Case Report
National Gallery DC

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

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 - A Linux distribution based on Debian and used for Security Auditing and advanced Penetration Testing.
Autopsy 4.10.0 - Is an open source digital forensics platform.
SQLite 3.11.2 - SQLite is small, light weight, SQL database engine and is also the most used database engine in the world.

Details of Tracy's iPhone

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 3G	vol5/mobile/library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtewlve's iPhone	vol5/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	vol5/mobile/library/Logs/AppleSupport/general.log
Install Time	Created: 6/6/2012 12:03:28 -0700	vol5/mobile/library/Logs/AppleSupport/general.log
User Email	tracy.sumtwelve@nationalgallerydc.org	vol5/mobile/library/Mail

	tracysumtwelve@gmail.com	
Phone Number	(703) 340-9661	vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	vol5/mobile/library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log.1
IMEI	012021003735398	vlo5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577 ccb534ca0d1e83ffd27683e621607	

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
Alt Email: coralbluetwo@hotmail.com
Relationship: Accused
Alias: Coral

Pat:

Phone Number: (571) 308-3236
Email: patsumtwelve@gmail.com
Alt Email: perrypatsum@yahoo.com
Relationship: Brother of the Accused
Alias: Perry

Terry:

Phone Number: (703) 829-6071
Email: Unknown
Relationship: Daughter of the Accused

Joe:

Phone Number: Unknown
Email: joe.sum.twelve@gmail.com
Relationship: Ex-husband of the Accused

Carry:

Phone Number: (202) 725-2124
Email: carrysum2012@yahoo.com
Relationship: Friend of the Accused

King:

Email: throne1966@hotmail.com
Relationship: Partner in crime for stealing stamps

The above information was gathered in Autopsy. The email addresses for Tracy were based on the mailboxes present on the iPhone's image. Tracy's phone number was obtained from the information on the iPhone. The Phone numbers for Terry, Pat and Carry were determined based on the iPhone's address book and sms traffic. Pat's, Joe's and Carry's emails were determined from message traffic between the accounts listed for Tracy.

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.

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps. We can see there is a lot of incriminating evidence against King Pat and Tracy. They exchanged messages via email and sms texts. Tracy's phone also

contained images of the stamps they planned on stealing from the art gallery as we will see below

Pat sends a message to herself as a zip file with the stamp images and insurance quotes for how much the stamps are worth. The images can be found below (Artifact CE01)

Pat starts by emailing King and threatening him that if he does not help them with stealing the stamps he will be arrested for parole Violation (Artifact CE02)

King replies back to pat agreeing to help with the heist and attaches a file (needs.txt) with the tools he will need to complete the heist (Artifact CE03)

Pat forwards the email to tracy with needs.txt attachment to let her know the tools King will need (Artifact CE04)

Pat messages Tracy via SMS text that she will need to open needs.txt as a PDF in order to view it (Artifact CE18)

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

For The Internal use of National Gallery and MyIStamp Collections Only.

Artifact CE01

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

For The Internal use of National Gallery and MyIStamp Collections Only.

Artifact CE02

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

For The Internal use of National Gallery and MyIStamp Collections Only.

Artifact CE03

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 and Tracy exchange messages about sneaking a tablet into to the art gallery and saying that it will be worth the while (CE07)

Carry emails Tracy asking for the security guard schedule, tracy tells carry that she needs to be careful and carry says she needs the money (CE08)

Carry texts tracy asking her where they should meet and tracy replies out front so that she can take the tablet from her (CE16)

Tracy texts carry asking how the “flash mob” is doing (CE17)

Plot Timeline

6/19/12	Pat sends Tracy information about a virtual machine
7/5/12	Text messages between Tracy and Carry about meeting up at Bubba's grill.
7/6/12	Tracy meets up with Carry at Bubba's grill.
7/6/12-7/10/12	Correspondence between Tracy, Pat, and King about the tools needed for the stamp heist.
7/8/12	Tracy photographs the stamps that they are interested in stealing.
7/9/12	Tracy sends herself copies of memos regarding insurance for specific stamps.
7/11/12	Tracy meets up with Carry again to take Carry's tablet in with her.
7/12/12	Tracy asks to Carry about the status of the "flash mob"

Conclusion

Evidence found on Tracy's iPhone indicated the following:

