| Cybersecurity |
| --- |
| 21.3 The Final Report |

Case Report

National Gallery DC

### 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)

# 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.

[Provide a brief summary of your findings here.]

### Equipment and Tools

Kali Linux was utilized to conduct the forensic analysis, employing software such as Autopsy and the Image Viewer for examining the evidence.

# Details of Tracy’s iPhone

| **Name** | **Findings** | **Location in iPhone image file** |
| --- | --- | --- |
| Model | Iphone 1, 2 | vol5/mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelve | vol5/logs/lockdownd.log.1 |
| OS Version | Iphone OS 4.2.1. (8C148) | vol5/mobile/Library/Logs/AppleSupport/general.log |
| Install Time | 6/6/2010 12: 03: 28 -0700 | vol5/mobile/Library/Logs/AppleSupport/general.log |
| User Email | Personal Email: tracysumtwelve@gmail.com  Work Email: tracy.sumtwelve@nationalgallerydc.org | vol5/mobile/Library/Mail |
| Phone Number | 703 304 9661 | vol5/logs/lockdownd.log.1 |
| Serial Number | 86004482Y7H | vol5/mobile/Library/Logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | vol5/logs/lockdownd.log.1 |
| IMEI | 010221003735398 | vol5/root/Library/Lockdown/activation\_records/wil dcard\_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](mailto:tracysumtwelve@gmail.com) (real)

[coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) (fake)

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Terrys mum, pats sister, Joe's ex wife, carries a friend

Pat:

Phone Number: (571) 308-3236 

Email: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com) (fake) 

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

Relationship: Brother

Terry:

Phone Number: (703) 829-6071

Email: N/A

Relationship: Joes and tracy's child

Joe: 

Phone Number: N/A

Email: joe.sum.twelve@gmail.com

Relationship: Terry's Father Tracy's EX husband

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: Tracy's friend ( flash mob )

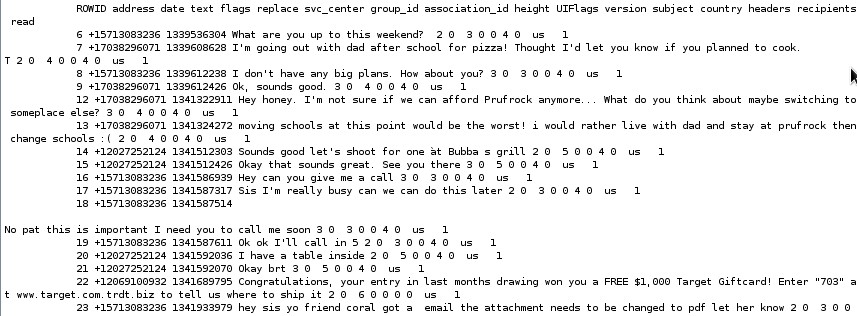
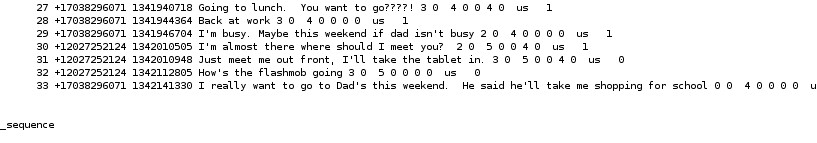
King:

Phone Number: N/A

Email: [throne1966@hotmail.com](mailto:throne1966@hotmail.com)

Relationship Pats friend

In the image I provided we can see the messages from carry, Joe, Pat, and Terry

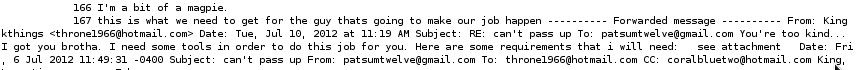
We can also see that carry and tracy are meeting bubbas grill where they meet up round 3 and carry saying she has a table inside they also meet up another time and carrys sends a message saying how's the flashmob going

