



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.

There are three suspects involved in the theft of stamps. Tacy, Pat, and carry. There are several findings the show these three are involved such as, Email messages and images discussing the plan to steal the stamps.

## Equipment and Tools

Autopsy, a program inside kali linux was used to find the evidence in tracys phone.

## Details of Tracy's iPhone

### Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	Iphone1, 2	Vol5, mobile, library, Logs, AppleSupport
Host Name	Tracy Sumtwelve's Iphone	Vol5, lockdownd.log.1
OS Version	Iphone OS 4.2.1 (8C148)	Vol5, Mobile, Library, Logs, Applesupport
Install Time	6/6/2012 12:03:28 -0700	Vol5, Mobile, Library, Logs, Applesupport
User Email	tracysumtwelve@gmail.com	Vol 5, Mobile, Addressbook

Phone Number	(703) 340-9661	Vol5, logs, lockdownd.log.1
Serial Number	86004482Y7H	Vol 5, Mobile, Library, Applesupport
ICCID	89014103255195342366	Vol 5, logs, lockdownd.log
IMEI	010221003735398	Vol5, root, Library, Lockdown, activation_records, wildcard_record.plist
MD5 Hash		
SHA256 Hash		

## 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  
 Relationship: Tracys sister

Terry:

Phone Number: (703) 829-6071

Email:

Relationship: Tacys daughter

Joe:

Phone Number:

Email: joe.sum.twelve@gmail.com

Relationship: Tracys ex husband

Carry:

Phone Number: (202) 725-2124

Email: carriesum2012@yahoo.com

Relationship: Flash mob

The listed above are the only contacts tracy has with anyone we could find. Carry and pat are the only 2 known to be involved with tracy in the theft.

## 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.

[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

## 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.

[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

## Plot Timeline

[Provide an outline of the key events in the order they occurred. Note the date of each event.]

## Conclusion

Evidence found on Tracy's iPhone indicated the following:

- There is email evidence that tracy and pat planned to steal the stamps
- Tracy is known to have financial troubles from the messages with terry
- Tracy sent carry info about National gallery DC. to start a flash mob
- Tracy sent herself documents of the stamps insured price

## Appendix A: Correspondence Evidence

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

[Paste your Correspondence Evidence Worksheet here.]

## Appendix B: WiFi and GPS Location Information

[Paste your GPS Evidence Worksheet here.]