Tracy was having Financial difficulties due to her recent divorce from her Ex-husband Joe. Her daughter Terry goes to Prufrock private school. Tracy could not afford for her daughters tuition and Joe refused to pay unless Terry would come and live with him. Terry made it clear that she would rather live with her father if that meant she gets to stay at her school. Tracy started working with Pat and King to steal the art gallery stamps. Tracy Pat and King exchanged plenty of incriminating messages via email and SMS, All the Evidence related to the Stamp theft can be found above in the "Evidence Related to Stamp Theft" Section . Tracy was also colluding with Carry and the "Flash Mob" to deface the Art Gallery. Carry, who had a political vendetta to push exchanged multiple messages with Tracy that were quite explicit with their plan to deface the art

gallery. Evidence relating to defacement can be found in “Evidence Related to Defacement of Museum Art” section Above.

Appendix A: Correspondence Evidence

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

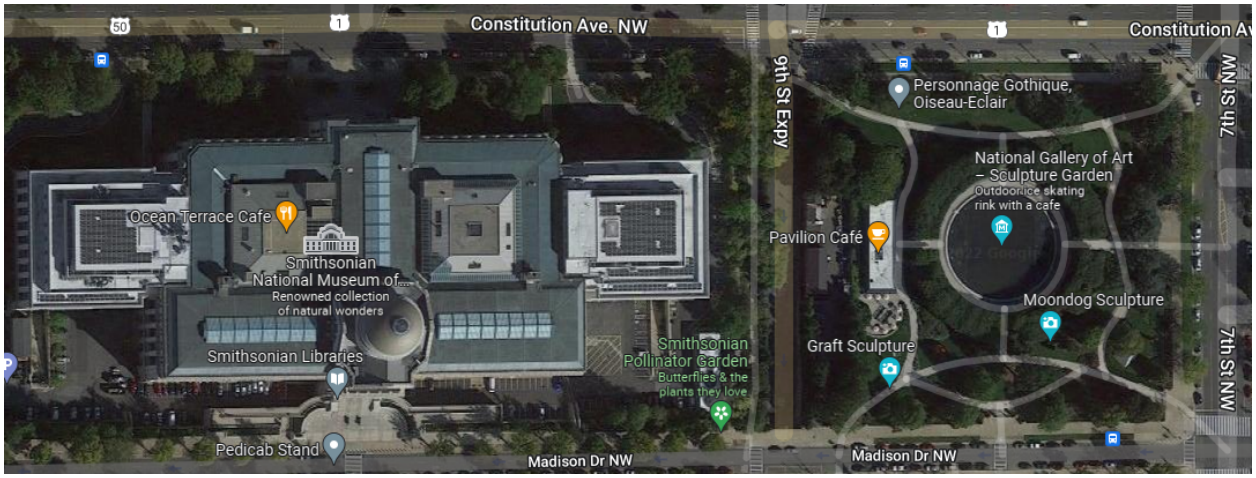
Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
CE01	Mon, 9 Jul 2012 07:47:57 -0700 (PDT)	From: tracysumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: things	Body is only “somethings” Attachment: documents.zip Files are “Stamp insurance #” These files show the insured value of the stamps on display at the National Gallery: $260,000	8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
CE02	Fri, 6 Jul 2012 11:49:31 -0400	From: patsumtwelve@gmail.com To: throne1966@hotmail.com CC: coralbluetwo@hotmail.com Subject: can’t pass up	Pat threatens King with arrest for parole violation if he does not help with a planned heist at the National Gallery	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
CE03	Tue, Jul 10, 2012 at 11:19 AM	From: throne1966@hotmail.com To: patsumtwelve@gmail.com Subject: RE: can’t pass up	King agrees to help and provides attachment of tools needed as needs.txt	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
CE04	Tue, 10 Jul, 2012 08:24:57 -0700 (PDT)	From: patsumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: Fwd: can’t pass up	Pat forwards to Tracy the needs.txt file from King SMS between Pat and Tracy show this is a pdf, see below for screen shot	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
CE05	Tue, 19 Jun 2012 14:38:59 -0700 (PDT)	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subjet: Crazydave by the VMs	Pat sends Tracy an mp3 purporting to be a new song by the VMs Attachment: Crazydave1.mp3 Embedded within the .mp3 file are instructions for downloading and	3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx

