Case Report

National Gallery DC

by Will Lunn

### 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)

Appendix C: Pictures

# 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.

Open finishing the thorough investigation it appears that Tracy (Alias: Carol) and her brother, Pat (Alias: Perry), made a plan to steal stamps from the National Gallery. For additional help, Pat threatened to abuse his relationship to an unknown suspect’s (Alias: King) parole officer.

### Equipment and Tools

The two core equipment tools for this investigation was the Kali Linux virtual machine and Tracy’s iPhone. It provided all the tools necessary to perform gathering and analyzing evidence.

Tools Used:

* Autopsy
* Command Line
  + SQLite DB Browser
  + Unzip
  + Xdg-open
* Google Maps

# Details of Tracy’s iPhone

A picture containing timeline

Description automatically generated

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

[perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)

Relationship: Tracy’s Sibling (Brother)

Terry:

Phone Number: (703)829-0671

Email: N/A

Relationship: Tracy and Joe’s Daughter

Joe:

Phone Number: N/A

Email: N/A

Relationship: Tracy’s Ex-Husband

Carry:

Phone Number: (202)725-2124

Email: N/A

Relationship: Tracy’s Partner in Crime

# 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.

Based on the examination of the phone’s data, we have found a trail of evidence detailing the intentions to steal valuable stamps.

On 6/19/2012, Pat sends an email (SUBJECT: “Paris Speak and answer”) to Tracy, accepting the proposition.

Artifact #1, Appendix A

Text, letter

Description automatically generated

Later in the day, Pat and Tracy have an email exchange (SUBJECT: “Look me up sometime”) where the heist idea is proposed, accepted, and then decide to use aliases.

Artifact #2, Appendix A

Graphical user interface, text

Description automatically generated

On that same day, Coral (Tracy’s Alias) receives an email (SUBJECT: “Crazydave by the VMs”) with an audio file that provides instructions on installing a Virtual Machine (VM).

Artifact #3, Appendix A

Text, letter

Description automatically generated

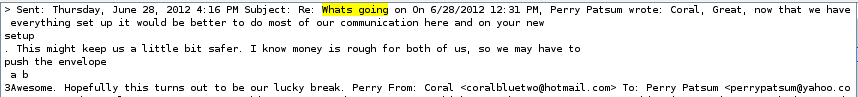
After that email, Coral (Tracy’s Alias) responds to Perry’s (Pat’s Alias) email (SUBJECT: “Re: ???”) asking if she was receiving his emails.

Artifact #4, Appendix A



On 6/28/2012, Perry (Pat’s Alias) emails Coral (Tracy’s Alias) (SUBJECT: “Whats going on”) about continuing their line of communication and that they may need to push the limits to solve financial problems.

Artifact #5, Appendix A



On 6/29/2012, Perry (Pat’s Alias) emails Coral (Tracy’s Alias) (SUBJECT: “Re: Whats going on”) that he believes IA has been sniffing around.

Artifact #6, Appendix A



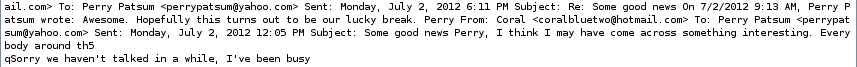
Later that day, Perry (Pat’s Alias) emails (SUBJECT: “hey sis”) Tracy calling her “sister” and suggests they all get dinner as friends.

Artifact #7, Appendix A



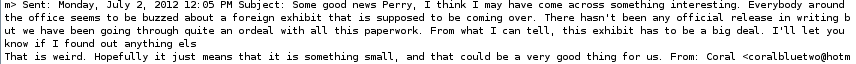
On 7/2/2012, Coral (Tracy’s Alias) and Perry (Pat’s Alias) exchange emails (SUBJECT: “Re: Some good news”) discussing a future gallery exhibit and that it could be the opportunity they’ve been looking for.

Artifact #8, Appendix A



On that same day, Coral (Tracy’s Alias) emails Perry (Pat’s Alias) mentioning the gallery exhibit,

Artifact #9, Appendix A



On 7/3/2012, Tracy and Joe (Tracy’s Ex-Husband) exchange emails (SUBJECT: “Re: Regarding Terry”) discussing their daughter’s tuition.

Artifact #10, Appendix A



On 7/5/2012, Carry emails Tracy (SUBJECT: “Long time no see…) to have lunch since she noticed she was having a hard time recently.

Artifact #11, Appendix A

Graphical user interface, text, application

Description automatically generated

On 7/6/2012, Tracy emails Pat (SUBJECT: “Good News”)

Artifact #12, Appendix A



Later that day, Tracy is CC’ed in an email (SUBJECT: “can’t pass up”) from Pat to King detailing his proposition on a heist he plans to carry out.

Artifact #13, Appendix A

Text, letter

Description automatically generated

After that email, Pat emails (SUBJECT: “Re: Good News”) Tracy with account login information.

Artifact #14, Appendix A



On 7/8/2012, Tracy takes pictures from 12:41:41 PM – 1:00:23 PM for information gathering.

Artifact #1 - #19, Appendix C (Grouped)

A screen shot of a computer

Description automatically generated with low confidence

On 7/9/2012, Tracy emails herself a zip folder (SUBJECT: “things”) containing insurance documents related to stamps.

Artifact #15, Appendix A

Text

Description automatically generated

Artifact #15 (Stamp insurance 1.pdf), Appendix A

Graphical user interface, text, application

Description automatically generated

Tracy took a picture of each stamp the day prior.

