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

Case Report

National Gallery DC

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

Team Members:

Jordan Heller

Drew Newton

Andrew Arnold

Lauren Ferguson

Austin Obeng

Jett Janssen

# 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.

* Alex is seeking to embarrass the United States and damage public relations by defacing foreign art belonging to Majavia that is on display at the National Gallery during the month of July. He plans a flash mob with Carry, who hides many of her correspondence in steg files and encrypted files.
* Carry contacts Tracy about organizing a “Flash mob” at the gallery, and will give money for her help. Tracy agrees and the two stay in correspondence about sneaking in Carry’s tablet to the museum.
* Tracy has been in contact with her brother Pat about plans to steal stamps from the National Gallery.
* Criminal with alias “King” blackmailed by Pat to aid in the National Gallery heist. He shared a list of supplies to bring to the heist with Pat and Tracy.

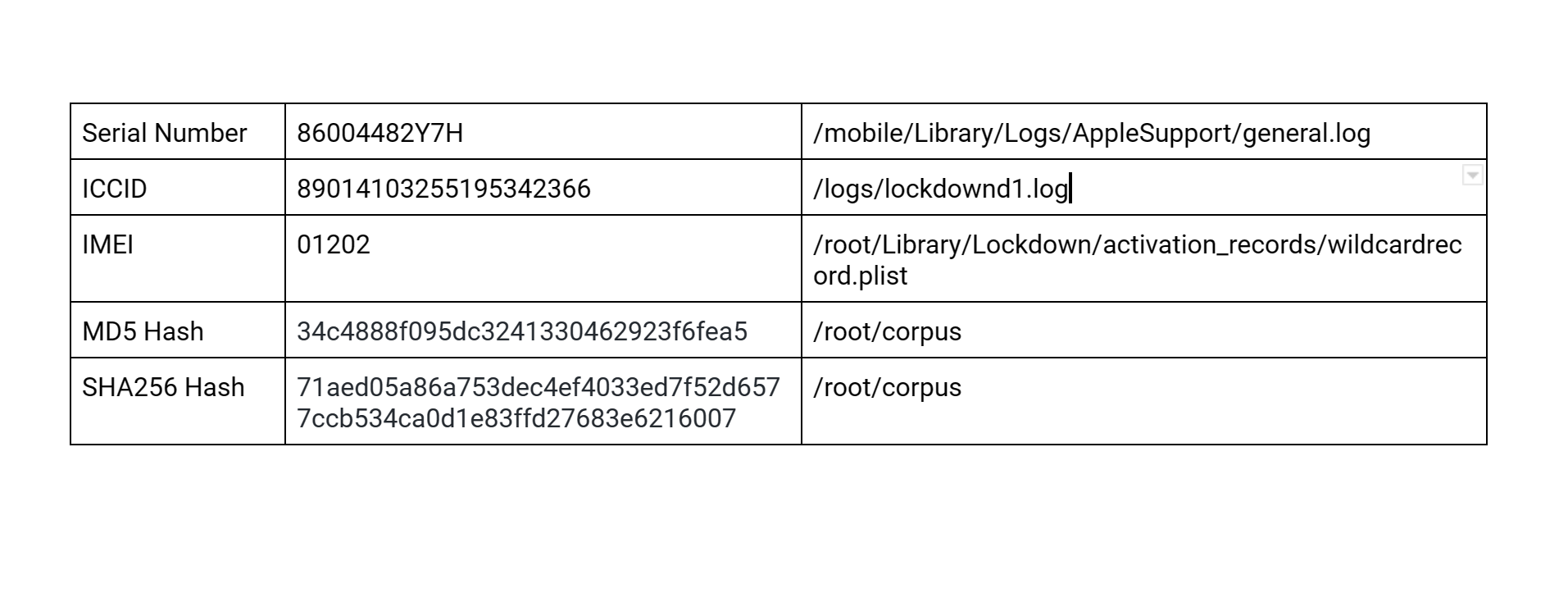
### Equipment and Tools

Using the digital forensic platform Autopsy, investigators secured information from multiple emails with attachment, sms text messages and GPS locations that were plugged into Google maps. Within a Kali VM, investigators viewed hashes and utilized a program called fcrackzip to crack a document.zip’s password.