			setting up a VM	
CE06	Mon July 2, 2012 at 4:06 pm	From: Joe.sum.twelve@gmail.com To: tracysumtwelve@gmail.com Subject:	Pat asks Joe to help pay for Terry to continue to attend school at Prufrock. Joe declines to pay for Terry's schooling if she is not living with him.	vol_vol5/mobile/Library/Mail/Protected Index Line/Item 76
CE07	Tue, 10 Jul 2012 06:48:40 PDT	From: carrysum2012@yahoo.com To: tracysumtwelve@gmail.com Subject: Re: Long time no see…	Email thread between Carry and Tracy. Carry will "make it worth your while" for Tracy to smuggle a tablet through security, Tracy agrees.	vol_vol5//$CarvedFiles/f0408520.plist
CE08	Wed, Jul 11, 2012 1:24 PM	From: carrysum2012@yahoo.com To: tracysumtwelve@gmail.com	Email thread between Carry and Tracy. Carry asks Tracy for the security schedule, specifically shift change. Tracy agrees, cautions Carry to be careful as Tracy could get in trouble, but mentions needing the money.	vol_vol5//$CarvedFiles/f0401136.plist
CE09	Tue, 19 Jun 2012 13:26:47 -0700 (PDT)	From: perrypatsum@yahoo.com To: tracysumtwelve@gmail.com	Email thread for "perry" saying Tracy should have her "friend" Alias get in touch.	vol_vol5//$CarvedFiles/f0401136.plist
CE10	Mon, July 2, 2012 12:05 PM	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com Subject: Some good news	Tracy mentions to Pat that a new exhibit is coming to the National Gallery	vol_vol5/mobile/Library/Mail/Protected Index Line/Item 171,172
CE11	Mon, July 2, 2012 6:11 PM	From: patsumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: Re: Some good news	Pat responds with the hope this will be their break	vol_vol5/mobile/Library/Mail/Protected Index Line/Item 171,172
CE12	Thursday, June 28,2012 4:16 PM	From: patsumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: Re: Whats going on	Pat responds to Tracy that communication should be over the new setup and that he has to be more careful as "IA has been sniffing around" Also mentions they are both in need of money and that they need to "'push the envelope'"	vol_vol5/mobile/Library/Mail/Protected Index Line/Item 173,174

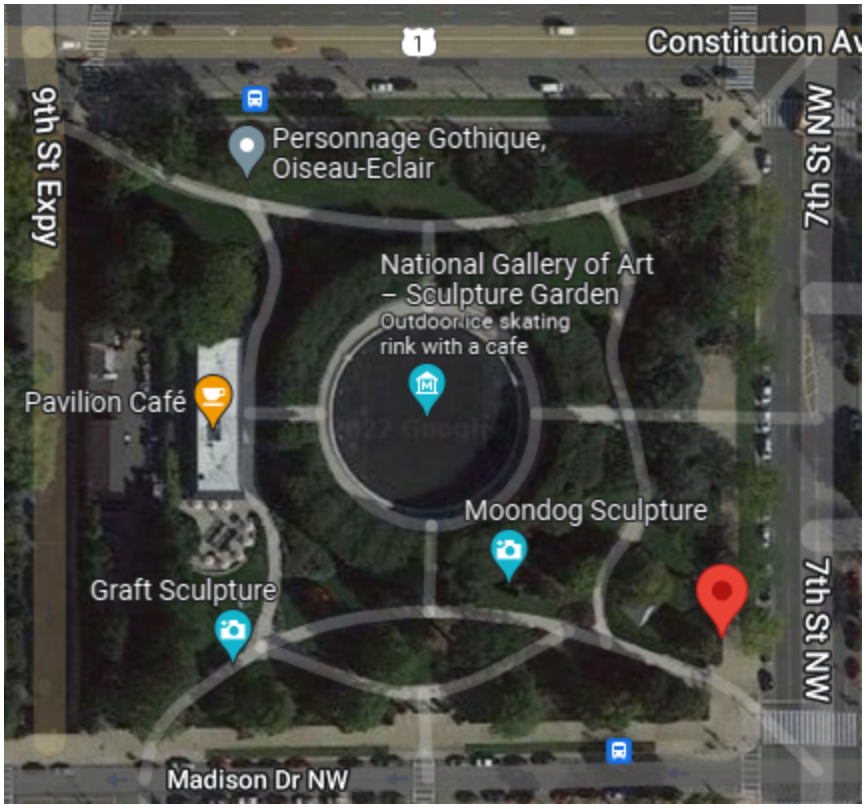
CE13	Tue, 19 Jun 2012 16:06:33 -0400	From: patsumtwelve@gmail.com To: tracysumtwelve@gmail.com Subject: Paris Speak and answer	Message in French from Pat to Trace to create and use an alias. Seems to be a follow to item CE09 above.	f0401136.plist
CE14	Fri Jul 6, 2012 11:42 AM	From: Pat/Perry To: Tracy/Coral	Email from Pat to Tracy, based on context, login info for something is: coralblue@hotmail.com PW: legalBee Possibly for the VM mentioned in artifact CE05.	Protected Index: Line/Item 99
CE15		From: carrysum2012@yahoo.com To: tracysumtwelve@gmail.com Subject: Google+ Gallery invite	Carry adds Tracy to her Google+ and shares an album.	Protected Index: Line/Item 52, 53, 56. 122, 131
CE16	7/11/2012 12:41:45	From: +1202752214 (Carry) To: Tracy Subject: N/A (SMS Conversation	Carry asks where to meet Tracy, Tracy responds out front and she (Tracy) will take the tablet in	SMS.db ROWID 30 & 31
CE17	7/12/2012 17:06:45	From: Tracy To: +1202752214 (Carry) Subject: N/A (SMS Conversation)	Tracy asks Carry how the flash mob is going	SMS.db ROWID 32
CE18	7/10/2012 15:26:19	From: +17038296071 (Pat) To: Tracy Subject: N/A (SMS Conversation)	Pat tells Tracy that her “friend coral” got a message with a .txt extension that should be a .pdf which when applied to needs.txt revealed a list of equipment	SMS.db ROWID 23
CE19	7/3/2012 14:04:32	From: +15713083236 (Terry) To: Tracy Subject: N/A (SMS Conversation)	Terry tells Tracy that she (Terry) would rather live with Dad (Joe) if it means staying in her school (Prufrock)	SMS.db ROWID 13
CE20	7/7/2012 19:36:35	From: +12069100932 To: Tracy Subject: N/A (SMS Conversation)	This may be a spam/phishing text, but as it occurs after Carry and Tracy’s lunch meeting it’s possible this is being used to disguise payment	SMS.db ROWID 22

