Cybersecurity

21.3 The Final Report

# Case Report
# National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

# Table of Contents

# 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.

- Found evidence that Tracy corresponded with Pat Sumtwelve about operations.
- Found further evidence that they knew the value of the stamps that were targeted.
- Found evidence of other motivated parties with skills that would help in the heist.
- Found evidence of obfuscation of file types and other means of covering up incriminating evidence. Such as pdf files marked as text files and even Tracy creating an alias to hide her identity as Coral.
- Further found that Tracy and her brother Pat (a corrupt police officer) worked with another party named "King" at throne1966@hotmail.com to steal these stamps from the National Gallery.
- Tracy's friend Carry also appears to have something to do with the distraction of the flash mob and some suspicious payments via a bogus target URL.

# Equipment and Tools

In the investigation, evidence was obtained from Tracy's phone and analyzed by a Kali Linux program called "autopsy". This tool leveraged the tool called "sqlitebrowser" to help analyze the metadata to gain a better understanding of correspondence with the accused. Other tools to help included the Epoch converter to convert the timestamps into human readable verbiage from the sqlitebrowser (https://www.epochconverter.com/). We also used https://www.google.com/maps/ to show the locations found in the GPS coordinates with longitude latitude specifications. We also used Nano text editor to scroll through many of the large text files to enumerate the series of events.

# Details of Tracy's iPhone

## Case Name: 2012-07-15-National-Gallery

## Case #: 1EZ215-P

---

### Details of Tracy's iPhone

| Name | Findings | Location in iPhone image file |
|---|---|---|
| Model | iPhone (1-2) | library/logs/applesupport/general.log |
| Host Name | Tracy Sumtwelve's iPhone | vol5/logs/lockdownd.log.1 |
| OS Version | iPhone OS 4.2.1 (8C148) | mobile/logs/apple Support/general.log |
| Install Time | 6/6/2012 19:03:28 | mobile/logs/apple Support/general.log |
| User Email | tracysumtwelve@nationalgallerydc.org and tracysumtwelve@gmail.com | vol5/mobile/Library/Mail/POP /INBOX.mbox/Messages |
| Phone Number | (703) 340-9661 | vol5/logs/lockdownd.log.1 |
| Serial Number | 86004482Y7H | mobile/logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | vol5/logs/lockdownd.log.1 |
| IMEI | 012021003735398 | /root/Library/Lockdown/activation_records/wildcard_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | N/A Image |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | N/A Image |

# Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy (aka Coral):

| | |
|---|---|
| Phone Number: | (703) 340-9961 |
| Personal Email: | tracysumtwelve@gmail.com |
| Work Email: | tracy.sumtwelve@nationalgallerydc.org |
| Alias Email: | coralbluetwo@hotmail.com |
| Relationship: | Accused |

Pat (aka Perry):

Phone Number: (571) 308-3236
Email: and patsumtwelve@gmail.com
Alias Email: perrypatsum@yahoo.com
Relationship: Tracy's brother

Terry:

Phone Number: (703) 829-6071
Email: unknown
Relationship: Daughter of Tracy/Joe

Joe:

Phone Number: unknown
Email: joe.sum.twelve@gmail.com
Relationship: Ex-husband

Carry:

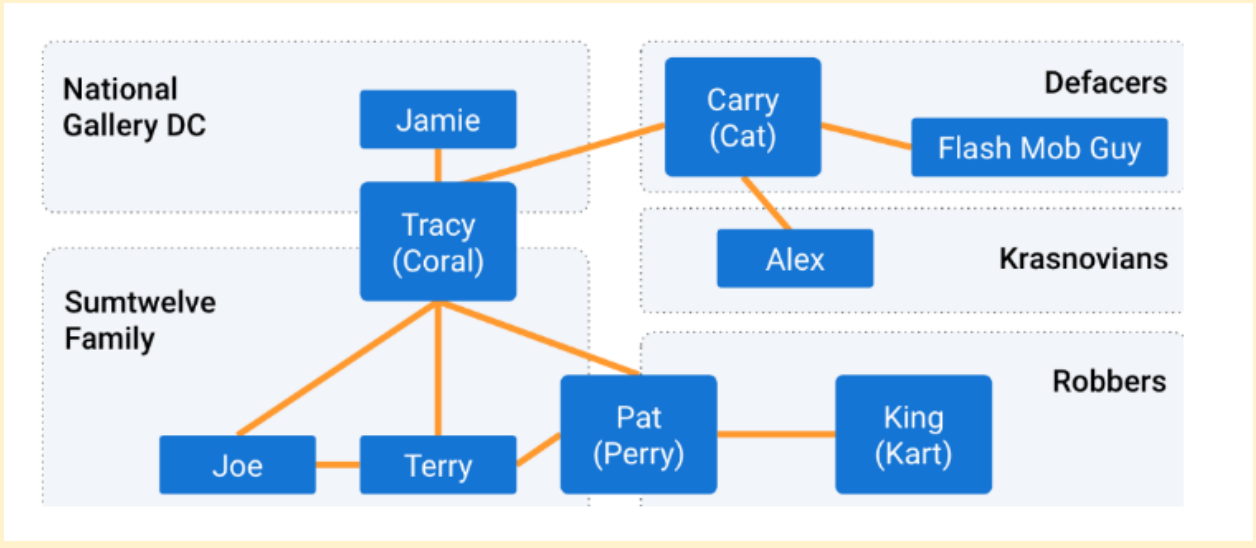
Phone Number: (202) 725-2124
Email: carrysum2012@yahoo.com
Relationship: Tracy's friend