# Details of Tracy’s iPhone

[Module 21 iPhone Details Worksheet](https://docs.google.com/document/d/1F0VZXZdCVohIwCzJjeaAFipWKKQU4D6jJ2vWQwxSHro/edit?usp=sharing)





# Evidence to Establish Personas

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

Tracy (“Coral”):

Phone Number: (703) 340-9961

Personal Email: tracysumtwelve@gmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused

Pat (“Perry”)::

Phone Number: 571-308-3236

Email: patsumtwelve@gmail.com , perrypatsum@yahoo.com

Relationship: Tracy’s Brother

Terry:

Phone Number: 703-829-6071

Email: Currently Unknown

Relationship: Tracy and Joe’s Daughter

Joe:

Phone Number: Currently Unknown

Email: joe.sum.twelve@gmail.com

Relationship: Soon-to-be ex-husband of Tracy

Carry (“Cat”):

Phone Number: 202-725-2124

Email: carrysum2012@yahoo.com

Relationship: somewhat criminally involved individual and Krasnovian supporter who

shares family ties with Alex. Acquaintances with Tracy.

King (“Kart”):

Phone Number: N/A

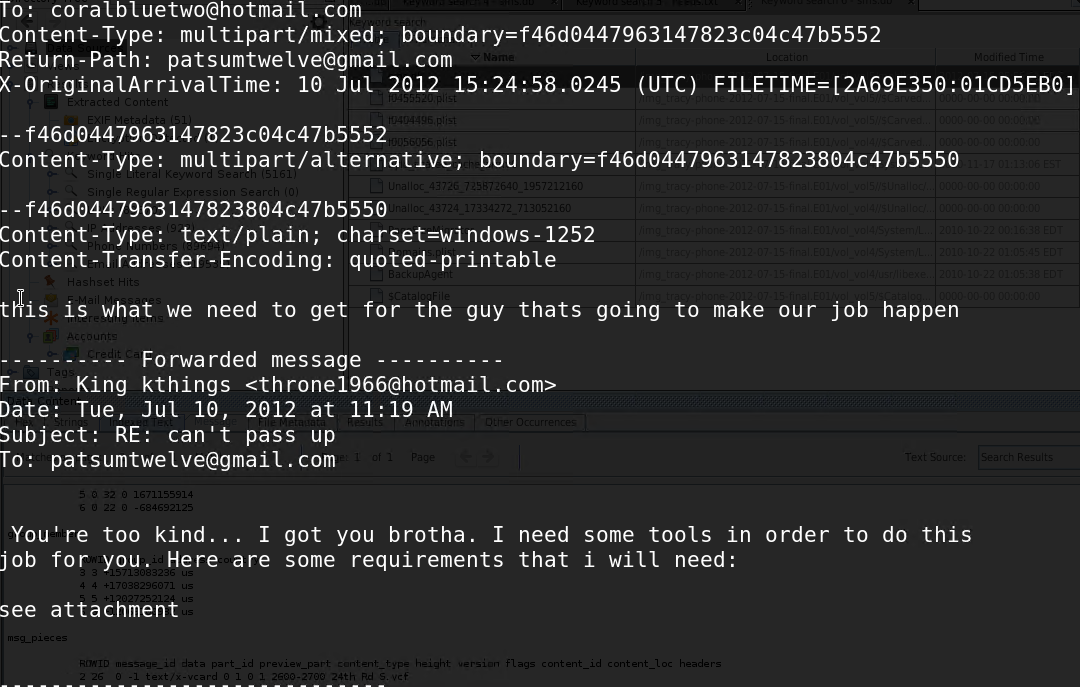
Email: throne1966@hotmail.com

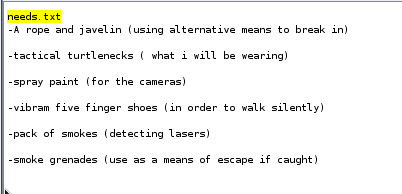
Relationship: blackmailed by Pat to participate in heist

