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

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

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	Iphone 1, 2	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's phone	preferences/SystemConfiguration/com.apple.mobilegestalt.plist
OS Version	iPhone OS 4.2.1 (8C148)	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28	/mobile/Library/Logs/AppleSupport/general.log
User Email	tracy.sumtewelve@nationalgallerydc.org, tracysumtwelve@gmail.com, coralbluetwo@hotmail.com	mobile/Library/Mail
Phone Number	(703) 340-9661	/logs/lockdownd1.log
Serial Number	86004482Y7H	/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	/logs/lockdownd1.log
IMEI	01202	/root/Library/Lockdown/activation_records/wildcardrecord.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	/root/corpus
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e6216007	/root/corpus

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”):

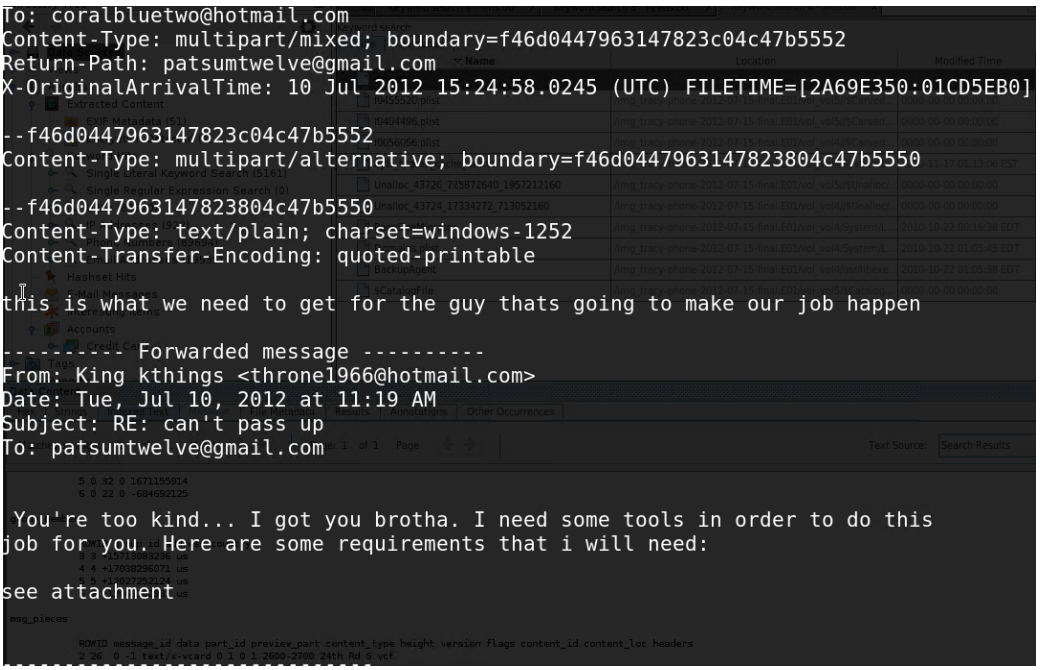
Phone Number: N/A
Email: throne1966@hotmail.com
Relationship: blackmailed by Pat to participate in heist

Evidence relating to theft of valuable stamps

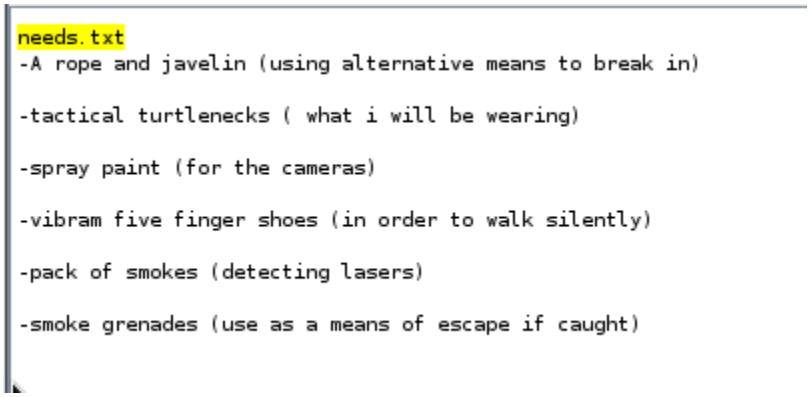
Primary evidence of stamp fraud is found in Terry’s email that she sent to herself, see Email #3, which includes a document.zip attachment. The password to this zip file is Hercules, which was