King:

Phone Number: unknown
Email: throne1966@gmail.com
Relationship: Pat's friend

With the help of her brother Pat (aka Perry), Tracy (aka Coral) plotted together to steal valuable stamps from the National Gallery. They used alias emails to try and hide their identity.

***Persons of interest***



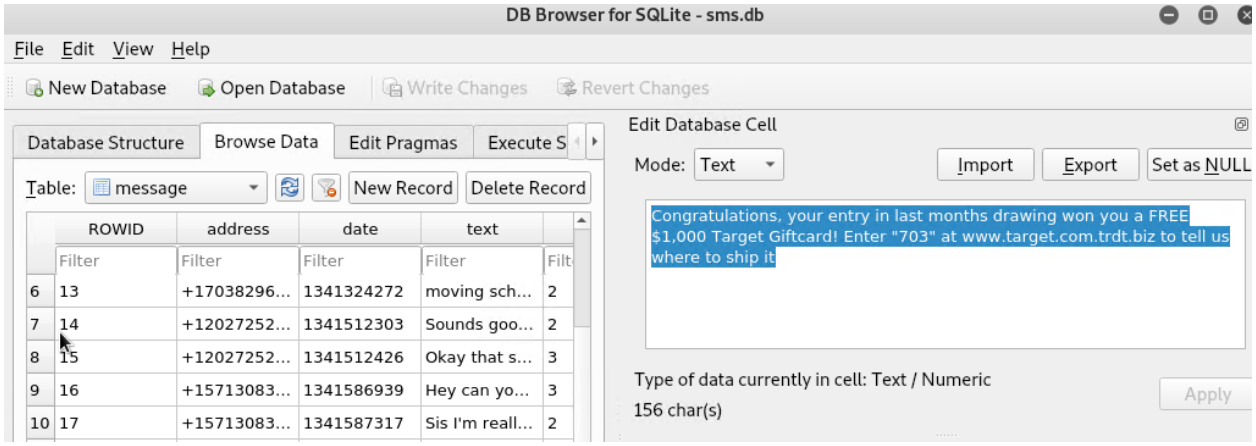

# Evidence relating to theft of valuable stamps

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

See Artifact 27, the needs.txt file, shows tools that could have been used to help steal and get away with the valuable stamps (spray paint/smoke grenade/smokes/ropes and javelin).

```
-A rope and javelin (using alternative means to break in)

-tactical turtlenecks ( what i will be wearing)

-spray paint (for the cameras)

-vibram five finger shoes (in order to walk silently)

-pack of smokes (detecting lasers)

-smoke grenades (use as a means of escape if caught)
```

The evidence shows that Carry and Tracy planned a flash mob on the same day they planned to sneak a tablet into the gallery (see Appendix - Artifact 14, 15, 24, 25). This was likely the distraction they needed to get the tablet in and have King make away with the loot. More evidence, being a possible payoff method of a $1000 target gift card was sent over email (Artifact 12). This payment was around the same time Tracy and Carry meetup to discuss the operation (Artifact 10 and 11). The website is a clue used to show that the site was not actually a target site. The domain ended with .trdt.biz which would have taken you to a separate site to help disguise another item.




In searching for stamp queries I found 3 pdfs of stamps: Stamp_insurance1.pdf - Stamp_insurance2.pdf - Stamp_insurance3.pdf; shown below to show the value that some of these stamps had. path shown here for reference.