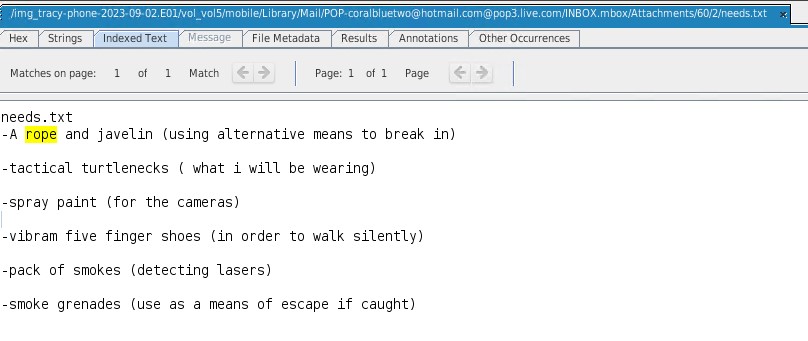
# Evidence relating to theft of valuable stamps

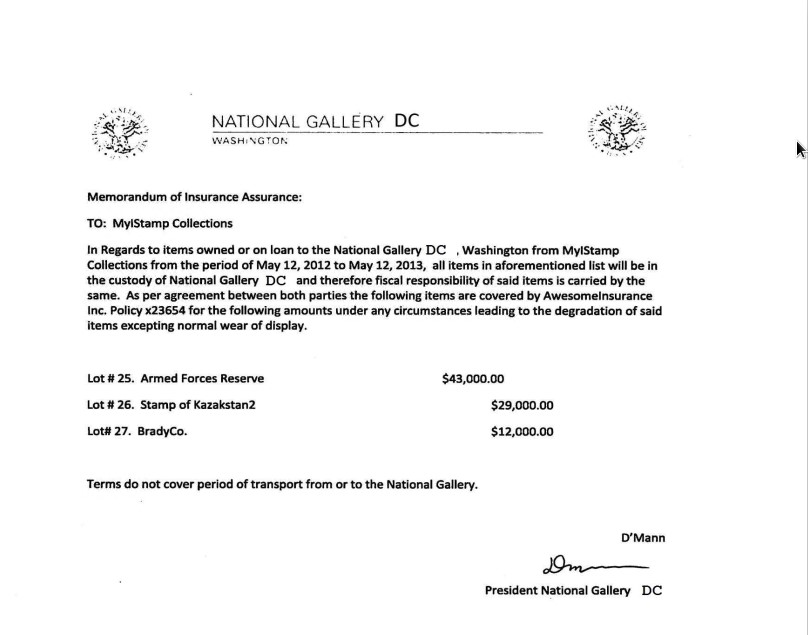
This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

From the evidence I found which consists of photos and emails and what they would need to pull off this heist it shows that Tracy is working with pat and his friend king to steal valuable stamps.

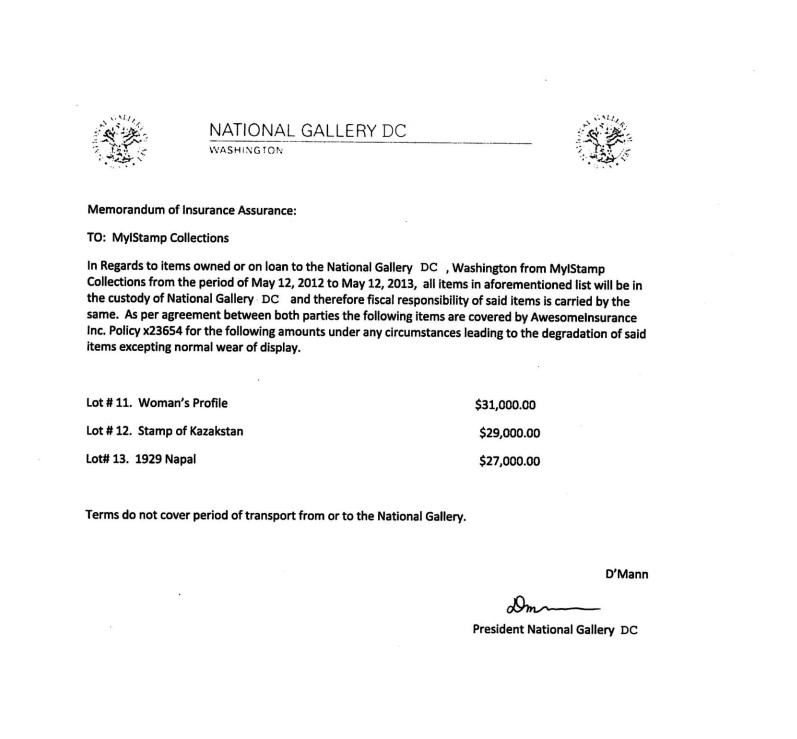
Tracy also had photos of what they were going to steal and how much they worth she also received a suspicious message saying she won $1000 target gift card and for her to put in a code this came from a website called www.traget.com.trdt.biz my this domain does not belong to anyone and is used to conceal the fact its in relation with the heist most likely payment to tracy form Carry.