Full worksheet with additional/original information: [21.3 Correspondence Evidence Worksheet]

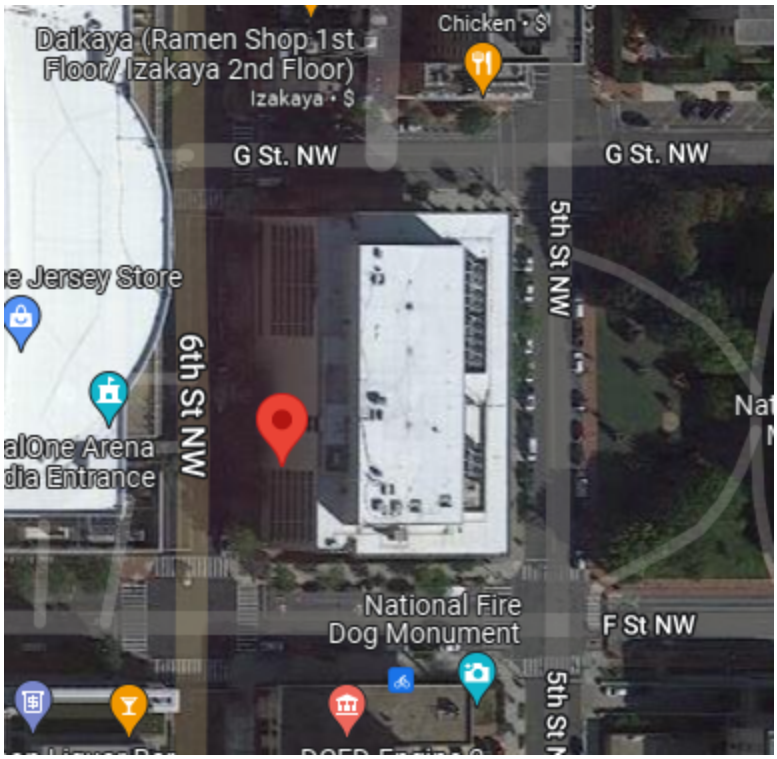
Appendix B: WiFi and GPS Location Information