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.



```
To: coralbluetwo@hotmail.com
Content-Type: multipart/mixed; boundary=f46d0447963147823c04c47b5552
Return-Path: patsumtwelve@gmail.com
X-OriginalArrivalTime: 10 Jul 2012 15:24:58.0245 (UTC) FILETIME=[2A69E350:01CD5EB0]

--f46d0447963147823c04c47b5552
Content-Type: multipart/alternative; boundary=f46d0447963147823804c47b5550

--f46d0447963147823804c47b5550
Content-Type: text/plain; charset=windows-1252
Content-Transfer-Encoding: quoted-printable

this is what we need to get for the guy thats going to make our job happen

---------- Forwarded message ----------
From: King kthings <throne1966@hotmail.com>
Date: Tue, Jul 10, 2012 at 11:19 AM
Subject: RE: can't pass up
To: patsumtwelve@gmail.com

You're too kind... I got you brotha. I need some tools in order to do this
job for you. Here are some requirements that i will need:

see attachment
```



needs.txt

```
-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)
```

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

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, 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 # 1. Douglas MacArther	**$35,000.00**
Lot # 2. Nederland	**$30,000.00**
Lot# 3. Mongolia	**$24,000.00**

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

D'Mann

President National Gallery DC

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

Evidence relating to defacement of museum art

Email #4 from patsumtwelve@gmail.com to throne1966@hotmail.com and 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 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.

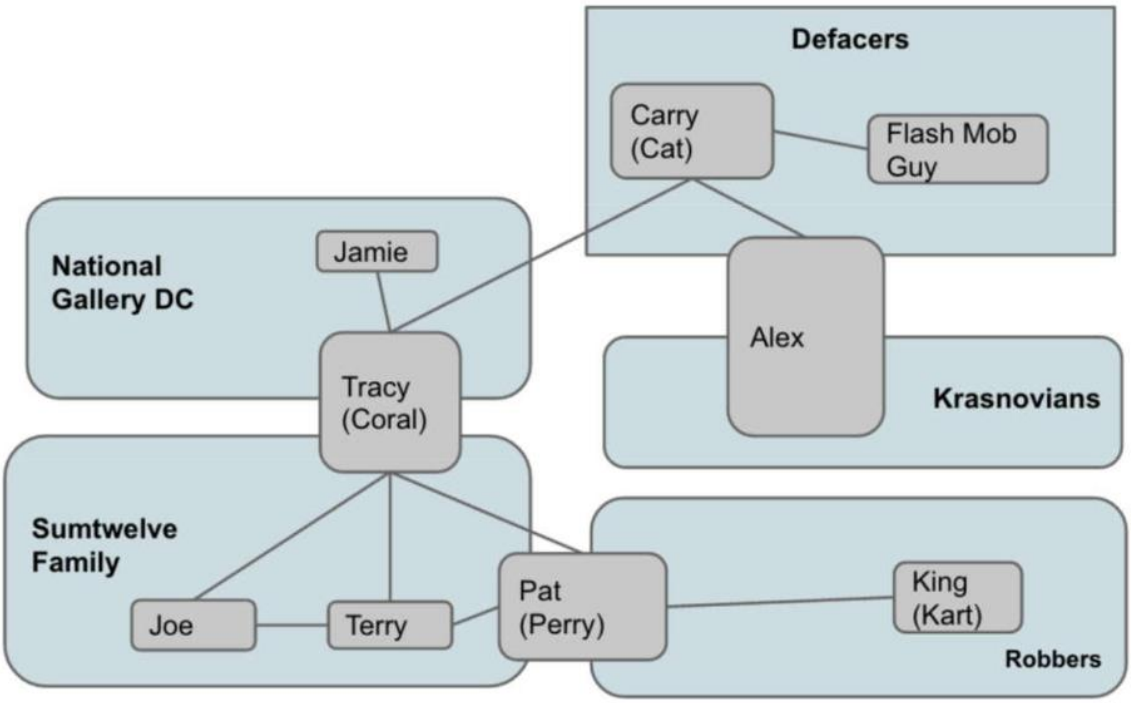
```
X-Mailer: YahooMailWebService/0.8.120.356233
Message-ID: <1341928120.60574.BPMail_high_carrier@web120304.mail.ne1.yahoo.com>
Date: Tue, 10 Jul 2012 06:48:40 -0700 (PDT)
From: Carry Sumttwentytwelve <carrysum2012@yahoo.com>
Subject: Re: Long time no see...
To: tracysumtwelve@gmail.com
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Awesome this will be a big help.  Can i come in tommorrow, around 9?
------------------------------
On Tue, Jul 10, 2012 6:29 AM PDT Tracy Sumtwelve wrote:
>Hey,
>I can definitely help get your tablet in. Our security guards can be pretty ridiculous sometimes! When would you want to get i
n and take a look around?
>Tracy
>On Jul 9, 2012, at 2:18 PM, Carry Sumttwentytwelve wrote:
>> 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 :) But really I
would happy to get lunch again or something else for your help.  I want to get some pictures for my flash mob event I told you
about.  Let me know.
>> ------------------------------
>> On Fri, Jul 6, 2012 10:55 AM PDT Tracy Sumtwelve wrote:
>> Hey Carry,
>> Just wanted to say thanks for lunch. I had a great time and it was good catching up with you. We should do lunch more often.
>> Tracy
>> On Jul 5, 2012, at 11:51 AM, Carry Sumttwentytwelve wrote:
>>>
>>> Hi,
>>>
>>> I saw on facebook that you were having a hard time lately, and i realized that we haven't spoken face to face in quite a
while. I was really hoping that we could get together and have lunch. Does this Friday sound good? Let me know.
>>>
>>> -Carry
```