Stamp insurance 1.pdf 100%

NATIONAL GALLERY DC
WASHINGTON

**Memorandum of Insurance Assurance:**

**TO: MyIStamp Collections**

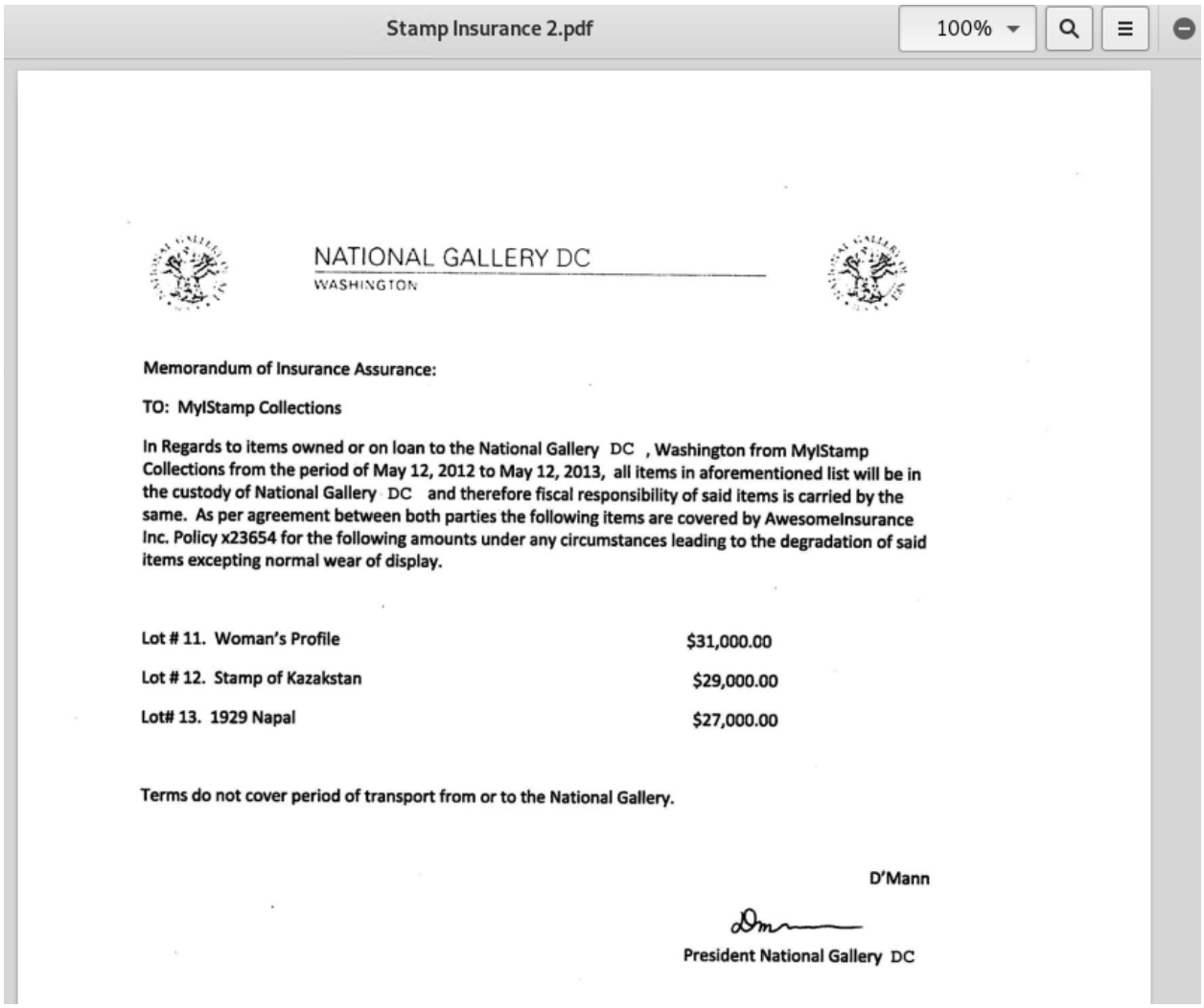
**In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.**