In order of left to right: (Artifact #6, Artifact #5, Artifact #7, Appendix C)

A picture containing calendar

Description automatically generated Text

Description automatically generated with low confidence A screenshot of a video game

Description automatically generated with medium confidence

Artifact #15 (Stamp Insurance 2.pdf), Appendix A

Graphical user interface, text, application

Description automatically generated

Tracy took a picture of each stamp the day prior.

In order of left to right: (Artifact #16, Artifact #3, Artifact #2, Appendix C)

A computer screen capture

Description automatically generated with low confidence Text

Description automatically generated with low confidence A picture containing qr code

Description automatically generated

Artifact #15 (Stamp insurance 3.pdf), Appendix A

Graphical user interface, text, application, Word

Description automatically generated

Tracy took a picture of each stamp the day prior.

In order of left to right: (Artifact #4, Artifact #14, Artifact #19, Appendix C)

Text

Description automatically generated A picture containing graphical user interface

Description automatically generated Graphical user interface

Description automatically generated

On 7/10/2012, Carry emails Tracy (SUBJECT: “Re: Long time no see…”) asking to help sneak in a tablet and would be compensated if she did.

Artifact #16, Appendix A

Graphical user interface, text, application

Description automatically generated

Later in the same thread, Carry also emails Tracy (SUBJECT: “Re: Long time no see...”) confirming a meeting time for the museum and agreeing to help with sneaking in the tablet.

Artifact #17, Appendix A

Graphical user interface, text, application

Description automatically generated

On that same day, Tracy is forwarded an email (SUBJECT: “RE: can’t pass up“) from King who agrees to the heist and provides a list of tools needed to do it.

Artifact #18, Appendix AText

Description automatically generated

Artifact #18 (needs.txt), Appendix A

Graphical user interface, text, application

Description automatically generated

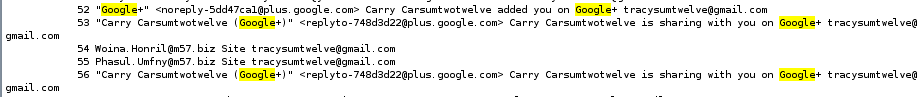
Later that same day, Tracy and Carry confirm a meeting time at 9 AM in an email (SUBJECT: “Re: Long time no see…”).

Artifact #19, Appendix A



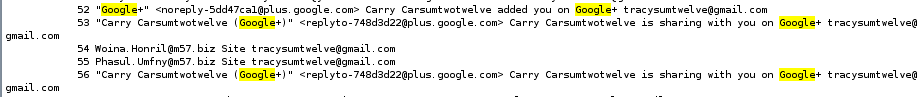
On 7/11/2012, Tracy also receives a notification from Google+ when Carry shared an album with her.

Artifact #20, Appendix A



On 7/12/2012, Tracy receives another notification from Google+ informing her that Carry shared another album.

Artifact #21, Appendix A



Later that day, Tracy emailed (SUBJECT: “RE: Long time no see…”) Carry what she meant by “It will be gun”.

Artifact #22, Appendix A



# 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 relating to any defacement of museum art on this iPhone.

# Plot Timeline

Diagram

Description automatically generated

Diagram

Description automatically generated

Text

Description automatically generated

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy and Pat were corresponding with one another using two additional email aliases.
  + Tracy’s Alias: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)
  + Pat’s Alias: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)
* Pat brings in another person, King, by threatening to abuse his friendship with King’s parole officer if he doesn’t help with the proposed gallery heist.
  + King’s Alias: [throne1966@hotmail.com](mailto:throne1966@hotmail.com)
* Carry and Tracy have a long email thread coordinating when they will be meeting and how they will be dealing with the security guards at the gallery during the heist.
  + Carry’s email: [carrysum2012@yahoo.com](mailto:carrysum2012@yahoo.com)
* Tracy takes multiple photos of the stamps at the exhibit.
  + Artifact #1 - #19, Appendix C
* Tracy emails a zip file containing insurance information on 3 insured stamps her Carol Alias email account.
  + Tracy’s email: [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)
  + Stamps: Armed Forces Reserve (Artifact #6, Appendix C)  
     Stamp of Kazakstan2 (Artifact #20, Appendix C)

BradyCo (Artifact #5, Appendix C)  
Woman’s Profile (Artifact #16, Appendix C)   
Stamp of Kazakstan (Artifact #3, Appendix C)  
Woman’s Profile (Artifact #16, Appendix C)  
1929 Napal (Artifact #2, Appendix C)  
Douglas MacArther (Artifact #4, Appendix C)

Nederland (Artifact #14, Appendix C)  
Mongolia (Artifact #19, Appendix A)

* Pat emailed Coral (Tracy’s Alias), an audio clip that is hidden instructions on how to install a Virtual Machine.
  + Pat’s email: [perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)
* King provides a list of items they need for the heist if he is going to help.
* Carry shares Google+ album with Tracy.

# Appendix A: Correspondence Evidence

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

Text

Description automatically generated with medium confidence

Text

Description automatically generated

Diagram, text

Description automatically generated with medium confidence

Diagram

Description automatically generated

Diagram

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

# Appendix B: WiFi and GPS Location Information

Tracy’s WiFi and GPS Location: /vol\_vol5/root/Library/Caches/locationd/consolidated.db

WiFi/Cell Tower Data:

Text

Description automatically generated

WiFi GPS Data:

Text

Description automatically generated

Opened in SQLiteBrowser and sorted by Timestamp. Took location coordinates anytime the Timestamp changed.

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated

A picture containing text

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generated

# Appendix C: Pictures

Text

Description automatically generated

Text

Description automatically generated with low confidence

Text

Description automatically generated