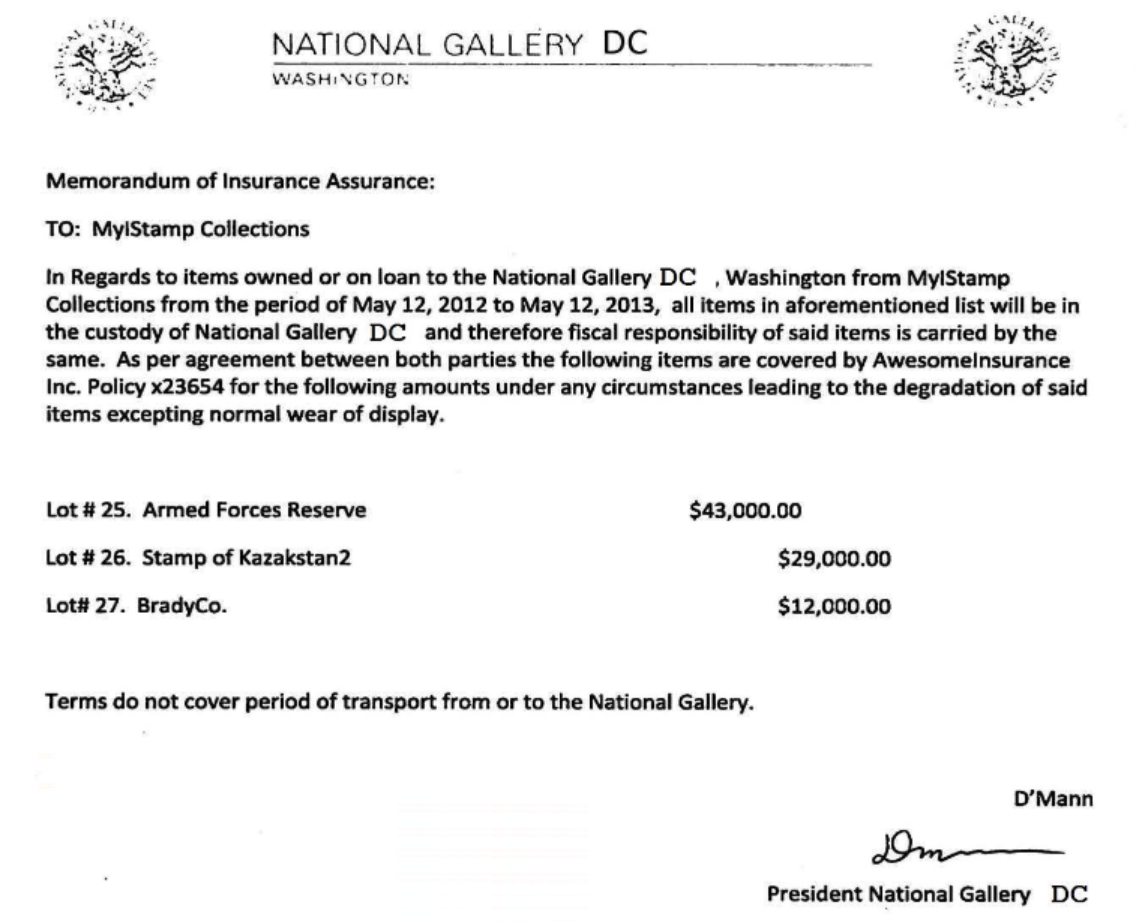
# Evidence relating to theft of valuable stamps

Primary evidence of stamp fraud is found in Terry’s email that she sent to herself, see Email #3, which includes a document.zip attachment. The password to this zip file is Hercules, which was cracked using fcrackzip. It contains PDFs of stamp insurance. Pictures of stamps on Terry’s device match the description of the stamps that were insured.

