Case Report

National Gallery DC

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

8/7/2021

Jacob Seiger

Rich Wager

Tyson Bengtzen

Zylar Wright

Andrew Nguyen

# 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.

Our team had found that Tracy (Coral) and Pat (Perry) were looking for the right opportunity to make money illegally. The opportunity presented itself with a foreign exhibition of a rare stamp collection that they would attempt to steal. Pat know’s a person named “King”. Pat threatens “King” to help with the heist or he would cause issues with his parole. The following report is a documentation of our findings related to the case as well as visual evidence of the involved parties in the collusion.

### Equipment and Tools

* Kali Linux
* Autopsy
* SQLite Browser
* Google Maps
* Unix Time Converter

# Details of Tracy’s iPhone

* iPhone 3G’s
* iPhone OS (8c148)
* Install Time: 2010-11-17 03:33:32
* Phone Number: 703-340-9661
* Serial Number: 86004482y7h
* ICCID: 89014103255195342366
* IMEI: 004999010640000

# 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: Brother / Co-Conspirator

Terry:

Phone Number: (703) 829-6071

Email: N/A

Relationship: Daughter

Joe:

Phone Number: N/A

Email: joe.sum.twelve@gmail.com

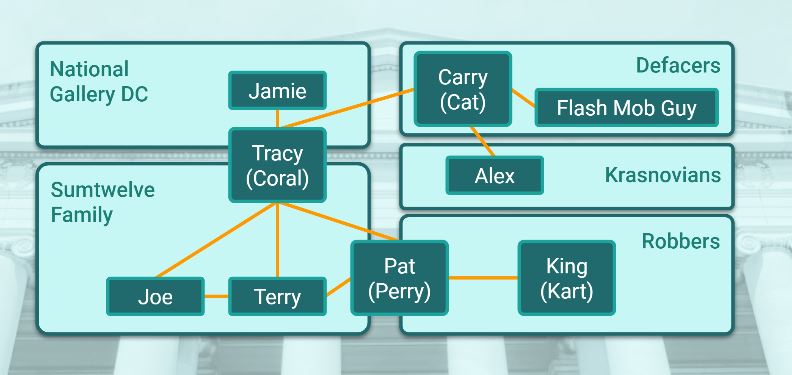
Relationship: Divorced Spouse / Terry’s Father

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Relative / Co-Conspirator



# 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 #22, 27, 28, 29 show Tracy finding out about the valuable stamps collection at the exhibit. Pat and Tracy think that this is their chance because the exhibit is small and valuable. Tracy and Pat bring on a guy named King, who is on parole and has a criminal background. Tracy and Pat use intimidation and blackmail to get King to agree to the heist, and after agreeing, King sends a list of requirements, in an attachment, to Pat who forwards it to Tracy with some instructions on how to open it.

# 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.

Carry me with Tracy over lunch, and got Tracy to help Carry sneak a tablet into the National Gallery for Carry’s flash mob event she told Tracy about. Carry gives the tablet to Tracy who sneaks it inside. Tracy also provided Carry with security shift change times and information as well. Carry mentioned that she would be compensating Tracy for her help.

Tracy later asks Carry how the flash mob is going. Although Tracy did share security info with Carry, the message from Tracy shows that Tracy was only aware of the flash mob and not the defacement.

# Plot Timeline

1. Contact and initial Reconnaissance
   1. In artifacts five and eight we see the first documented contact between the two prime suspects.
2. Acceptance of association
   1. In artifact 8 we can see Tracys initial acceptance of involvement pat had planned
3. Initial setup
   1. In artifacts 9, 10 and 11 we see the documentation between tracy and pat to accomplish three things
      1. Setting up a virtual machine
      2. Using their alias’ from now on (perry for pat and coral for tracy)
      3. Using said virtual machines and alias’ to communicate from here on out
   2. In artifact 14 there are 3 things to note as well
      1. perry/pat acknowledge the fact of what they're doing is illegal
      2. Perry /pat informs tracy that he has some friends in the business that he can reach out to that will help
      3. perry /pat also asks tracy to keep him informed of any interesting news, this leads into active reconnaissance
4. Active Reconnaissance
   * 1. In artifact 17 we see that perry /pat had discussed what a good opportunity would look like with tracy
     2. In artifact 18 we see documentation of tracy on a new email thread informing that there was a new high value exhibit
     3. In artifact 20 we gain details as to why this is a good opportunity and it is because the physical items are lightweight and easy to ship
     4. In artifact 22 we gain documented details as to what exactly is the target, an exhibit of historic stamps. Perry also requests more active recon from tracy/coral before they continue
     5. In artifact 23 carry, a third member, reaches out to tracy regarding tracys money problems, offers to meet and help
     6. As seen in earlier artifact 16, in artifact 27 we see again terry and pat referring to coral as a third person, most likely a misdirect, as well as pat referencing a third affiliate, known as king
5. Attack implementation
   * 1. In artifact 28 we see an email from pat with a CC from an affiliate named king, pat had reached out to him and forced him to be a part of the plan through coercion. This is the first step in the implementation phase as it sets a plan into motion
     2. In artifact 29 we see a document from “king” containing details of needed items for the crime titled needs.txt.
     3. On artifacts 30 and 31 we see the newly formed group collate their data on a secure VM as well as share the data relating to the theft
     4. In artifacts 32, 33, 38, 39 and 40 we see the implementation of carry and tracy's attack with four key items
        1. tracy agrees to bring a tablet inside the museum
        2. Carry suggests that tracy will be compensated for the work
        3. Tracy meeting terry via sms and taking the tablet inside
        4. Tracy promises to be careful not to be caught with the tablet as well as promising carry the information on the security shift changes

