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

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 provided below, it was discovered a supervisor at the National Gallery, Tracy, was in coordination with her brother, Pat, to plan a stamp heist at the NGDC.

The heist was planned due to financial hardship for Tracy, stemming from the inability to pay tuition for her daughter, Terry, to attend Prufrock Preparatory School.

Tracy was utilizing the alias “Coral”, while her brother, Pat, was utilizing the alias “Perry”.

Further evidence indicates Tracy was aware of Pat’s attempts to recruit an individual by the name of “King” to help with the heist.

With the installation of a key logger on the family laptop, Joe, Tracy's ex-husband, discovers the conspiracy and informs authorities.

### Equipment and Tools

● Autopsy

● Kali Linux

● SQLite DB Browser

● Google Maps

● Nano (text editor)

### Details of Tracy’s iPhone

| **Name** | **Findings** | **Location in iPhone image file** |
| --- | --- | --- |
| Model | iPhone 1, 2 | general.log |
| Host Name | Tracy Sumtwelve’s iPhone | lockdownd.log |
| OS Version | iPhone OS 4.2.1 | general.log |
| Install Time | 6/6/2012 | general.log |
| User Email | [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com) [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | Envelope Index |
| Phone Number | (703) 340-9661 | lockdownd.log.1 |
| Serial Number | 86004482Y7H | general.log |
| ICCID | 89014103255195342366 | lockdownd.log.1 |
| IMEI | 012021003735398 | wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | cd /root/corpus/ | cat tracy.original.md5log.txt |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | cd /root/corpus/ | cat tracy.original.sha256log.txt |

# Evidence to Establish Personas

**This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.**

**Tracy:** (Alias: Coral Blue)

Phone Number: (703) 340-9961

Personal Email: [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)

Alias Email: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)

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

Relationship: Accused

**Pat:** (Alias: Perry)  
 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: N/A

Relationship: Tracy and Joe’s daughter

**Joe:**

Phone Number: N/A

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

Relationship: Terry’s father, Tracy’s ex-husband

**Carry:** (Alias: Cat)

Phone Number: (202) 725-2124

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

Relationship: Tracy’s friend/colleague

**King:** (Alias: Kart)

Phone Number: N/A

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

Relationship: Pat’s acquaintance

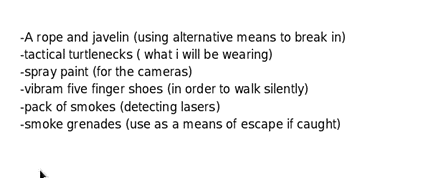
Email and SMS data collected from Tracy’s iPhone revealed Personal Identity Information and connections of all parties associated with the planned National Gallery heist.

# 

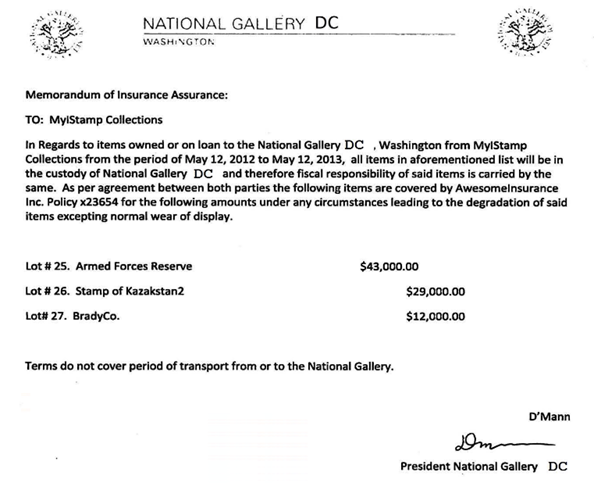
# Evidence relating to theft of valuable stamps