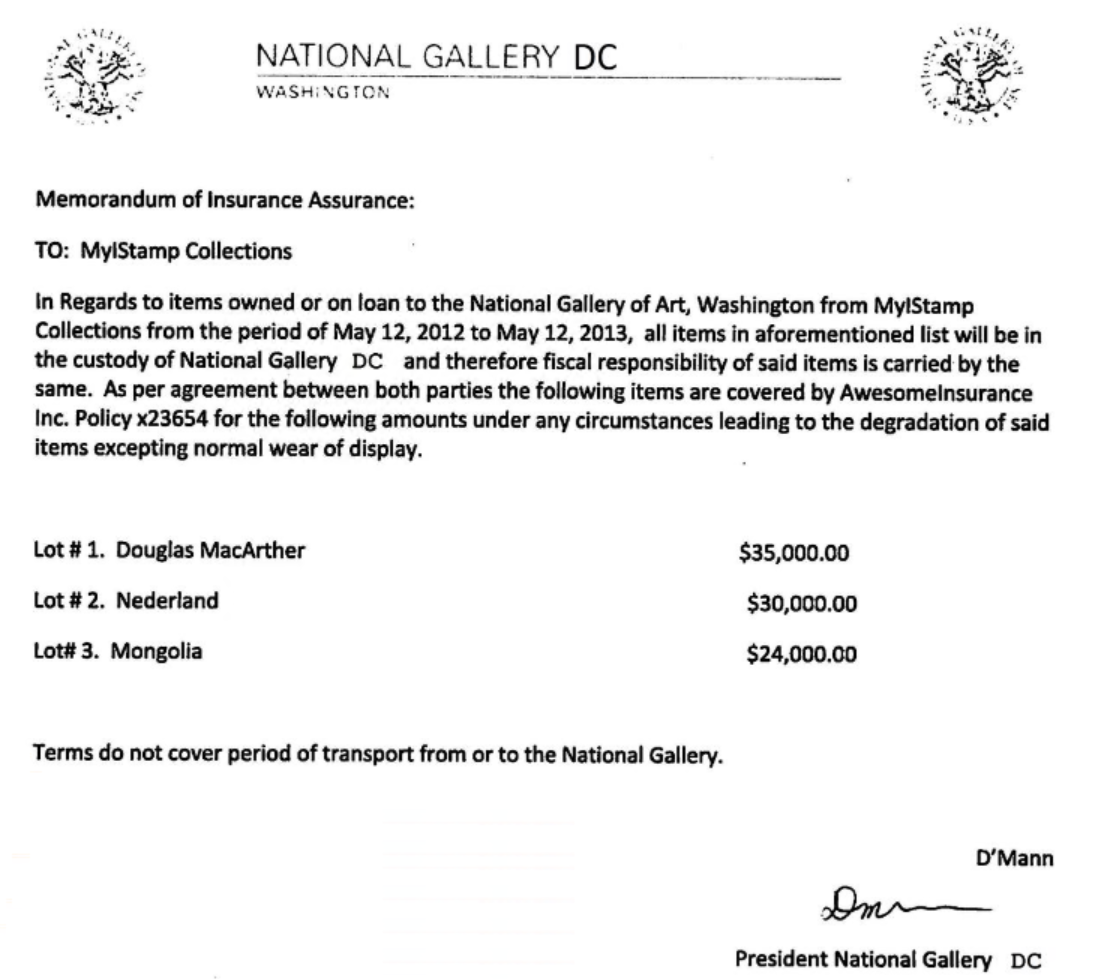
As evident in Email #4, “King” is being blackmailed to participate in the heist by Pat with threats to call his parole officer. Detailed in the case report is Pat’s plan on stealing the stamps during the heist.



