



Cybersecurity

## 21.3 The Final Report

# Case Report National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

# Table of Contents

---

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[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.

The aim of this report is to present all the information about tracy's investigation doing an extensive analysis of their device, the people she interacted with, how are they related to the crime, the steps they took to plan it, the reasons why they did it, the location and phone numbers as well as email and other personal data. An anonymous actor called king also came into the picture giving us more insight with this types of crimes.

Tracy who worked at Nation Gallery of Art was approached by Carry who was connected to Alex (a foreigner) who wanted to embarrass the US by defacing certain museum items. Tracy who was struggling with money decided to use this event as a distraction and planning a heist with his brother Pat. Pat Approached another criminal 'King' and blackmailed him to help him in this matter. King agreed and asked for certain items. Tracy plan was when carry would start flashmob and all security busy with her, then at the same time King would steal the precious stamps. All her plan was got exposed when Joe (her soon to ex husband) who put keylogger in her system knew about it and report to the police.

## Equipment and Tools

We employed advanced digital forensic tools and software for in-depth investigations, such as Autopsy and SQLite DB, Kali Linux as the operating system, Nano as the text editor, Hyper VM to connect to the KALI machine and Docker Container to run Autopsy . Our primary aim was to uncover vital data for a comprehensive case understanding all

the interactions between Tracy, Pat, Terry, Joe, Carry, Coral, and King . Utilizing diverse techniques inherent to digital forensics, we systematically scan the digital artifacts within Tracy's iPhone image, ensuring a meticulous examination to find all possible solutions and answers.

## Details of Tracy's iPhone

- OS Version: iPhone OS 4.2.1 (8C148)
- iPhone Model: 1,2
- Serial Number: 86004482Y7H
- Host Name: Tracy sumtwelve
- Email: tracysumtwelve@gmail.com
- ICCID Number: 89014103255195342366
- IMEI Number: 012021003735398

This information pertains to an iPhone device, including its operating system version, model, serial number, host name, associated email, ICCID number, and IMEI number. The host name suggests that the device is linked to Tracys device, and the email is associated with the same individual.

## Evidence to Establish Personas

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

### 1. Tracy:

- Phone Number: (703) 340-9961
- Personal Email: tracysumtwelve@gmail.com
- Work Email: tracy.sumtwelve@nationalgallerydc.org
- Relationship: Accused

### 2. Pat:

- Phone Numbers: +12027252124, +15713083236
- Email: patsumtwelve@gmail.com

- Relationship: Brother

3. Terry:

- Phone Number: +17038296071
- Email: Not provided
- Relationship: Daughter

4. Joe:

- Phone Number: Not provided
- Email: Not provided
- Relationship: Soon-to-be ex-husband

5. Carry:

- Phone Number: +12027252124
- Email: carrysum2012@yahoo.com
- Relationship: Partner in crime

6. Coral:

- Phone Number: Not provided
- Email: coralbluetwo@hotmail.com
- Relationship: Friend / Partner in crime

7. King:

- Phone Number: Not provided
- Email: throne1966@hotmail.com
- Relationship: Anonymous / Partner in crime

In summary, the information includes contact details and relationships of individuals named Tracy, Pat, Terry, Joe, Carry, Coral, and King. Tracy is accused, Pat is a brother, Terry is a daughter, Joe is a soon-to-be ex-husband, Carry is a partner in crime, Coral is a friend/partner in crime, and King is an anonymous partner in crime. Some individuals have missing contact details.

## 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 found among Tracy, Pat and co-conspirator “King kthings throne1966@hotmail.com” (referenced in Appendix A).

166 I'm a bit of a magpie.  
167 this is what we need to get for the guy thats going to make our job happen ----- Forwarded message  
----- From: King kthings <throne1966@hotmail.com> Date: Tue, Jul 10, 2012 at 11:19 AM Subject: RE: can't pass up To:  
patsumtwelve@gmail.com 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 Date: Fri, 6 Jul 2012 11:49:31 -0400 Subject: can't pass up From:  
patsumtwelve@gmail.com To: throne1966@hotmail.com CC: coralbluetwo@hotmail.com King, Long time no see...I have  
168 I have not. Do you?

**“King kthings” in one of his email had an attachment with a list of items needed for the heist.**

- Rope and Javelin
- Smoke grenades
- Spray paint
- Turtlenecks
- Pack of smokes

## 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.

The suspects were trying to infiltrate a prohibited item/device into the museum without authorization.