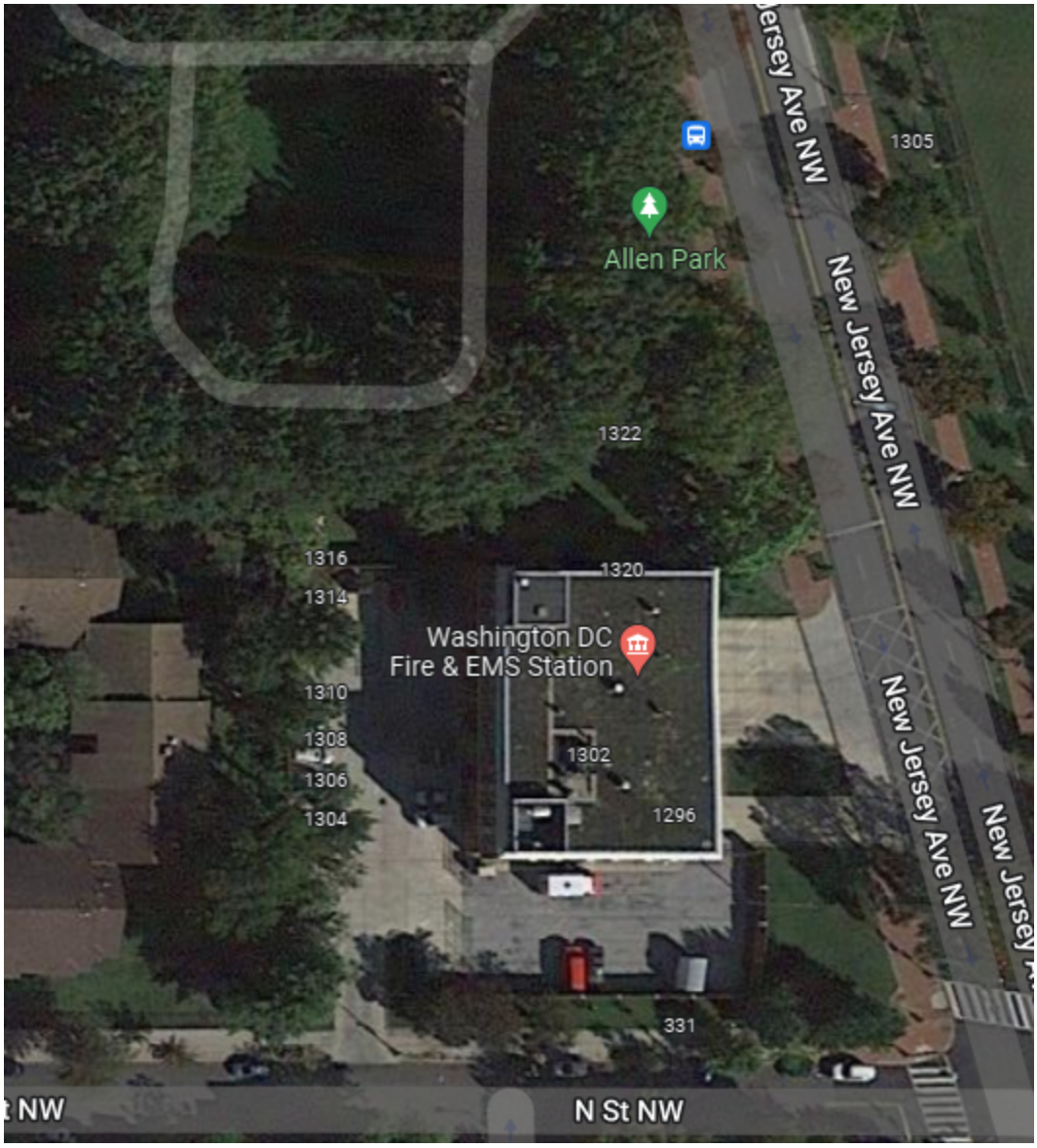
38.89166667	-77.0235	Northwest Washington, Washington, DC 20408
38.89133333	-77.02283333	7th St NW, Washington, DC 20408
38.89133333	-77.0225	Northwest Washington, Washington, DC 20408
38.89083333	-77.02216667	Northwest Washington, Washington, DC 20408



38.89083333 -77.02216667 Northwest Washington, Washington, DC 20408



38.89766667 -77.01966667 600 5th St NW, Washington, DC 20001



38.9085 -77.01816667 1321 5th St NW, Washington, DC 20001