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

Tracy used the alias Coral and Pat used the alias Perry.

Tracy was motivated by money, due to her financial hardship, and was the reason for the planned heist.

Tracy emailed National Gallery letters to her personal email and to Pat’s personal email as well.

Tracy and Pat formed a plan to steal the stamps.

Tracy knew that Pat was trying to get someone named King to help them with the heist.

Tracy helped sneak in a tablet for Carry for financial gain as well. Tracy also gave Carry security shift change information to make it easier for Carry’s flash mob.

Tracy didn’t know Carry’s true plan of defacing the art.

# Appendix A: Correspondence Evidence

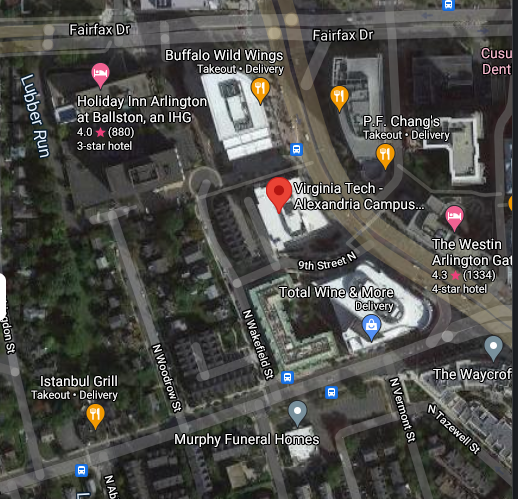
This subsection will provide an amalgamation of the email and SMS corresponce evidence.

