMS/sms.db |
| 19 | Fri, Jul 6, 2012 3:18:50 PM | Call from 571-308-3236 (Pat) |  | /vol5/wireless/Library/CallHistory/call\_history.db |
| 21 | Fri, Jul 6 2012 04:27:50 PM | SMS to 202-725-2124 (Carry) | "Okay brt" | /vol5/mobile/Library/SMS/sms.db |
| 22 | Fri Jul 6 2012 11:49:31 AM | Email  F: patsumtwelve@gmail.com  T: [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  Cc: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: 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 drugs 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. | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx |
| 20 | Fri, Jul 6 2012 04:27:16 PM | SMS from 202-725-2124 (Carry) | "I have a table inside" | /vol5/mobile/Library/SMS/sms.db |
| 21 | Fri, Jul 6 2012 04:27:50 PM | SMS to 202-725-2124 (Carry) | "Okay brt" | /vol5/mobile/Library/SMS/sms.db |
| 23 | Sat, Jul 7 2012 07:36:35 PM | SMS from 206-910-0932 (unknown) | "Congratulations, your entry in last months drawing won you a FREE $1,000 Target Giftcard! Enter ""703"" at www.target.com.trdt.biz to tell us where to ship it" | /vol5/mobile/Library/SMS/sms.db |
| 24 | Mon, Jul 9 2012 10:44:11 AM | Email  F: Tracy Sumtwelve [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  T: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: things  Attach: documents.zip  Attach: docs.zip | Somethings  **NOTE1:** The attachment docs.zip contains 3 pdf files describing “stamp insurance” that totals $84k + $87k + $89k = $260k  **NOTE2:** The attachment documents.zip is a password protected file containing the same 3 .pdf files describing “stamp insurance”. The password ‘Hercules’ was discovered with fcrackzip | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx |
| 25 | Tue, Jul 10 2012 11:19 AM | Email  F: King kthings [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  T: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  Subject: RE: can’t pass up  Attach: needs.txt | 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  **NOTE: The attachment needs.txt reads:**  **-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)** | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx |
| 26 | Tue, Jul 10 2012 11:24 AM | Email  F: Pat TeeSumTwelve [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  T: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: Fwd: can’t pass up | “This is what we need to get for the guy that’s going to make our job happen” | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx |
| 27 | Tue, Jul 10 2012 03:26:19 PM | SMS from 571-308-3236 (Pat) | "hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know" | /vol5/mobile/Library/SMS/sms.db |
| 28 | Tue, Jul 10 2012 03:58:04 PM | SMS to 571-308-3236 (Pat) | "Sure thing I'll get on it" | /vol5/mobile/Library/SMS/sms.db |
| 29 | Tue, Jul 10 2012 05:18:38 PM | SMS to 703-829-6071 (Terry) | "Going to lunch. You want to go????!" | /vol5/mobile/Library/SMS/sms.db |
| 30 | Tue, Jul 10 2012 06:19:24 PM | SMS to 703-829-6071 (Terry) | "Back at work" | /vol5/mobile/Library/SMS/sms.db |
| 31 | Tue, Jul 10 2012 06:58:24 P | SMS from 703-829-6071 (Terry) | "I'm busy. Maybe this weekend if dad isn't busy" | /vol5/mobile/Library/SMS/sms.db |
| 32 | Wed, Jul 11 2012 04:18:03 | Email  F: [microsoft@reply.digitalriver.com](mailto:microsoft@reply.digitalriver.com)  To: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subj: Only 30 days left! Start a free Office trining course now. | *--Commercial spam – not relevant.--* | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/01FE9965-A923-40CF-A78A-72CE3BD26571.emlx |
| 33 | Wed, Jul 11 2012 12:41:45 PM | SMS from 202-725-2124 (Carry) | "I'm almost there where should I meet you? " | /vol5/mobile/Library/SMS/sms.db |
| 34 | Wed, Jul 11 2012 12:49:08 P | SMS to 202-725-2124 (Carry) | "Just meet me out front, I'll take the tablet in." | /vol5/mobile/Library/SMS/sms.db |
| 35 | Thu, Jul 12 2012 05:06:45 PM | SMS to 202-725-2124 (Carry) | "How's the flashmob going" | /vol5/mobile/Library/SMS/sms.db |
| 36 | Fri, Jul 13 2012 01:02:10 AM | SMS from 703-829-6071 (Terry) | "I really want to go to Dad's this weekend. He said he'll take me shopping for school" | /vol5/mobile/Library/SMS/sms.db |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix B: WiFi and GPS Location Information

WiFi locations gathered from /vol5/root/Library/Caches/locationd/consolidated.db and plotted using maps.google.com

Map

Description automatically generated

Cell locations gathered from /vol5/root/Library/Caches/locationd/consolidated.db and plotted using maps.google.com

Map

Description automatically generated

Location of the National Gallery embedded in the cell location map.

Map

Description automatically generated