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, 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, tracysumtwelve@gmail.com, coralbluetwo@hotmail.com. It also includes her phone number (703) 340-9661.

- Tracy and Pat used alias emails, coralbluetwo@hotmail.com and patsumtwelve@gmail.com, and alias names, Coral and Pat.
- Pat coordinated with "King", 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 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 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 to 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	From Pat to Tracy patsumtwelve@gmail.com	Pat is blackmailing King to help with the heist by threatening to call their	9F0508B8-04FB-490E-

	08:24:58	To coralbluetwo@hotmail.com Pat forwarded King's email from throne1966@hotmail.com Subject: can't pass up	parole officer. King sent a list of needs for the heist in needs.txt. Pat then forwarded King's response to Tracy.	A7F0-3E23B0E7C59B.emlx
Email #5	5 July 2012 12:58:42	From Woina to Tracy Woina.Honril@m57.biz To 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 To 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

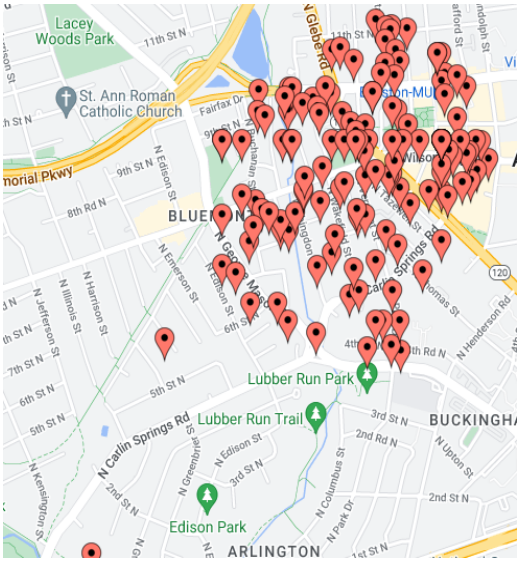
SMS #8	July 12, 2012 17:06:45	From Tracy to Carry (703) 340-9961 To (202) 725-2124	Tracy asks Carry how the flash mob is going.	/vol5/mobile /Library/SMS /sms.db