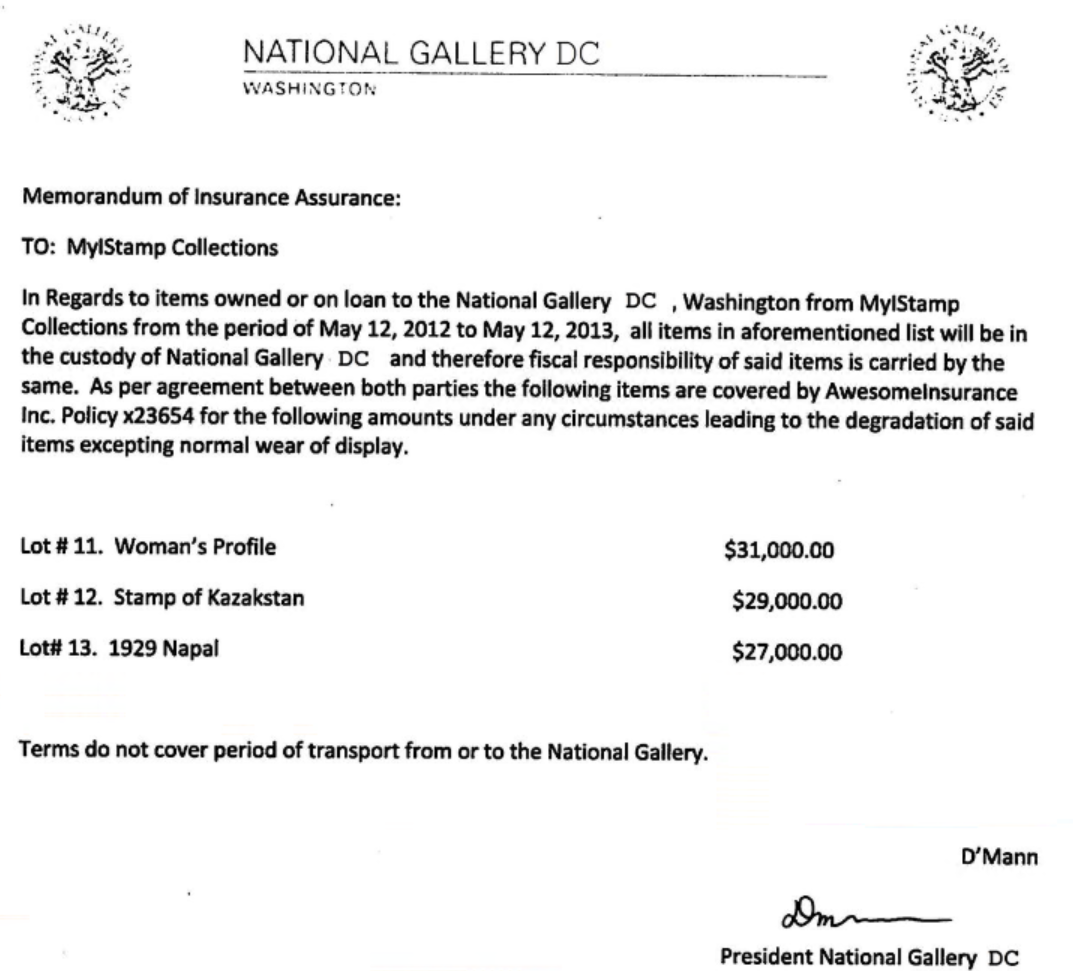










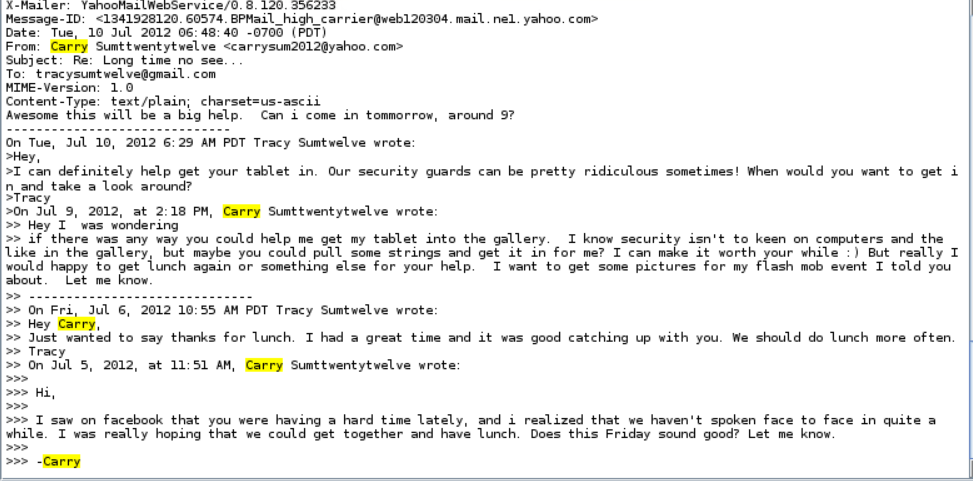


# Evidence relating to defacement of museum art

Email #4 from [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com) to [throne1966@hotmail.com](mailto:throne1966@hotmail.com) and [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) details a plan to deface the national gallery. Attached is needs.txt, which lists supplies to bring to the heist. Supplies include a rope and javelin, tactical turtlenecks, spray paint, vibram five finger shoes, pack of smokes, and smoke grenades.

In Email #6, [carrysum2012@yahoo.com](mailto:carrysum2012@yahoo.com) asks tracysumtwelve@gmail.com to sneak her tablet into the gallery for her flash mob event. Tracy agrees to help her. Over text, SMS #2, Carry setting up plans to meet Tracy for lunch at Bubba’s grill. Tracy tells Carry to meet outside so that she can sneak her tablet into the gallery. In a follow up, SMS #6, Tracy asks Carry how the flash mob is going.