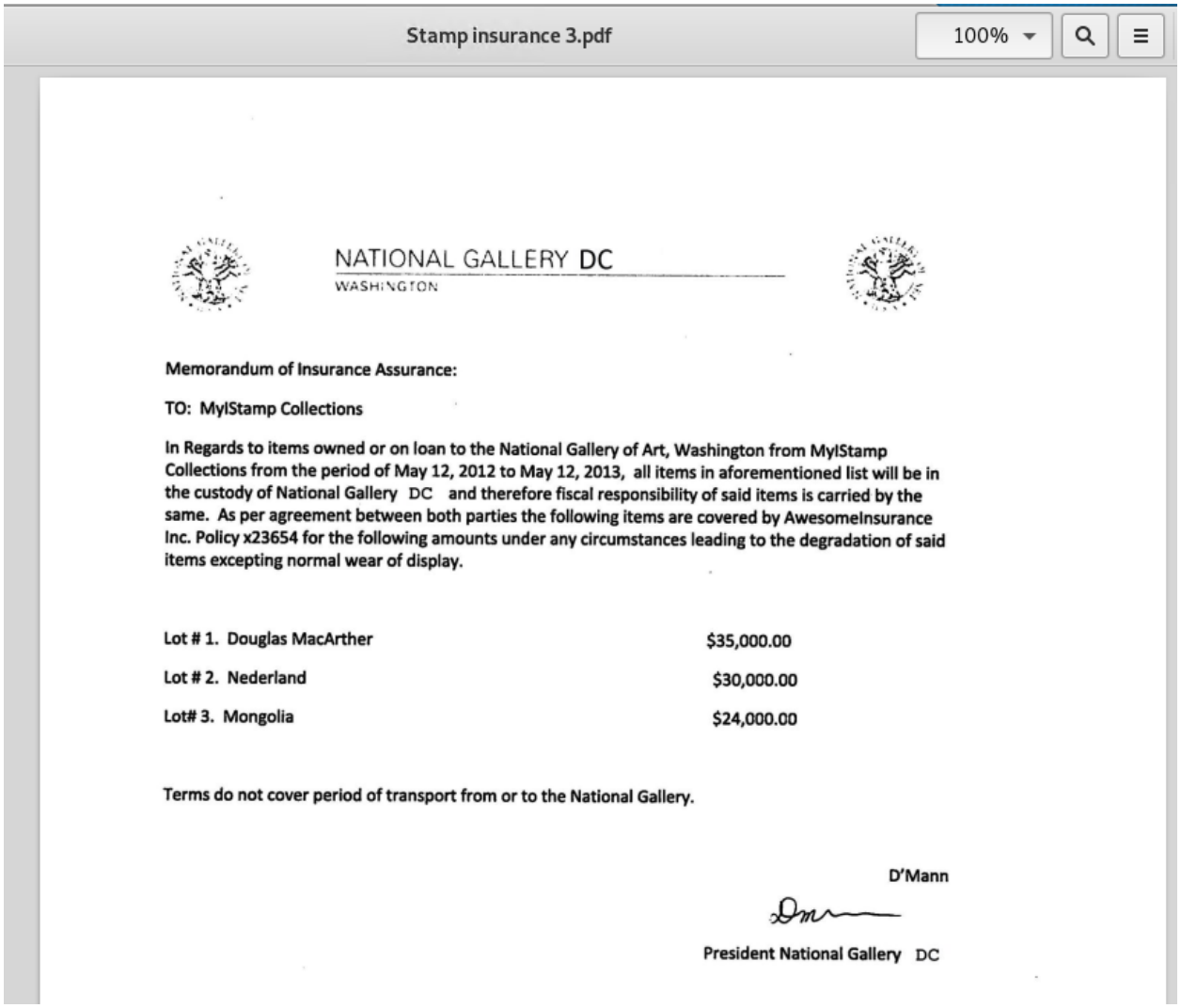
| | |
|---|---|
| **Lot # 25. Armed Forces Reserve** | **$43,000.00** |
| **Lot # 26. Stamp of Kazakstan2** | **$29,000.00** |
| **Lot# 27. BradyCo.** | **$12,000.00** |

**Terms do not cover period of transport from or to the National Gallery.**

**D'Mann**

**President National Gallery DC**


Stamp Insurance 2.pdf
100%
NATIONAL GALLERY DC
WASHINGTON
Memorandum of Insurance Assurance:
TO: MyIStamp Collections
In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.
Lot # 11. Woman's Profile $31,000.00
Lot # 12. Stamp of Kazakstan $29,000.00
Lot# 13. 1929 Napal $27,000.00
Terms do not cover period of transport from or to the National Gallery.
D'Mann
President National Gallery DC




Artifacts 6-8 show that there was a financial motivation to get some quick cash so Tracy can afford to keep her daughter Terry in school. She then reaches out to her brother Pat to get his help to form a plan for the heist (Artifact 9). Evidence that Pat and Tracy blackmailed and threatened King to help with the “heist at the national gallery” was clearly stated in the email between these three and Pat didn’t think to use his alias and links him directly to the crime (Artifact 18). The message from Tracy to Carry shows that they had indeed planned the flashmob which would have been the distraction they needed to pull the security away long enough for the heist (Artifact 25).

# 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 direct evidence that they defaced the museum but there were several clues that show they did have the cover and materials to vandalize the museum. See Artifact 27, the needs.txt file, added for reference, shows tools that could have been used to deface the museum (spray paint/smoke grenade/smokes/ropes and javelin).