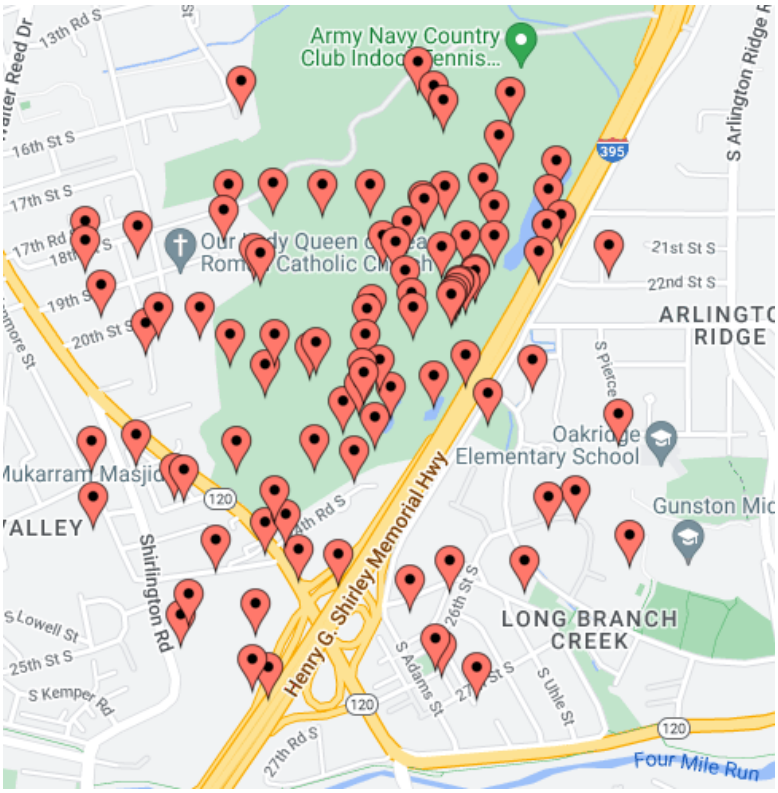
21.3 Correspondence Evidence Worksheet - MASTER LIST

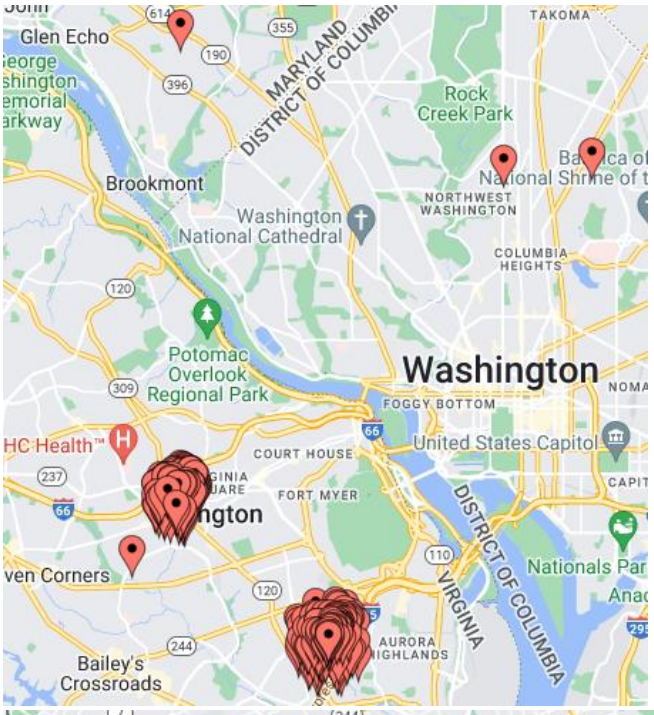
Appendix B: WiFi and GPS Location Information