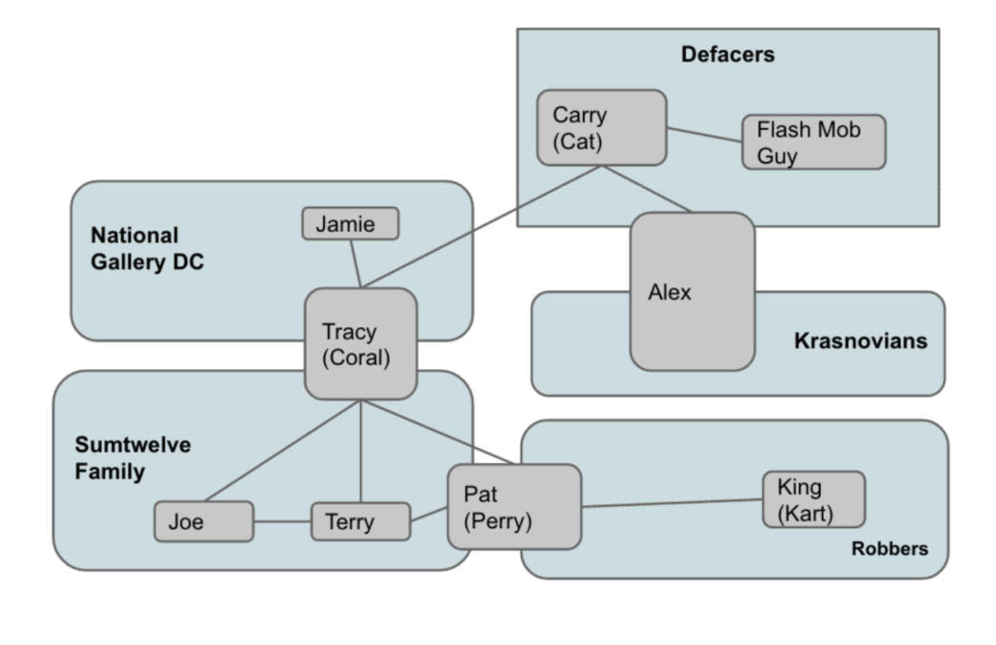
SMS #5 likely shows payment from Carry or Alex to Terry in the form of $1000 spoofed Target Gift Card.



# Plot Timeline

* Tue, Jun 19, 2012 02:38:59 PM Pat emails Tracy with the Crazydave1.mp3 audio recording attachment.
* Thu, Jul 5 2012 06:18:23 PM Tracy and Carry agree to meet at Bubbas grill to discuss the plan.
* Fri, Jul 6 2012 11:49:31 AM Pat emails someone who is named King and blackmails them to take part in a heist at the National Gallery.
* Fri, Jul 6 2012 4:27:16 PM Tracy and Carry confirm the meeting at Bubba’s.
* Sat, Jul 7 2012 7:36:35 PM Tracy receives an SMS message from an unknown number that states that she has received a Target Gift Card worth $1000. The URL, [www.target.com.trdt.biz](http://www.target.com.trdt.biz), is not actually related to Target. Conclusion, this is payment for services.
* Mon, Jul 9 2012 10:44:11 AM Tracy sent an email containing attachments documents.zip, docs.zip. Inside these attachments were documents on stamp insurance.
* Tue, Jul 10 2012 11:19 AM Pat forwarded the emails to King. King then replied with a list of materials he will need for the job.
* Tue, Jul 10 2012 11:24 AM Pat forwarded the email with the materials to Tracy (coralblue) on what King needs to get the job done.
* Wed, July 11th, 2012 Tracy conspires with Carry to sneak Carry’s tablet into the gallery.
* Thu, July 12th, 2012 Tracy contacts Carry to ask how the flashmob is going.

Persons under investigation:



# Conclusion

* Tracy’s iphone model 1, 2 includes three of her emails: [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org), [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com), [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com). It also includes her phone number (703) 340-9661.
* Tracy and Pat used alias emails, [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) and [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com), and alias names, Coral and Pat.
* Pat coordinated with “King”, [throne1966@hotmail.com](mailto:throne1966@hotmail.com), to break into the national gallery to steal stamps. Pat blackmails King into cooperating by threatening to call his parole officer.
* Tracy sends herself documents of insured stamps, which match the stamps she is looking to steal.
* Tracy receives a Target giftcard with a spoofed URL for a $1000 Gift Card, likely payment from Carry or Alex.
* There are three clusters of Wi-Fi and Cell locations in Washington, DC.