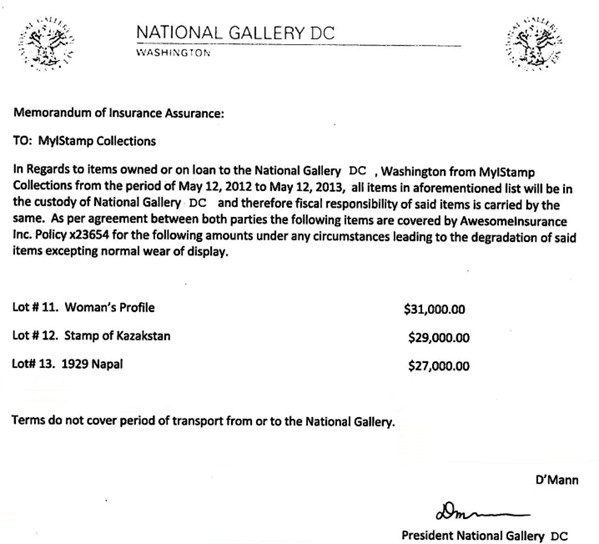
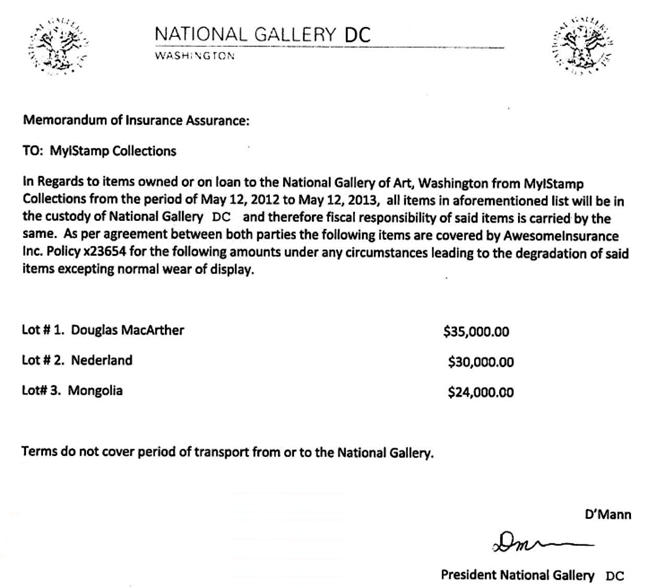
**This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.**

* Email and SMS messages were exchanged between Tracy, Pat, and “King” regarding plans for the heist. (Further referenced in Appendix A).
* An email from “King” contained an attachment with a list of items needed for the heist.



* An MP3 audio file attachment (Crazydave1.mp3) gives instructions on installing a VM to be used as cover for additional planning.
* Email attachments noted as ‘Memoranda of Insurance’ for various stamps were discovered in Mobile/Mail/Attachments:



* Photo images of the stamps associated with the insurance documents were discovered within the phone DCIM.  
  





# 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.**

* NGDC colleague, Carry, reached out to Tracy for lunch.
* Carry asks Tracy for help sneaking a tablet into the NGDC for a “flashmob” event.
* Carry mentions compensating Tracy for help. Tracy agrees.
* Carry asked Tracy for information on security shift changes in exchange for compensation. Tracy agrees.
* Tracy messaged Carry asking how the flash mob was going.
* Alleged “location scouting” images were discovered on Tracy’s phone:



* Aside from the tablet and security shift information exchange, it is believed Tracy has no further knowledge or involvement with the defacement.

# Plot Timeline

| **DATE** | **DESCRIPTION** |
| --- | --- |
| Tues, June 18, 2012 - 2:38pm | Pat sends Tracy information about installing a virtual machine. |
| Thurs, July 5, 2012 - 6:18pm | SMS between Tracy and Carry to meet at Bubba’s grill. |
| Fri, July 6, 2012 - 11:49am | Pat emails King about a proposition to heist the National Gallery. |
| Fri, July 6, 2012 - 4:27pm | Tracy meets with Carry at Bubba’s grill. |
| Sun, July 8, 2012 - 12:41pm | Tracy photographs specific stamps planned for the heist. |
| Mon, July 9, 2012 - 10:44am | Tracy emails herself “Memorandum of Insurance” for specific stamps. |
| Tue, July 10, 2012 - 11:19am | King emails Pat confirming tools needed for the heist. |
| Tue, July 10, 2012 - 11:24am | Pat emails Tracy confirming tools needed for the heist. |
| Wed, July 11, 2012 - 12:49pm | Tracy meets with Cary to bring the tablet in. |
| Thurs. July 11, 2012 - 5:06pm | Tracy asks Carry how the “flashmob” is going. |

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy and Pat colluded in planning a heist of valuable stamps at the NGDC.
* Tracy used the alias ‘Coral’, Pat used the alias ‘Perry’.
* Tracy’s motive was due to financial hardship, stemming from inability to pay tuition for her daughter, Terry.
* Pat coordinated with ‘King’, an acquaintance with a criminal past, to assist with the heist.
* Due to email exchanges, Tracy knew of Pat’s planning with King.
* Tracy knew the value of specific stamps due to saved “Memorandum of Insurance” documents and associated images on her phone.
* Tracy helped Carry smuggle a tablet into NGDC with data pertaining to a “flashmob”, along with security rotation information.
* Tracy had no other knowledge of a museum defacement.