# Plot Timeline

***Also see Appendix A below***

- 06/19/2012 Pat emails Tracy from his alias email and tells her to use her alias email too.
- 06/19/2012 Pat sends an email in French from his alias email, possibly a hidden message.
- 07/03/2012 Tracy tried to get some help with Terry's tuition from Joe but he will not help unless Terry moves in with him creating a need for some quick cash.
- 07/03/2012 Terry states that she would rather live with her father than switch schools.
- 07/03/2012 Carry and Tracy meet up in person to discuss something in private.
- 07/06/2012 Tracy sends a message to Pat that she needs to talk urgently about something.
- 07/06/2012 Tracy receives a suspicious message from target about a $1000 gift card which is likely a payoff to someone. Possibly how Carry was paid off.
- 07/09/2012 Coral (alias)sends Tracy  (herself) a zip file with the information about the stamps and their value.
- 07/09/2012 Carry emails Tracy to see if she can help her get the tablet into the museum bypassing the security.
- 07/10/2012 Tracy agrees to help Carry get the tablet through security and asks when she would like to look around.
- 07/10/2012 Pat texted Tracy to change the doc type of txt file to a pdf to obfuscate its use.
- 07/10/2012 Pat (using his actual email incriminating himself) emails King (throne) and Tracy (coral blue email alias). Pat threatens to turn King in if he doesn't help with the "heist" at the gallery. This is the smoking gun that proves they colluded to steal these stamps and that all three of them were involved directly.

- 07/11/2012 Tracy messages Carry that she will meet her out front and take the tablet in with her.
- 07/12/2012 Carry and Tracy email one another and Tracy states she needs the money but to be careful. Carry says not to worry and that it will be gun (possible reference to weapons used?)
- 07/12/2012 Tracy messages Carry about how the flash mob is going (the security distraction)

# Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy used the alias "Coral" coralbluetwo@hotmail.com and her brother Pat used the alias "Perry" perrypatsum@yahoo.com to conspire together with secret messages and instructions.
- There were three main parties involved in the plot to steal stamps from the museum, being: Tracy, Pat and King. Carry was likely involved but didn't find the direct evidence in writing.
- Tracy had hit hard times and couldn't afford the private school and needed money for Terry's school.
- The school costs could have been the cause for the robbery.
- There was a suspicious 1000$ gift card from "target" that could have been how they washed the payment to Carry.
- There was a lot that went into Tracy's plan to steal the stamps and there is a lot of evidence that she took steps to hide her correspondence with the team.
- Carry, Tracy's friend, took extra steps to sneak her tablet into the museum even though she knew the guards wouldn't allow it and used Tracy as the inside person to get this key tool into the museum.
- Carry and Tracy used a flash mob to distract the security guards while the robbery was taking place. Would appear that this is the time that King pulled off the heist.
- Pat appears to have blackmailed King into helping them in their scheme.
- The locations of the Wifi and Cell towers will take further analysis to determine if the locations and times of use would correlate to the robbery at this time.

# 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 | 06/12/2012 9:25:04 | Text from Tracy to Terry | what are you up to this weekend? | vol5/mobile/Library/SMS/sms.db |
| 2 | 06/13/2012 5:30:28 | Text from Terry to Tracy | I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook | vol5/mobile/Library/SMS/sms.db |
| 3 | 06/19/2012 14:39:04 | F: perrypatsum@yahoo.com<br>T: coralbluetwo@hotmail.com<br>Subject: Crazydave by the VMs | Secret .mp3 file Crazydave1.mp3. Base should be bass so some hidden message there too?<br><br>"Just got your email. That took longer than expected! Oh well! you've got to check out this new song by the VMs. i love the Base..Tell me what you think!"<br><br>*Contained an encoded mp3 that contains instructions | /INBOX.mbox/Messages |
| 4 | 06/19/2012 20:06:33 | F: patsumtwelve@gmail.com<br>T: tracysumtwelve@gmail.com | Email message in French<br><br>*possibly a hidden message | /vol5/mobile/Library/Mail/Protected Index |
| 5 | 06/19/2012 20:26:47 | F: perrypatsum@yahoo.com<br>T: tracysumtwelve@gmail.com | Tracy, talked to our brother about an email. You should have our friend, Alias, send me an email. Thanks Perry | /vol5/mobile/Library/Mail/Protected Index |
| 6 | 07/03/2012 09:29:37 | F/T: joe.sumtwelve@gmail.com<br>T/F: | Joe, sorry to bother you, but I have a serious question about Terry and her school. Her tuition is getting a bit too | /vol5/mobile/Library/Mail/Protected |