104 Mon Jul 09, 2012www.theonion.com Rick Reilly Columns Increasingly Laden With Cries For Help 02.28.11 BRISTOL, CT  
-For the past six months, the columns and essays written by ESPN's Rick Reilly, including "Why Michael Vick Deserves Redemption  
More Than I Do," "The Hot Stove And Why I Want To Put My Head In It," and "Caddying F... News in Brief » Mexican Program Aims To  
Reach Drug Lords Before They Get Caught Up In Cartels American Voices » Hottest 12 Months On Record "I was wondering why I was  
complaining so much." opinion » Anchor's Gotta Spend Some Time Away by Jim Anchower By Jim Anchower  
105 Hey I was wondering if there was any way you could help me get my tablet into the gallery. I know security isn't  
to keen on computers and the like in the gallery, but maybe you could pull some strings and get it in for me? I can make it wor  
th your while :) But really I would happy to get lunch again or something else for your help. I want to get some pictures for my  
flash mob event I told you about. Let me know. ----- On Fri, Jul 6, 2012 10:55 AM PDT Tracy Sumtwelve  
wrote: Hey Carry, Just wanted to say thanks for lunch. I had a great time and it was good catching up with you. We should d  
106

## Plot Timeline

- Thursday Jul 5 2012 06:18:23 PM Carry and Tracy decided to meet at Bubba's Grill through sms.
- Friday Jul 6 2012 11:49:31 AM Pat emails to "King" (throne1966@hotmail.com) and Tracy.
- Monday Jul 9 2012 10:44:11 AM Tracy sends an email about stamps to steal, and how much they are insured for.
- Monday, Jul 9 2012 10:44:11 AM, Pat and king discuss the stuff needed to complete this heist.
- Tuesday Jul 10 2012 11:24 AM, Pat sends the list to Tracy.
- Wednesday Jul 11 2012 12:41:45 PM, Tracy arrange to deliver table to carry through sms.

## Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Both Tracy and Pat used alias; Pat used '[patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)' and Tracy used coralbluetwo@hotmail.com'. Pat's real email address is [perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com) , and Tracy's real email address is [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)
- Pat communicated with a criminal 'King' with email address 'throne1966@hotmail.com' to help him steal valuable stamps. Pat knows King's parole officer, so he blackmailed him.
- Tracy plans with Carry to arrange a flashmob that Carry wants to organize. This would distract the security guards while King commits the theft.
- Tracy already sends herself email details regarding the stamps and its worth.
- There are three clusters of WiFi and Cell location info, but do not know its significance.

## 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	5 july 2012	Sms from carry +12027252124	Tracy and carry agrees to meet	vol5/mobile/library/SMS/sms.db
2	6 july 2012	Sms to Pat +15713083236	Tracy asking pat to cal her	vol5/mobile/library/SMS/sms.db
3	6 july 2012	Sms from Pat +15713083236	Pat tells tracy that he is busy	vol5/mobile/library/SMS/sms.db
4	6 july 2012	Sms to Pat +15713083236	Tracy insisted pat to call its urgent	vol5/mobile/library/SMS/sms.db
5	6 july 2012	Sms from Pat +15713083236	Pat agrees to call in 5 min	vol5/mobile/library/SMS/sms.db
6	6 july 2012	Call from Pat +15713083236	Pat calls tracy	vol5/mobile/library/CallHistory/call_history.db
7	6 july 2012	From - <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To- <a href="mailto:throne1966@hotmail.com">throne1966@hotmail.com</a> Cc- coralbluetwo@hotmail.com	Pat tried to convince king to help him min the heist	INBOX-mbox-Messages
8	10 july 2012	To - coralbluetwo@hotmail.com	King asking for certain things to complete the task	INBOX-mbox-Messages



9	10 july 2012	From - <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To - coralbluetwo@hotmail.com	Pat sends the list of thing king needs for the heist	vol5/mobile/library/Mail
10	10 july 2012	Sms from Pat +15713083236	Uses tracy alias coral and asked her to check new list in the email	vol5/mobile/library/SMS/sms.db
11	10 july 2012	Sms to Pat +15713083236	Tracy promised to get the things needed	vol5/mobile/library/SMS/sms.db
12	11 july 2012	Sms from carry +12027252124	Letting tracy knows that carry is almost there	vol5/mobile/library/SMS/sms.db
12	11 july 2012	Sms to carry +12027252124	Tracy asked carry to meet at the front to get table in	vol5/mobile/library/SMS/sms.db
13	12 July 2012	Sms to carry +12027252124	Tracy asked about the flashmob	vol5/mobile/library/SMS/sms.db

## Appendix B: WiFi and GPS Location Information