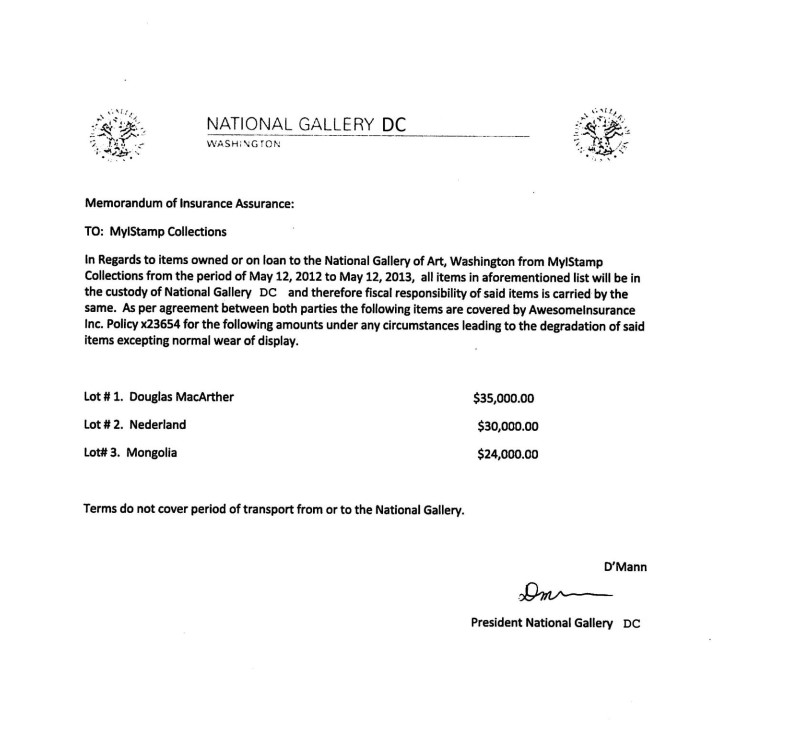


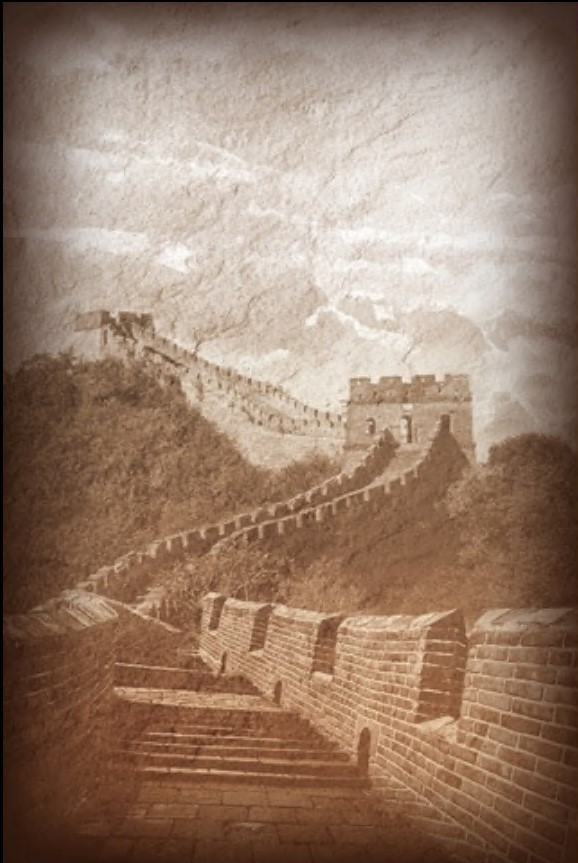












[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

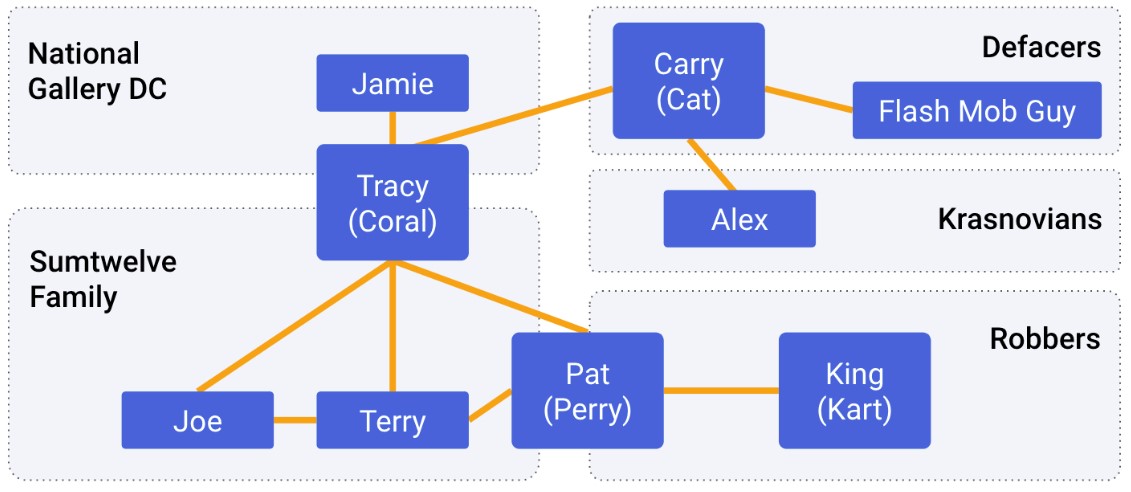
# Evidence relating to defacement of museum art

There was no specific evidence regarding the defacement of the museum's art. Instead, the evidence focused on what items they intended to steal, the tools they planned to use, how they would execute the heist, and when they intended to steal the stamps.

# Plot Timeline

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

| **Date/Time** | **Event Description** |
| --- | --- |
| Tue, Jun 19, 2012, 02:38 PM | Pat (perrypatsum@yahoo.com) emails Tracy (coralbluetwo@hotmail.com) an MP3 audio recording with instructions to install VirtualBox on her computer. |
| Thu, Jul 5, 2012, 06:18:23 PM | Tracy and Carry agree via SMS to meet at Bubba’s Grill. |
| Fri, Jul 6, 2012, 11:49:31 AM | Pat arranges via email a "proposition" with "King" (throne1966@hotmail.com) and Tracy. |
| Fri, Jul 6, 2012, 04:27:16 PM | Tracy and Carry confirmed the meeting at Bubba’s Grill via SMS. |
| Sat, Jul 7, 2012, 07:36:35 PM | Tracy receives an SMS claiming she won a $1000 Target Gift Card with a suspicious URL. |
| Mon, Jul 9, 2012, 10:44:11 | Tracy sends herself an email detailing which stamps to steal and their insured value. |
| Mon, Jul 9, 2012, 10:44:11 | Pat and "King" arrange via email tasks related to their plan. |
| Tue, Jul 10, 2012, 11:24 | Pat forwards the task list to Tracy via email. |
| Wed, Jul 11, 2012, 12:41:45 | Carry and Tracy coordinate via SMS for Tracy to deliver a tablet to Carry. |
| Thu, Jul 12, 2012, 05:06:45 PM | Tracy texts Carry about the progress of a flashmob via SMS. |



# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* [Summarize your final conclusions of the case and Tracy’s Iphone here.]
* [For example: Tracy used the alias Coral and Pat used the alias Perry.]

# Appendix A: Correspondence Evidence

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

[Paste your Correspondence Evidence Worksheet here.]

