Case Report

National Gallery DC

### Tracy’s iPhone [2012-07-15-National-Gallery]

Tim Smith

# 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.

1. Digitech found evidence that indicated Tracy was using the alias Coral and Pat was using the alias Perry.
2. Evidence indicated Tracy was motivated by financial gain in planning the stamp heist.
3. Evidence of email correspondence to what is believed to be Tracy’s personal email and Pat containing the National Gallery DC stamp letters.
4. Found evidence indicating Tracy was creating a plan to steal stamps with Pat. Also found evidence Tracy knew that Pat was working with someone named king to help with the heist.
5. Found evidence Tracy helped Carry for financial gain. The evidence was sharing sensitive security schedules for the National Gallery to Carry. There is evidence indicating that Tracy helped Carry smuggle a tablet into the Gallery. Evidence shows Tracy was unaware of Carry’s full plan.

### Equipment and Tools

The following tools were used for forensic analysis:

1. Digital Forensics
2. Forensic Carving tools
3. Forensic imaging tools
4. Google Earth
5. DB Browser for SQLite 3.7.0
6. Microsoft Excel

# Details of Tracy’s iPhone

Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone model 2 | \_vol5/mobile/Library/Logs/AppleSupport |
| Host Name | Tracy Sumtwelve’s iPhone | \_vol5/mobile/Library/Logs/AppleSupport |
| OS Version | 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 | [Tracy.sumtwelve@nationalgallerydc.org](mailto:Tracy.sumtwelve@nationalgallerydc.org)  tracysumtwelve@gmail.com | \_vol5/mobile/library/mail |
| Phone Number | (703) 340-9661 | Vol5/logs/lockdown.logs.1 |
| Serial Number | 86004482Y7H | \_vol5/mobile/Library/Logs/Applesupport |
| ICCID | 89014103255195342366 | Vol5/logs/lockdown.logs.1 |
| IMEI | 012021003735398 | /root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 |  |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 |  |

# 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

Relationship: Is the brother to Tracy and the Uncle of Terry

Terry:

Phone Number: (703) 829-6071

Email:

Relationship: Daughter of Tracy and Joe. (Had the key logger on her computer)

Joe:

Phone Number: (202) 725-2124

Email: Joe.sum.twelve@gmail.com

Relationship: Ex-Husband to Tracy, Father of Terry. Put the key logger on his daughter Terry’s computer to monitor he online activity.

Carry:

Phone Number: (202) 725-2124

Email: carrysum2021@yahoo.com

Relationship: An acquaintance of Tracy.

[Provide a summary of your conclusions here.]

# 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.

Artifacts 10, 11, 13, 15 give details about how Tracy came across the valuable stamp collection exhibit. They also show Tracy and Pat being interested in stealing it since it’s small and valuable. Shown in artifacts 15 and 16, Pat tries to enroll someone named King, who has a criminal history and is currently on parole. King agrees to the heist and sends a list of what he needs shown in artifact 21. Pat forwards the list to Tracy with instructions on how open the attachment over SMS, shown in artifact 21.

Tracy emails the Insurance documents regarding the stamp collection exhibit which were marked as confidential to Pat shown in artifact 18. Artifact 18 shows two attachments, documents.zip that is unencrypted and docs.zip which is encrypted. Docs.zip contains 3 Stamp Insurance documents.

Tracy’s iPhone had photos of the stamps mentioned in the insurance documents.

# 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.

After Carry reaches out to Tracy, they met for lunch shown in artifact 19. In the same email Carry also asks Tracy for help sneaking a tablet into the national Gallery for a flash mob event being planned. Carry also mentions compensation for the help.

# 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:

* Tracy was using the alias Coral and Pat was using the alias Perry
* Tracy emailed National Gallery DC stamp letters to her personal email account as well as Pat
* Tracy’s motive for planning the heist was financial gain.
* Tracy and Pat worked together to steal the stamps
* Tracy also help Carry for financial gain
* Tracy was aware of Pat trying to bring in someone by the name of king to help with the heist
* Tracy helped Carry sneak the tablet into the Gallery
* Tracy gave Carry the information on the Security rotations for the National Gallery
* Tracy was not aware of Carry’s bigger plan she had in mind