| | | | | |
|---|---|---|---|---|
| | | tracysumtwleve@gmail.com | much for me right now and I could use a little help. I hate to impose on you for this, but is there any way you would be willing to help me out with her tuition this year?<br>Sorry Tracy. I'm not going to be paying for Terry's school if shes not living with me. I hope things take an upturn for you<br><br>*more financial motivation | Index |
| 7 | 07/03/2012<br>13:41:51 | F: Tracy<br>T: Terry | Hey honey. I'm not sure if we can afford Prufrock anymore….What do you think about maybe switching to someplace else?<br><br>*Evidence that they needed money | vol5/mobile/Library/SMS/sms.db |
| 8 | 07/03/2012<br>14:04:32 | F: Terry<br>T: Tracy | moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools :( | vol5/mobile/Library/SMS/sms.db |
| 9 | 07/06/2012<br>09:10:54 | F: Tracy<br>T: Pat | Urgent text to call soon. | vol5/mobile/Library/SMS/sms.db |
| 10 | 07/06/2012<br>16:27:16 | Tracy to Carry | I have a table inside | vol5/mobile/Library/SMS/sms.db |
| 11 | 07/06/2012<br>16:27:50 | Carry to Tracy | Okay brt | vol5/mobile/Library/SMS/sms.db |
| 12 | 07/06/2012<br>19:36:35 | from 206-910-0932 to Tracy | Congratulations, your entry in last months drawing won you a free $1000 Target gifftcard! Enter "703" at www.target.com.trdt.biz to tell us where to ship it<br><br>*possibly the payment method for the deal soon after the meeting with Carry | vol5/mobile/Library/SMS/sms.db |
| 13 | 07/09/2012<br>07:47:58 | F: tracysumtwelve@gmail.com<br>T: coralbluetwo@hotmail.com | Correspondence from Coral to Tracy (her alias). Contains a Documents.zip about insurance information for the | /INBOX.mbox/Messages |

| | | | | |
|---|---|---|---|---|
| | | Subject:somethings | stamps, showing their value. (see pictures of the stamps values above) | |
| 14 | 07/09/2012 unclear time | F: carrysum2012@yahoo.com T: tracysumtwelve@gmail.com | Hey I was wondering if there was any way you could help me get my tablet into the gallery. I know security isn't to keen on computers and the like in the gallery, but maybe you could pull some strings and get it in for me? I can make it worth your while :)..... | vol5/mobile/Library/Mail/Protected Index |
| 15 | 07/10/2012 unclear time | F/T: carrysum2012@yahoo.com T/F: tracysumtwelve@gmail.com | Awesome this will be a big help. Can i come in tomorrow, around 9? - - Hey, I can definitely help get your table in. Our security guards can be pretty ridiculous sometimes! When would you want to get in and take a look around? | vol5/mobile/Library/Mail/Protected Index |
| 16 | 07/10/2012 9:26:19 | F: Pat T: Tracy | (Attachment needs to be changed to pdf. Altering doc types to obfuscate.) hey sis yo friend coral got a email the attachment needs to be change to pdf let her know | vol5/mobile/Library/SMS/sms.db |
| 17 | 07/10/2012 15:58:04 | T: Pat F: Tracy | Sure thing I'll get on it | vol5/mobile/Library/SMS/sms.db |
| 18 | 07/10/2012 15:24:57 | F:patsumtwelve@gmail.com T: throne1966@hotmail.com CC: coralbluetwo@hotmail.com Subject: can't pass up | King, Long time no see….I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole officer go years back. He is a very strict fellow. If he were to find out htat you were dealing drugs and shooting dope in your veins every night, i feel he wouldn't be too happy. It's very easy for a person to phone the feds with an anonymous tip that you are on drugs and the location of your stash. All they have to do is ive you a drug tes and | /INBOX.mbox/Messages |

| | | | | |
|---|---|---|---|---|
| | | | since you're on parole, the feds don't need a search warrant. Well hit me up. You know where to find me.<br><br>*the full blackmail message (Blackmailing King (throne - Kart) and getting them involved. A robber for the heist. Tracy's alias email coral was used. Sender IP 209.85.214.180.) | |
| 19 | 07/10/2012<br>17:18:38 | F: Tracy<br>T: Terry | Going to lunch. You want to go? | vol5/mobile/Library/SMS/sms.db |
| 20 | 07/10/2012<br>18:19:24 | F: Tracy<br>T: Terry | Back at work | vol5/mobile/Library/SMS/sms.db |
| 21 | 07/10/2012<br>18:58:24 | T: Tracy<br>F: Terry | I'm busy. Maybe this weekend if dad isn't busy | vol5/mobile/Library/SMS/sms.db |
| 22 | 07/11/2012<br>12:41:45 | F: Carry<br>T: Tracy | I'm almost there where should I meet you? | vol5/mobile/Library/SMS/sms.db |
| 23 | 07/11/2012<br>12:49:08 | F: Tracy<br>T: Carry | Just meet me out front, I'll take the tablet in. | vol5/mobile/Library/SMS/sms.db |
| 24 | 07/12/2012<br>01:24:00 | F/T:<br>carrysum2012@yahoo.com<br>T/F:<br>tracysumtwelve@gmail.com | Hey so i'm putting together this eve. > (T)Okay carrie I'm going to send this but you need to make sure no one else sees it okay I could get in a bunch of trouble. I want to help you and I could really use some extra cash too but please please be careful > (C)don't Worry so much. It willbe gun. > What do you mean by that?<br><br>*very suspicious nervous energy and talk about a gun? | vol5/mobile/Library/Mail/Protected Index |
| 25 | 07/12/2012<br>17:06:45 | F: Tracy<br>T: Carry | How's the flashmob going?<br><br>*the diversion | vol5/mobile/Library/SMS/sms.db |
| 26 | 07/13/2012 | T: Tracy | I really want to go to Dad's this | vol5/mobile/L |