### 

| 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 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. | 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 |
| 27. | 6/12/2012 21:25:04 | F: Pat  T: Tracy | Pat asks Tracy about her plans for the weekend | SMS |
| 28. | 6/13/2012 17:30:28 | F: Terry  T: Tracy | I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. T | SMS |
| 29. | 6/13/2012 18:30:38 | F: Tracy  T: Pat | Tracy replies to Pats message saying that she has no big plans and enquires about his plans. | SMS |
| 30. | 6/13/2012 18:33:46 | F: Tracy  T: Terry | Ok, sounds good. | SMS |
| 31. | 7/3/2012 14:04:32 | F: Terry T: Tracy | Terry replies back saying that she doesn’t want to switch schools and would rather stay with her dad and continue at Prufrock | SMS |
| 32. | 7/5/2012 18:18:23 | F: Carry T: Tracy | Carry sets up the time and location as 1pm at Bubba’s grill for meeting with Tracy | SMS |
| 33. | 7/5/2012 18:20:26 | F: Tracy T: Carry | Tracy confirms the meeting time and location | SMS |
| 34. | 7/6/2012 15:02:19 | F: Tracy T: Pat | Tracy asks Pat to give her a call | SMS |
| 35. | 7/6/2012 15:08:37 | F: Pat T: Tracy | Pat says he is busy and suggests calling later | SMS |
| 36. | 7/6/2012 15:11:54 | F: Tracy T: Pat | Tracy says its important and insists that pat call her soon | SMS |
| 37. | 7/6/2012 15:13:31 | F: Pat T: Tracy | Pat says he will call in 5 min | SMS |
| 38. | 7/6/2012 15:18:50 | F: Pat T: Tracy | Pat calls Tracy and they speak for 4 min 4 secs. | SMS |
| 39. | 7/6/2012 16:27:16 | F: Carry  T: Tracy | Carry messages saying she has a table inside | SMS |
| 40. | 7/6/2012 16:27:50 | F: Tracy  T: Carry | Tracy replies back saying that she will be there. | SMS |
| 41. | 7/10/2012 15:26:19 | 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 |
| 42. | 7/10/2012 15:58:04 | F: Tracy  T: Pat | Tracy acknowledges the email and message. | SMS |
| 43. | 7/10/2012 16:37:09 | F: Tracy T: Pat \*Failed | Tracy tried to share the following location with Pat over MMS message but it failed. Location: 2600-2700 24th Rd S, Arlington, VA 22206 | SMS |
| 44. | 7/10/2012 17:18:38 | F: Tracy T: Terry | Tracy messages Terry for Lunch | SMS |
| 45. | 7/10/2012 18:19:24 | F: Tracy T: Terry | Tracy messages Terry that she is back at work. | SMS |
| 46. | 7/10/2012 18:58:24 | F: Terry T: Tracy | Terry messages Tracy saying she is busy and suggests meeting up over the weekend if her dad isn’t busy. | SMS |
| 47. | 7/11/2012 12:41:45 | F: Carry T: Tracy | Carry messages Tracy informing that she is almost there (National Gallery) | SMS |
| 48. | 7/11/2012 12:49:08 | F: Tracy T: Carry | Tracy replies to Carry asking her to meet out front. She says that she will take the tablet in. | SMS |
| 49. | 7/13/2012 1:02:10 | F: Terry T: Tracy | I really want to go to Dad’s this weekend. He said he’ll take me shopping for school | SMS |

### 

# Appendix B: WiFi and GPS Location Information

[Paste your GPS Evidence Worksheet here.]

| **Timestamp** | **Location Type** | **Latitude** | **Longitude** | **Location Description** | **Artifact #** |
| --- | --- | --- | --- | --- | --- |
| Tuesday, July 10, 2012 | Cell Location | 38°51'05.1"N | 77°04'41.7"W | 1700 Army Navy Dr, Arlington, VA 22202 |  |
| Wednesday, June 13, 2012 | Cell Location | 38°52'51.3"N | 77°07'01.6"W | 4600 Fairfax Dr, Arlington, VA 22203 |  |
| Sunday, July 8, 2012 | Cell Location | 38°53'30.0"N | 77°01'24.6"W | Northwest Washington, Washington, DC 20408 |  |
| Wednesday, June 13, 2012 | Wifi Location | 38°52'50.0"N | 77°06'55.9"W | 900 N Glebe Rd, Arlington, VA 22203, USA |  |
| Tuesday, July 10, 2012 | Wifi Location | 38°49'39.5"N | 77°05'17.0"W | 4102 36th St S, Arlington, VA 22206 |  |
| Monday, July 2, 2012 | Wifi Location | 38°52'49.9"N | 77°06'52.0"W | 801 N Glebe Rd, Arlington, VA 22203 |  |
| Tuesday, July 10, 2012 | Wifi Location | 38°49'44.7"N | 77°05'05.1"W | 1701 Centre Plaza, Alexandria, VA 22302 |  |
| Tuesday, July 10, 2012 | Cell Location | 38°49'37.4"N | 77°05'10.0"W | 1737 W Braddock Pl, Alexandria, VA 22302 |  |
| Wednesday, June 13, 2012 | Cell Location | 38.87808389293063 | -77.11532449373422 | 703 N Wakefield St, Arlington, VA 22203 |  |