# Appendix A: Correspondence Evidence

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Master Timeline of NGDC | | | | |
| Artifact # | Timestamp | Header Information | Key Information | Evidence Location |
| 1. | 6/19/2012 20:06:33 | F: patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  Subject: Paris Speak and answer | Pat emails Tracy letting her know that he has accepted her proposal and asks her to email using her alias for further instructions. | Mailbox Data Structure |
| 2. | 6/19/2012 20:26:47 | F: perrypatsum@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Look me up sometime | Pat (Perry) emails Tracy to ask her to communicate using her alias. | Mailbox Data Structure |
| 3. | 6/19/2012 21:38:59 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Crazydave by the VMs Attachment: Crazydave1.mp3 | Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file. | Mailbox Data Structure |
| 4. | 6/19/2012 21:39:34 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Re: ??? | Pat (Perry) replies to Tracy (Coral) confirming that he was getting her emails. | Mailbox Data Structure |
| 5. | 6/21/2012 17:43:15 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Re: Crazydave by the VMs | Pat (Perry) replies to Tracy (Coral) on a email thread about Virtual Machine installation saying that she should listen to some other songs as well.   In the email thread Tracy (Coral) confirms that the instructions sent earlier in the audio file helped her. | Mailbox Data Structure |
| 6. | 6/28/2012 19:31:33 | 6/28/2012 19:31:33  F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Whats going on | Pat (Perry) emails Tracy (Coral) asking her to henceforth communicate using the aliases and the Virtual Machine setup to keep them safer. He also indicates that they might have to get into riskier/illegal business since both of them were facing financial hardships.   He tells her that few of his workplace friends were good at these businesses and that he will inform her should something pop-up; in the meantime they should keep discussing some ideas for the same. | Mailbox Data Structure |
| 7. | 6/29/2012 14:21:56 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Re: Whats going on | This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money.  To Pat’s suggestion that they use the Virtual Machines and aliases to communicate and keep looking for ways to make money, Tracy replies that she will keep her eyes open for opportunities and insists that Pat try to get in on some business soon, since her kid didn’t want to change schools. She also indicates that she is paying attention to documents especially insurance papers so that she could identify something of potential. Pat assures that he will make something happen although he is nervous because IA has been sniffing around. | Mailbox Data Structure |
| 8. | 6/29/2012 14:31:36 | F: perrypatsum@yahoo.com  T: tracysumtwelve@gmail.com  Subject: hey sis | Pat (Perry) emails Tracy addressing her as ‘sister’ and enquires about Terry. Asks her to check in with Coral with whom he has been planning some things. He also suggests all of them going together for dinner as friends.  He asks Tracy to check in with Coral.  Possible misdirection attempted by referring to Coral as a third person in the narrative. | Mailbox Data Structure |
| 9. | 6/29/2012 15:21:35 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Re: Whats going on | Pat (Perry) replies to the email thread allaying Tracy’s (Coral) concern about IA sniffing around him. Tracy in her earlier email in the thread says that although nothing interesting has turned up yet she expects something soon. Pat in his email mentions that they can certainly get the job done if something like what they had earlier discussed pops up. | Mailbox Data Structure |
| 10. | 7/2/2012 16:13:18 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Re: Some good news | Email Thread: Some good news  Tracy (Coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal.  Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for. | Mailbox Data Structure |
| 11. | 7/2/2012 20:00:31 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Re: Some good news | Email thread: Some good news  Following up on the earlier email about the exhibit, Tracy (Coral) mentions going through documents related to the exhibit from which she found that the exhibit is worth a lot of money but the shipping cost is very low comparatively.  Pat (Perry) emails back saying that such a thing may mean that the exhibit is something small which would be a very good thing for them. | Mailbox Data Structure |
| 12. | 7/3/2012 13:29:37 | F: joe.sum.twelve@gmail.com  T: tracysumtwelve@gmail.com  Subject: Re: Regarding Terry | Email Thread: Regarding Terry  Tracy emails Joe asking whether he could help her with Terry’s tuition this year since it is becoming too expensive for her.  Joe replies back saying that he won’t be paying Terry’s tuition if she is not living with him. | Mailbox Data Structure |