# 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 | Tue, Jun 19, 2012 02:38:59 PM | Email From: Pat (Perry)  To: Tracy (Coral) Subject: Crazydave by the VMs Attachment: 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!  (Attachment includes VM install instructions) | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/ |
| 2 | Tue, Jul 3 2012 01:41:51 PM | SMS to 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 |
| 3 | Tue, Jul 3 2012 02:04:32 PM | SMS from 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 |
| 4 | Thu, Jul 5 2012 06:18:23 PM | SMS from Carry | "Sounds good let's shoot for one àt Bubba s grill" | /vol5/mobile/Library/SMS/sms.db |
| 5 | Thu, Jul 5 2012 06:20:26 PM | SMS to Carry | "Okay that sounds great. See you there" | /vol5/mobile/Library/SMS/sms.db |
| 6 | Fri, Jul 6 2012 03:02:19 PM | SMS to Pat | "Hey can you give me a call" | /vol5/mobile/Library/SMS/sms.db |
| 7 | Fri, Jul 6 2012 03:08:37 PM | SMS from Pat | "Sis I'm really busy can we can do this later" | /vol5/mobile/Library/SMS/sms.db |
| 8 | Fri, Jul 6 2012 03:11:54 PM | SMS to Pat | "  No pat this is important I need you to call me soon" | /vol5/mobile/Library/SMS/sms.db |
| 9 | Fri, Jul 6 2012 03:13:31 PM | SMS from Pat | "Ok ok I'll call in 5" | /vol5/mobile/Library/SMS/sms.db |
| 10 | Fri, Jul 6 2012 04:27:50 PM | SMS to Carry | "Okay brt" | /vol5/mobile/Library/SMS/sms.db |
| 11 | Fri Jul 6 2012 11:49:31 AM | Email  From: Pat  To: King  Cc: Tracy (Coral)  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. | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages |
| 12 | Fri, Jul 6 2012 04:27:16 PM | SMS from Carry | "I have a table inside" | /vol5/mobile/Library/SMS/sms.db |
| 13 | Fri, Jul 6 2012 04:27:50 PM | SMS to Carry | "Okay brt" | /vol5/mobile/Library/SMS/sms.db |
| 24 | Mon, Jul 9 2012 10:44:11 AM | Email  From: Tracy  To: “Coral”  Subject: things  Attachment: documents.zip  Attachment: docs.zip | Somethings  ([Attachments include “Memorandum of Insurance”](#_9c6c6bbwi88v)) | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages |
| 14 | Tue, Jul 10 2012 11:19 AM | Email  From: King  To: Pat  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: | /vol5/mobile/Library/Mail/POP-colralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/ |
| 15 | Tue, Jul 10 2012 11:24 AM | Email  From: Pat  To: “Coral”  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/ |
| 16 | Tue, Jul 10 2012 03:26:19 PM | SMS from 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 |
| 17 | Tue, Jul 10 2012 03:58:04 PM | SMS to Pat | "Sure thing I'll get on it" | /vol5/mobile/Library/SMS/sms.db |
| 18 | Wed, Jul 11 2012 12:41:45 PM | SMS from Carry | "I'm almost there where should I meet you? " | /vol5/mobile/Library/SMS/sms.db |
| 19 | Wed, Jul 11 2012 12:49:08 P | SMS to Carry | "Just meet me out front, I'll take the tablet in." | /vol5/mobile/Library/SMS/sms.db |
| 20 | Thu, Jul 12 2012 05:06:45 PM | SMS to Carry | "How's the flashmob going" | /vol5/mobile/Library/SMS/sms.db |

# Appendix B: WiFi and GPS Location Information

| **Location Information** | | | | |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Header Information** | **Body** | **Map Screenshot** |
| 1 | Sun. Jul 8, 2012 12:34 PM | Cell Location | National Gallery of Art – Sculpture Garden  38°53'30.0"N 77°01'24.6"W  Constitution Ave NW &, 7th St  NW, Washington, DC 20408  Tracy Location Scouting |  |
| 2 | Sun. Jul 8 ,2012 12:37 PM | Cell Location | National Gallery of Art – Sculpture Garden  38°53'27.0"N 77°01'19.8"W  Constitution Ave NW &, 7th St  NW, Washington, DC 20408  Tracy Location Scouting |  |
| 3 | Sun. Jul 8 ,2012  12:41-12:42 PM  12:59-1:00 PM | Cell Location | National Gallery of Art  38°53'30.0"N 77°01'24.6"W  Constitution Ave NW &, 7th St  NW, Washington, DC 20408  Tracy Stamp Photos:  “Mongolia” “Stamp of Kazakhstan 2”  “Nederland” “Women’s Profile”  “Mongolia” |  |
| 4 | Sun. Jul 8 ,2012 12:49-12:50 PM | Cell Location | National Law Enforcement Officers Memorial  600 5th St NW, Washington, DC 20001  38°53'51.6"N 77°01'10.8"W  Tracy Stamp Photos:  “Douglas MacArthur” “Kazakhstan” “Armed Forces Reserve”  “BradyCo” |  |
| 5 | Sat. Jun 13, 2012  3:01 PM  through  Fri. Jul 10, 2012  12:46 PM | WiFi  Location | SW Washington DC  Various Meeting Locations:  -Bubba’s Grill  -Private Residences  -Insurance Firms |  |

### 