| Master Timeline of NGDC | | | | |
| --- | --- | --- | --- | --- |
| Artifact # | Timestamp | Header Information | Key Information | Evidence Location |
| 1 | 6/12/2012  20:04:50 | F: (650)-887-0260  T: Tracy | Call duration 20 seconds  Flag 4: Incoming call | Call |
| 2 | 6/12/2012  20:52:14 | F:(703)-829-6191  T: Tracy | Call duration 56 seconds  Flag 4: Incoming call | Call |
| 3 | 6/13/2012  16:29:13 | F: Tracy  T: Pat | Tracy calls Pat but Pat does not pick up.  Flag 5: Incoming call | Call |
| 4 | 6/13/2012 19:04:03 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 5 | 6/13/2012 18:30:38 | SMS Message  F: Tracy  T: Pat | Tracy replies to Pat’s message saying that she has no big plans and enquires about his plans. | SMS |
| 6 | 6/13/2012  19:01:21 | Cell Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 7 | 6/13/2012  19:01:22 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 8 | 6/19/2012 20:06:33 | F: patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  S: 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. | vol5/Mobile/Library/mail |
| 9 | 6/19/2012 20:26:47 | F: perrypatsum@yahoo.com  T: tracysumtwelve@gmail.com  S: Look me up sometime | Pat (Perry) emails Tracy to ask her to communicate using her alias. | vol5/Mobile/Library/mail |
| 10 | 6/19/2012 21:38:59 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: Crazydave by the VMs Attachment: Crazydave1.mp3 | Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file. | vol5/Mobile/Library/mail |
| 11 | 6/21/2012 17:43:15 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: Re: Crazydave by the VMs | Pat (Perry) replies to Tracy (Coral) on an 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. | vol5/Mobile/Library/mail |
| 12 | 6/22/2012  17:34:26 | F: (571)-245-8517  T: Tracy | Tracy missed a call from number: (571)-245-8517.  Flag 4: Incoming wall | Call |
| 13 | 6/23/2012 17:12:16 | Cell Location Local | Location: 22 West A Condominium 1177 22nd St NW Washington, DC 20037 | Location |
| 14 | 6/28/2012 19:31:33 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail |
| 15 | 6/29/2012 14:21:56 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail |
| 16 | 6/29/2012 14:31:36 | F: perrypatsum@yahoo.com  T: tracysumtwelve@gmail.com  S: 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. | vol5/Mobile/Library/mail |
| 17 | 6/29/2012 15:21:35 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail |
| 18 | 7/2/2012  16:13:18 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail |
| 19 | 7/2/2012  16:19:23 | Cell Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 20 | 7/2/2012  20:00:31 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail |
| 21 | 7/3/2012  13:42:42 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 22 | 7/3/2012  14:53:04 | F: perrypatsum@yahoo.com  T :coralbluetwo@hotmail.com  S: Re: Some good news | Tracy (Coral) emails Pat (Perry) saying that the exhibit is a valuable stamp collection and that is their opportunity. Pat (Perry) replies to Tracy (Coral) asking her to collect as much information as possible and that in the meantime he would look into options for pulling off the heist. | vol5/Mobile/Library/mail |
| 23 | 7/5/2012  15:51:31 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  S: 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. | vol5/Mobile/Library/mail |
| 24 | 7/5/2012  16:32:46 | Cell Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 25 | 7/5/2012  16:32:47 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) | Location |
| 26 | 7/6/2012  15:18:50 | F: Pat  T: Tracy | Call duration 4 minutes and 4 seconds.  Flag 4: Incoming call | Call |
| 27 | 7/6/2012  15:27:51 | F: patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  S: Re: 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. | vol5/Mobile/Library/mail |
| 28 | 7/6/2012  15:49:31 | F: patsumtwelve@gmail.com  T: throne1966@hotmail.com  Cc:coralbluetwo@hotmail.com  S: can't pass up | Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at the national gallery. He also threatens King to comply or else he would put King’s parole in jeopardy. | vol5/Mobile/Library/mail |
| 29 | 7/6/2012  11:49:31 | F: [throne7966@hotmail.com](mailto:throne7966@hotmail.com)  T: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  S. cant pass up | An email from ‘King’ containing a file with details on the needed items for the Defacement contains the Needs.txt file | vol5/Mobile/Library/mail/POP…..op3.live.com/INBOX.mbox/Attachments/60/2 |
| 30 | 7/6/2012  17:59:24 | F: patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  S: Re: 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 | vol5/Mobile/Library/mail |
| 31 | 7/9/2012  14:44:11 | F: tracysumtwelve@gmail.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail\_\_\_\_\_\_\_  Doc Location:vol5/Mobile/Library/mail/POP…..op3.live.com/INBOX.mbox/Attachments/61/2 |
| 32 | 7/9/2012  18:18:47 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  S: Re: 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. | vol5/Mobile/Library/mail |
| 33 | 7/10/2012 13:48:40 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  S: Re: 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. | vol5/Mobile/Library/mail |
| 34 | 7/8/2012  16:51:44 | IMG\_0064.JPG | Location: 1321 5th St NW Washington, DC 20001 | Location |
| 35 | 7/10/2012 15:24:57 | F: patsumtwelve@gmail.com  T: coralbluetwo@hotmail.com  S: 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. | vol5/Mobile/Library/mail |
| 36 | 7/10/2012 15:26:19 | SMS Message  F: Pat  T: Tracy | Pat messages Tracy telling her about the email and informing that the attachment needs to be changed to pdf. He asks Tracy to tell this information to Coral. | SMS |
| 37 | 7/10/2012  16:47:12 | Cell Location Local | Location: 1521 North Quaker Lane, Alexandria, VA 22302 | Location |
| 38 | 7/11/2012  12:41:45 | SMS Message  F: Carry  T: Tracy | Carry messages Tracy informing that she is almost there (National Gallery) | SMS |
| 39 | 7/11/2012  12:49:08 | SMS Message  F: Tracy  T: Carry | Tracy replies to Carry asking her to meet out front. She says that she will take the tablet in. | SMS |
| 40 | 7/11/2012  17:06:19 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  S: Re: 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”. | vol5/Mobile/Library/mail |
| 41 | 7/12/2012 18:03:51 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  S: 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”. | vol5/Mobile/Library/mail |

### 

# Appendix B: WiFi and GPS Location Information

***Due to the VERY limited resources that we have to work with (Google Maps, etc.), the images below are all APPROXIMATE locations of the cell and WiFi locations.***



| 6/13/2012  19:01:21 | Cell Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| --- | --- | --- | --- |
| 6/13/2012 19:01:22 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 6/13/2012 19:04:03 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 6/23/2012 17:12:16 | Cell Location Local | Location: 22 West A Condominium 1177 22nd St NW Washington, DC 20037 |  |
| 7/2/2012 16:19:23 | Cell Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 7/2/2012 16:19:24 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 7/3/2012 13:42:42 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 7/5/2012 16:32:46 | Cell Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 7/5/2012 16:32:47 | Wifi Location | Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203) |  |
| 7/18/2012  16:33:37 | Image of varied cell locations in the same spot. | Location: National Gallery of Art Gardens |  |
| 7/8/2012 16:51:44 | IMG\_0064.JPG | Location: 1321 5th St NW Washington, DC 20001 |  |
| 7/10/2012  16:47:12 | Cell Location Local | Location: 1521 North Quaker Lane, Alexandria, VA 22302 |  |