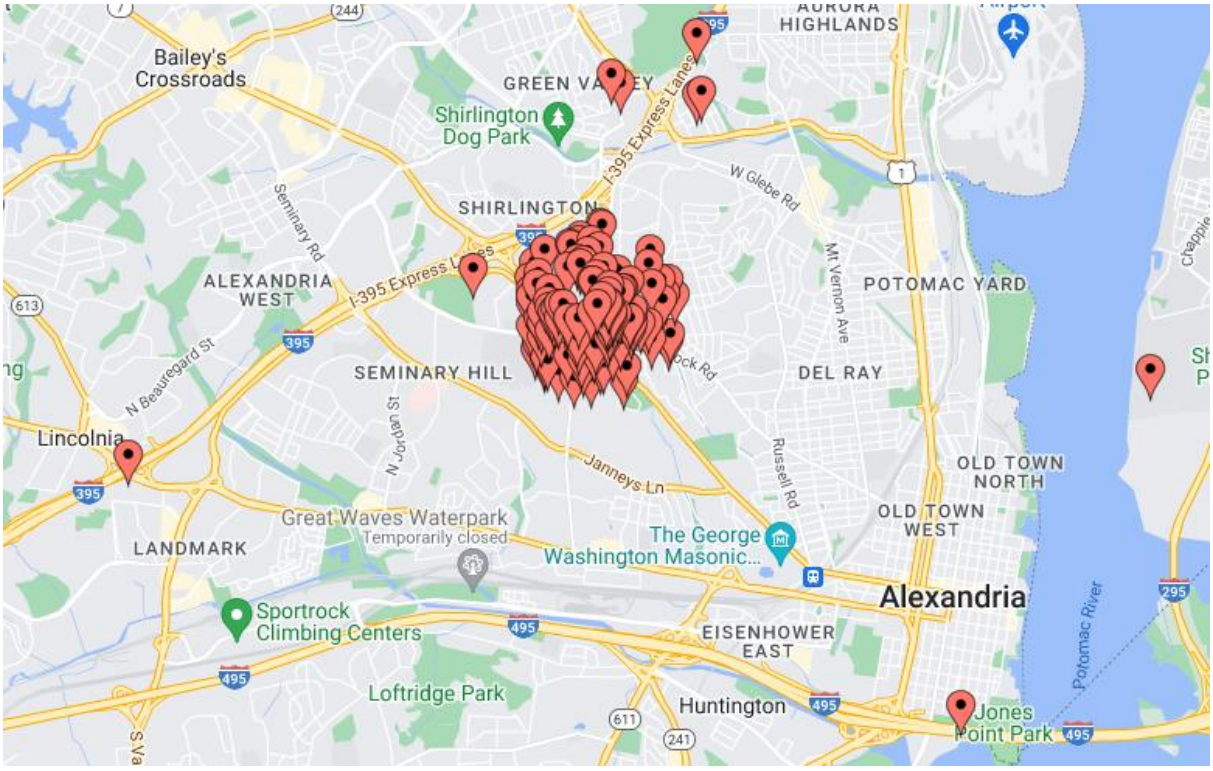
WiFi location data gathered from the /vol5/root/Library/Caches/locationd/consolidated.db and plotted using easymapmaker.com

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

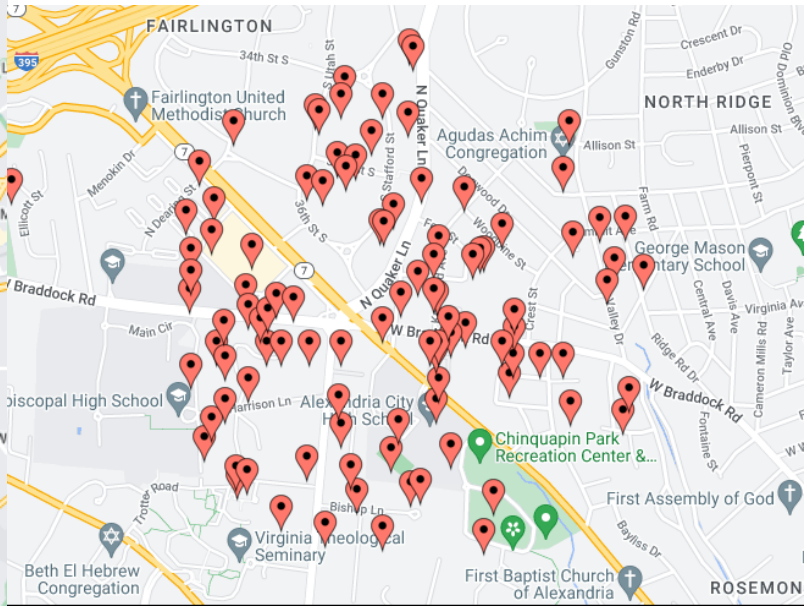

Lacey Woods Park
St. Ann Roman Catholic Church
Lubber Run Park
Lubber Run Trail
Edison Park
ARLINGTON