| | | | | |
|---|---|---|---|---|
| | 01:02:10 | F: Terry | weekend. He said he'll take me shopping for school | ibrary/SMS/sms.db |
| 27 | n/a FOR REFERENCE (not an email or text) | text file (needs.txt) | lists the gear used for the job:<br>`-A rope and javelin (using alternative means`<br>`-tactical turtlenecks ( what i will be wear`<br>`-spray paint (for the cameras)`<br>`-vibram five finger shoes (in order to walk`<br>`-pack of smokes (detecting lasers)`<br>`-smoke grenades (use as a means of escape i` | vol5/mobile/Library/POP-coralbluetwo@hotmail.com/INBOX.mbox/Attachments/60/2/needs.txt |

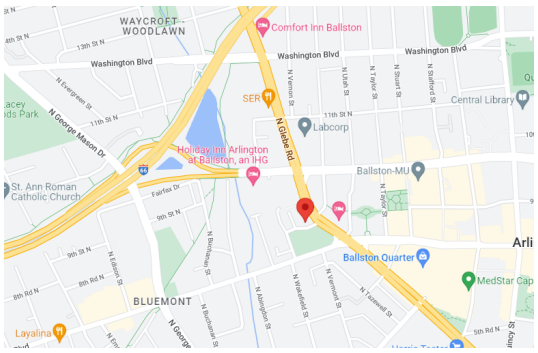
# Appendix B: WiFi and GPS Location Information

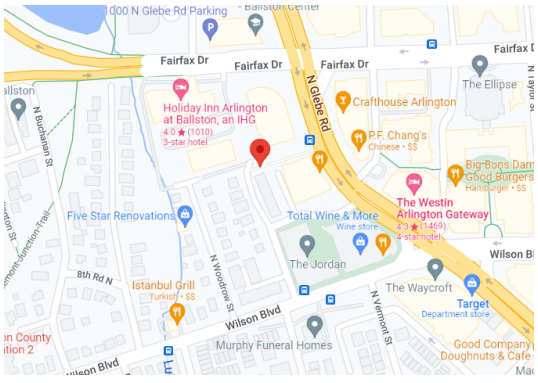
## Location Information

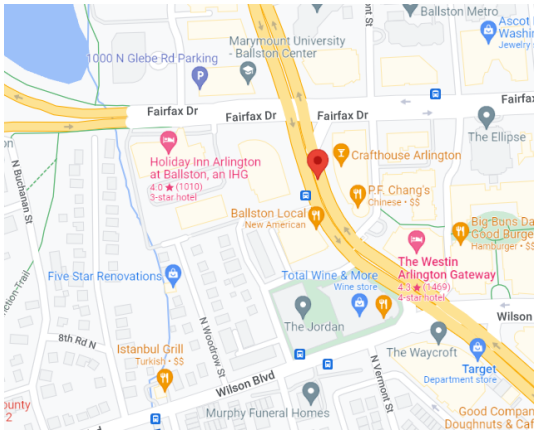
WifiLocation: found in /vol5/root/Library/Caches/locationd/consolidated.db

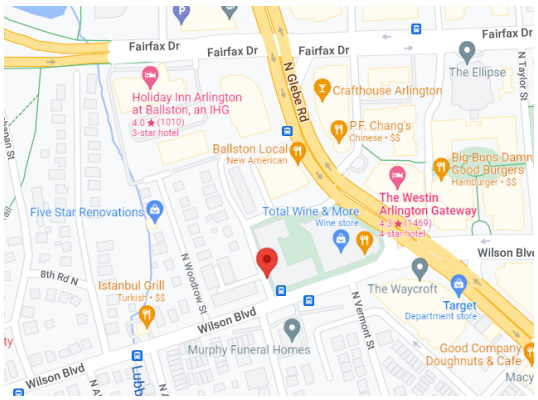
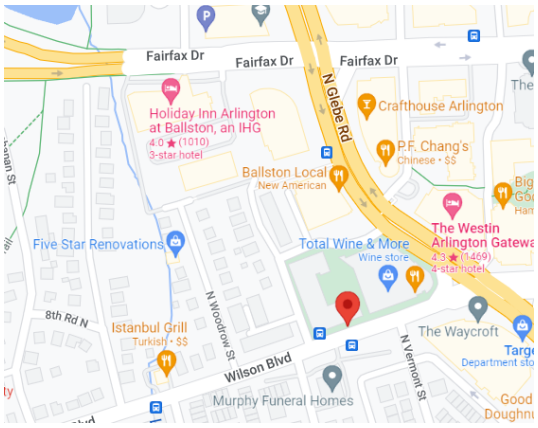
Group members:

---

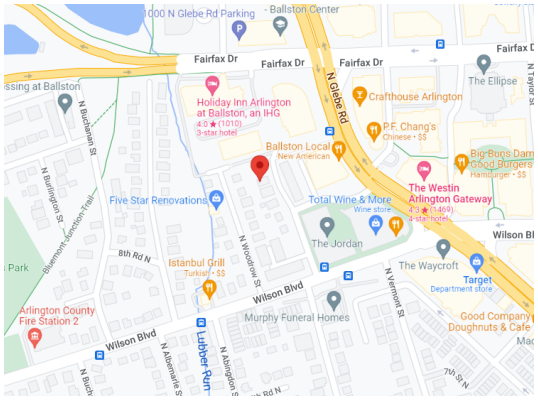
| Location Information | | | |
|---|---|---|---|
| **Artifact #** | **Latitude/Longitude** | **Address** | **Map Screenshot** |
| A | 38.88055896<br>-77.11553561 | 900 N Glebe Rd,<br>Arlington, VA 22203 |  |

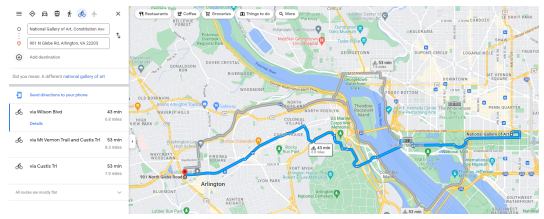
| | | | |
|---|---|---|---|
| B | 38.88106083<br>-77.11533838 | 901 N Glebe Rd,<br>Arlington, VA 22203 |  |
| C | 38.88005346<br>-77.11595332 | 801 N Wakefield St,<br>Arlington, VA 22203 |  |
| D | 38.88093715<br>-77.11640596 | Bluemont, Arlington,<br>VA 22203 |  |

| | | | |
|---|---|---|---|
| E | 38.87996816<br>-77.11601394 | 801 N Wakefield St,<br>Arlington, VA 22203 |  |
| F | 38.88138395<br>-77.11556851 | 851-977 N Glebe Rd,<br>Arlington, VA 22203 |  |
| G | 38.88139647<br>-77.11564362 | 982-900 N Glebe Rd,<br>Arlington, VA 22203 |  |

| | | | |
|---|---|---|---|
| H | 38.87974703<br>-77.11598318 | 801 N Wakefield St,<br>Arlington, VA 22203 |  |
| I | 38.87969022<br>-77.1154859 | 801 N Wakefield St,<br>Arlington, VA 22203 |  |
| J | 38.88161849<br>-77.11495679 | 901 N Glebe Rd,<br>Arlington, VA 22203 |  |
| L | 38.87982344<br>-77.11606764 | 802 N Wakefield St,<br>Arlington, VA 22203 |  |

| | | | |
|---|---|---|---|
| M | 38.88054466<br>-77.11439651 | 801 N Glebe Rd,<br>Arlington, VA 22203 |  |
| N | 38.88053315<br>-77.11445105 | 801 N Glebe Rd,<br>Arlington, VA 22203 |  |
| O | 38.88049459<br>-77.11436617 | 801 N Glebe Rd,<br>Arlington, VA 22203 |  |
| P | 38.88060778<br>-77.11446964 | 801 N Glebe Rd,<br>Arlington, VA 22203 |  |

| | | | |
|---|---|---|---|
| Q | 38.88046348<br>-77.11443722 | N Glebe Rd, Arlington, VA 22203 |  |
| R | 38.88053494<br>-77.11453396 | 801 N Glebe Rd, Arlington, VA 22203 |  |
| S | 38.88055533<br>-77.11455225 | 801 N Glebe Rd, Arlington, VA 22203 |  |
| T | 38.88063263<br>-77.11677783 | 828 N Wakefield St, Arlington, VA 22203 |  |

| | | | |
|---|---|---|---|
| K | MAPPED TO GALLERY | doesn't appear to be close to the above |  |

The consolidated.db file gave coordinates that all were in around the same area and were a good distance away from the gallery at the time so nothing can be confirmed about the locations found within this database.