# Appendix A: Correspondence Evidence

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

| **Master Timeline of NGDC** | | | | |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Header Information** | **Key Information** | **Evidence Location** |
| Email #1 | 11 July 2012 04:18:33 | [microsoft@reply.digitalriver.com](mailto:microsoft@reply.digitalriver.com)  [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: Only 30 days left! Start a free office training course now. | Microsoft office free trial spam. | 01FE9965-A923-40CF-A78A-72CE3BD26571.emlx |
| Email #2 | 19 June 2012 21:39:04 | From Pat to Tracy  [perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)  coralbluetwo@hotmail.com  Subject: Crazydave by the VMs | Perry attached an mp3 file called Crazydave1.mp3. | 3896FC6F-A083-4D39-B0A2-CE6836D44CA.emlx |
| Email #3 | 9 July 2012 10:44:11 | From Tracy to Tracy  [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com) to  [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: things | Attached file documents.zip sent from Tracy to herself | 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx |
| Email #4 | 10 July 2012 08:24:58 | From Pat to Tracy  [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  To [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Pat forwarded King’s email from [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  Subject: can’t pass up | Pat is blackmailing King to help with the heist by threatening to call their parole officer. King sent a list of needs for the heist in needs.txt. Pat then forwarded King’s response to Tracy. | 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx |
| Email #5 | 5 July 2012 12:58:42 | From Woina to Tracy  [Woina.Honril@m57.biz](mailto:Woina.Honril@m57.biz)  To [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: Busy | “I didn’t” is only text. Attached is 000001.doc  And 000002.doc | F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx |
| Email #6 | 9 July, 2012  02:18 PM | From [carrysum2012@yahoo.com](mailto:carrysum2012@yahoo.com)  To [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  Subject: Long time no see… | Carry asks Tracy to sneak her tablet into the gallery for her flash mob event. Tracy agrees to help her. | /vol5//$CarvedFiles/f0408520.plist |
| SMS #1 | July 3, 2012 13:41:51 | From Tracy to Terry  (703) 340-9961  To (703) 829-6071 | Tracy telling Terry that she can no longer afford to pay for her school. | /vol5/mobile/Library/SMS/sms.db |
| SMS #2 | July 5, 2012 18:18:23 | From Carry to Tracy  (202) 725-2124  To (703) 340-9961 | Carry setting up plans to meet Tracy for lunch at Bubba’s grill. | /vol5/mobile/Library/SMS/sms.db |
| SMS #3 | July 6, 2012  15:02:19 | From Tracy to Pat  (703) 340-9961  To (571) 308-3236 | In a series of texts, Tracy frantically tries to get Pat to talk on the phone. | /vol5/mobile/Library/SMS/sms.db |
| SMS #4 | July 6, 2012 16:27:16 | From Carry to Tracy  (202) 725-2124  To (703) 340-9961 | Carry confirms that she has a table inside, presumably at Bubba’s grill. This confirms that their lunch did happen. | /vol5/mobile/Library/SMS/sms.db |
| SMS #5 | July 7 2012 19:36:35 | From a fake Target giveaway to Tracy  (206) 910-0932  To (703) 340-9961 | Scam text claiming that Tracy has won a $1,000 Target giftcard with a spoofed URL. | /vol5/mobile/Library/SMS/sms.db |
| SMS #6 | July 10, 2012 15:26:19 | From Pat to Tracy  (571) 308-3236  To (703) 340-9961 | Text about coral email. Informs Tracy to change email attachment to a pdf. | /vol5/mobile/Library/SMS/sms.db |
| SMS #7 | July 11, 2012 12:49:08 | From Tracy to Carry  (703) 340-9961  To (202) 725-2124 | Tracy tells Carry to meet outside so that she can sneak her tablet into the gallery. | /vol5/mobile/Library/SMS/sms.db |
| SMS #8 | July 12, 2012 17:06:45 | From Tracy to Carry  (703) 340-9961  To (202) 725-2124 | Tracy asks Carry how the flash mob is going. | /vol5/mobile/Library/SMS/sms.db |

### [21.3 Correspondence Evidence Worksheet - MASTER LIST](https://docs.google.com/document/d/1-Jb-DekBVTW0pokL2HplFtxlAqTZu8kG0gMWH9FIy2o/edit?usp=sharing)

# 

# 

# 

# 

# 

# Appendix B: WiFi and GPS Location Information

WiFi location data gathered from the /vol5/root/Library/Caches/locationd/consolidated.db and plotted using easymapmaker.com

Figures B1 - B9 shown below are the plotted latitude and longitude data from her phone.