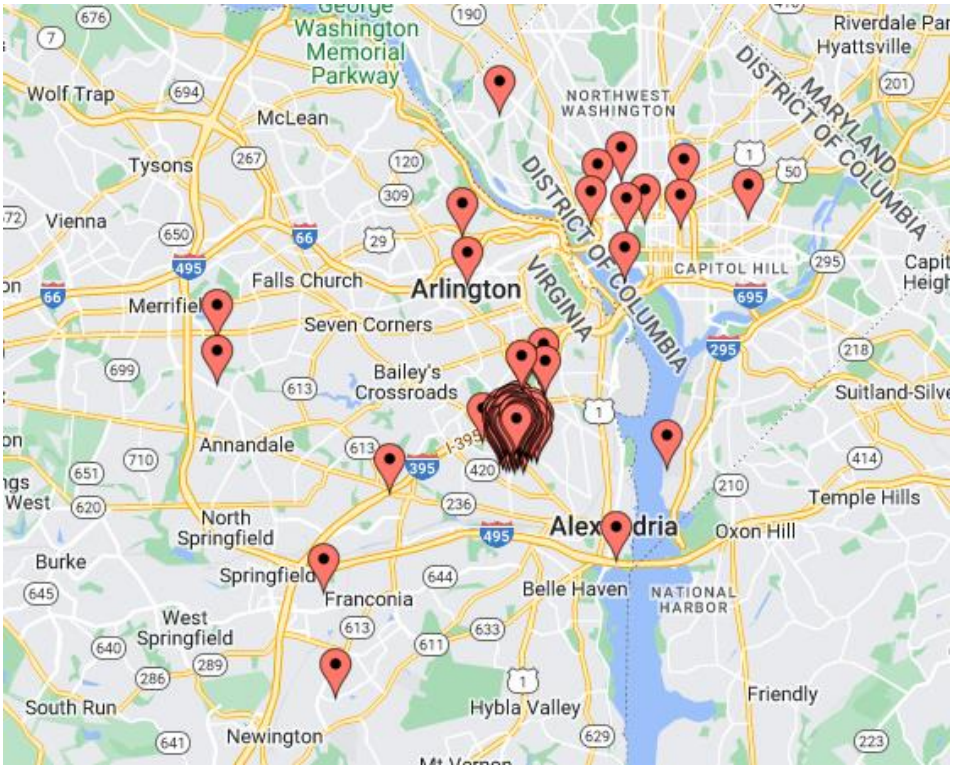

Army Navy Country Club
Henry G. Shirley Memorial Hwy
Oakridge Elementary School
LONG BRANCH CREEK
Four Mile Run
Shirlington Rd
S Arlington Ridge
ARLINGTON RIDGE

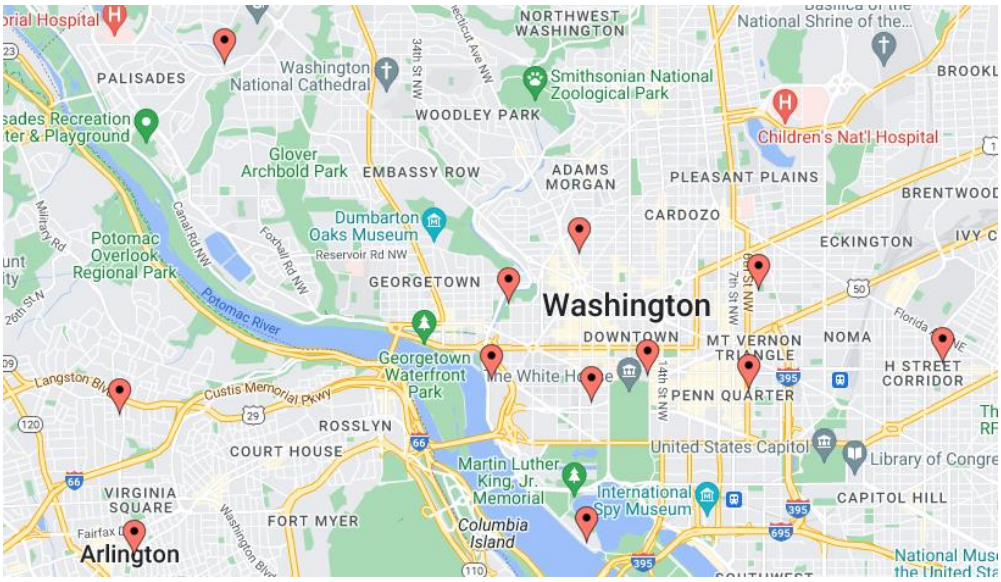

Glen Echo
Brookmont
Washington National Cathedral
Rock Creek Park
National Shrine of t
NORTHWEST WASHINGTON
COLUMBIA HEIGHTS
TAKOMA
Potomac Overlook Regional Park
Washington
FOGGY BOTTOM
United States Capitol
COURT HOUSE
FORT MYER
DISTRICT OF COLUMBIA
VIRGINIA
Nationals Par
AURORA HIGHLANDS
Bailey's Crossroads
MARYLAND
DISTRICT OF COLUMBIA