| 13. | 7/3/2012 14:53:04 | F: perrypatsum@yahoo.com  T :coralbluetwo@hotmail.com  Subject: Re: Some good news | Email Thread: Some good news  Tracy (Coral) emails Pat (Perry) saying that the exhibit is rare and highly valuable stamp collection and that may be this is their opportunity.  Pat (Perry) replies to Tracy (Coral) asking her to collect as much information as possible about the stamp exhibit and that in the meantime he would look into options for pulling off the heist. | Mailbox Data Structure |
| 14. | 7/5/2012 15:51:31 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Long time no see... | Carry reaches out to Tracy asking her if they could meet-up for lunch and suggests this Friday. She also mentions that through Facebook she realized that Tracy was having a hard time recently. | Mailbox Data Structure |
| 15. | 7/6/2012 15:27:51 | F: patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  Subject: Re: Good News | Email Thread: Good News  Tracy emailed Pat saying that she spoke with Coral and that Coral got some great news about her job and suggested that Pat catch up with Coral.  Pat replied back saying that he knows a guy called King. | Mailbox Data Structure |
| 16. | 7/6/2012 15:49:31 | F: patsumtwelve@gmail.com  T: throne1966@hotmail.com  Cc:coralbluetwo@hotmail.com  Subject: can't pass up | Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at national gallery. He also threatens King to comply or else he would put King’s parole in jeopardy. | Mailbox Data Structure |
| 17. | 7/6/2012 17:59:24 | F: patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  Subject: Re: Good News | Email Thread: Good News  Tracy suggests they (meaning King, Tracy and Pat) should hang out sometime.  Pat emails Tracy with account login information for:  coralblue@hotmail.com  Password: legalBee | Mailbox Data Structure |
| 18. | 7/9/2012 14:44:11 | F: tracysumtwelve@gmail.com  T: coralbluetwo@hotmail.com  Subject: things | documents.zip is a compressed ZIP folder containing 3 insurance documents related to stamps.  docs.zip is an encrypted ZIP folder containing 3 insurance documents related to stamps. | /mobile/Librar y/Mail/POP- coralbluetwo @hotmail.com @pop3.live.co m/INBOX.mbo x/Messages/8 A3BD06F- CDB1-4453- 9C69- 77E06823F2A E.emlx |
| 19. | 7/9/2012 18:18:47 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Re: Long time no see.. | Email Thread: Long time no see... Tracy thanked Carry for the lunch.  Carry emails Tracy asking for help sneaking in a tablet for a flash mob event they had spoken earlier about. Carry suggests that Tracy would be compensated in some way for the help. | Mailbox Data Structure |
| 20. | 7/10/2012 13:48:40 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Re: Long time no see... | Email Thread: Long time no see…  Tracy agrees to help Carry sneak in the tablet and asks when Carry would like to get in to take a look around the gallery.  Carry replies saying that this would be a big help and asks if she could come around 9 tomorrow. | Mailbox Data Structure |
| 21 | 7/10/2012 15:24:57 | F: patsumtwelve@gmail.com  T: coralbluetwo@hotmail.com  Subject: Fwd: can't pass up  Attachment: needs.txt | Email Thread: cant’ pass up  King agrees to help with the heist and sends in a document with equipment required for it. The attached document is saved as a ‘txt’ file.  Pat forwards that email to Tracy (Coral)  \*needs.txt is a pdf file which was saved with a wrong extension. | /mobile/Librar y/Mail/POP- coralbluetwo @hotmail.com @pop3.live.co m/INBOX.mbo x/Messages/9 F0508B8- 04FB-490E- A7F0- 3E23B0E7C5 9B.emlx |
| 22. | 7/11/2012 17:06:19 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Re: Long time no see... | Email Thread: Long time no see  Tracy confirms the meet at 9 tomorrow.  Carry wants Tracy to pass her information regarding shift changes of security. She suggests that Tracy would be well compensated for the information.  Tracy confirms that she will give the security shift information Carry requested in exchange for money but asks Carry to be careful with it.  Carry replies asking Tracy not to worry and says “It will be gun”. | Mailbox Data Structure |
| 23. | 7/11/2012 19:28:53 | F: "Google+" <noreply- 5dd47ca1@plus.google.com>  T: tracysumtwelve@gmail.com  Subject: Carry Carsumtwotwelve added you on Google+ | Email Thread: Long time no see  Previous email from the thread from Carry asking for the security shift details from Tracy. | Mailbox Data Structure |
| 24. | 7/11/2012 23:22:03 | F: "Carry Carsumtwotwelve (Google+)" <replyto- 748d3d22@plus.google.com>  T: tracysumtwelve@gmail.com    Subject: Carry Carsumtwotwelve is sharing with you on Google+ | Notification from Google+ informing Tracy that Carry had shared an album. | Mailbox Data Structure |
| 25. | 7/12/2012 16:12:07 | F: "Carry Carsumtwotwelve (Google+)" <replyto- 748d3d22@plus.google.com>  T: tracysumtwelve@gmail.com  Subject: Carry Carsumtwotwelve is sharing with you on Google+ | Notification from Google+ informing Tracy that Carry had shared an album. | Mailbox Data Structure |
| 26. | 7/12/2012 18:03:51 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Re: Long time no see... | Email Thread: Long time no see...  Tracy emailed Carry asking her what she meant by “It will be gun”.  Carry replies saying that it was a typographical error and she meant “It will be fun”. | Mailbox Data Structure |

# Appendix B: WiFi and GPS Location Information

[Paste your GPS Evidence Worksheet here.]