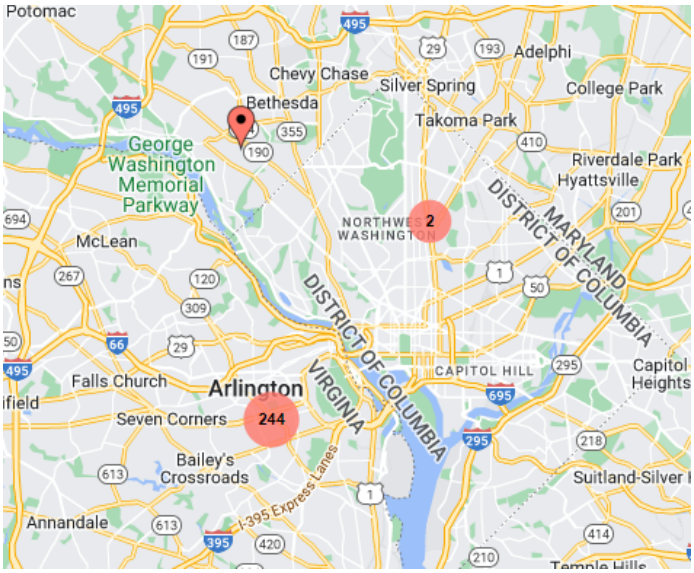

Bailey's Crossroads
AURORA HIGHLANDS
GREEN VALLEY
Shirlington Dog Park
I-395 Express Lanes
W Glebe Rd
SHIRLINGTON
Seminary Rd
ALEXANDRIA WEST
I-395 Express Lanes
POTOMAC YARD
Mt Vernon Ave
SEMINARY HILL
DEL RAY
N Beauregard St
N Jordan St
Janneys Ln
Russell Rd
Lincolnia
OLD TOWN NORTH
OLD TOWN WEST
Great Waves Waterpark
Temporarily closed
The George Washington Masonic...
LANDMARK
Alexandria
Sportrock Climbing Centers
EISENHOWER EAST
Potomac River
Loftridge Park
Huntington
Jones Point Park


West Falls Church
Seven Corners
Green Spring Gardens
Annandale
Braddock Rd
North Springfield
The St. James
Springfield
Franconia
KINGSTOWN


FAIRLINGTON
Fairlington United Methodist Church
Agudas Achim Congregation
NORTH RIDGE
George Mason
Braddock Rd
N Quaker Ln
Chinquapin Park Recreation Center &...
First Assembly of God
Virginia Theological Seminary
Beth El Hebrew Congregation
First Baptist Church of Alexandria
ROSEMONT


Washington Memorial Parkway
Wolf Trap
McLean
Tysons
Vienna
Falls Church
Arlington
Seven Corners
Bailey's Crossroads
Annandale
North Springfield
Springfield
Franconia
West Springfield
Burke
South Run
Newington
NORTHWEST WASHINGTON
DISTRICT OF COLUMBIA
MARYLAND
VIRGINIA
CAPITOL HILL
Riverdale Park
Hyattsville
Suitland-Silver
Temple Hills
Oxon Hill
Alexandria
Belle Haven
NATIONAL HARBOR
Friendly
Hybla Valley


NORTHWEST WASHINGTON
PALISADES
Washington National Cathedral
Smithsonian National Zoological Park
WOODLEY PARK
Glover Archbold Park
EMBASSY ROW
ADAMS MORGAN
PLEASANT PLAINS
Children's Nat'l Hospital
Dumbarton Oaks Museum
Reservoir Rd NW
CARDOZO
ECKINGTON
Potomac Overlook Regional Park
GEORGETOWN
Washington
DOWNTOWN
MT VERNON TRIANGLE
NOMA
H STREET CORRIDOR
Georgetown Waterfront Park
PENN QUARTER
ROSSLYN
COURT HOUSE
United States Capitol
Martin Luther King, Jr. Memorial
International Spy Museum
CAPITOL HILL
VIRGINIA SQUARE
FORT MYER
Columbia Island
Arlington


Potomac
Chevy Chase
Silver Spring
Adelphi
College Park
Bethesda
Takoma Park
George Washington Memorial Parkway
Riverdale Park
Hyattsville
NORTHWEST WASHINGTON
2
DISTRICT OF COLUMBIA
MARYLAND
McLean
CAPITOL HILL
Capitol Heights
Falls Church
Arlington
VIRGINIA
Seven Corners
244
Bailey's Crossroads
Suitland-Silver
Annandale
I-395 Express Lanes