



Cybersecurity

21.3 The Final Report

Case Report

National Gallery DC

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

Table of Contents

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

[Evidence relating to theft of valuable stamps](#)

[Evidence relating to defacement of museum art](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: WiFi and GPS Location Information](#)

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.

Tracy's iPhone has evidence of said conspiracy for theft and to damage foreign artwork at the National Gallery. It shows collusion between Tracy, Pat and King.

Equipment and Tools

- Autopsy
- Kali Linux
- DB Browser, SQLite
- Google Maps

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Mode I	iPhone 1,2	vol5/logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	Lockdownd.log.1

OS Version	iPhone OS 4.2.1 (8C148)	vol5/logs/AppleSupport/general.log
Install Time	6/6/12 19:03:28	vol5/logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com tracysumtwelve@nationalgallerydc.org	vol5/mobile/Library/Mail Envelope Index
Phone Number	(703) 340-9661	Vol5/logs/lockdownd.log.1
Serial Number	86004482y7h	vol5/logs/AppleSupport/general.log
ICCID	8991909000433785460	lockdownd.log.1
IMEI	012021003735398	wildcard_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

Eric Ledesma

Work Email: tracy.sumtwelve@nationalgallerydc.org
Relationship: Accused

Pat:

Phone Number: (571)308-3236
Email: patsumtwelve@gmail.com
Relationship: Brother

Terry:

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

Joe:

Phone Number:
Email: joe.sum.twelve@gmail.com
Relationship: Ex-husband of Tracy. Father of Terry

Carry:

Phone Number: (202)725-2124
Email: carrysum2012@yahoo.com
Relationship: Acquaintance of Tracy

King:

Phone Number:
Email: throne1966@hotmail.com
Relationship: Acquaintance of Pat

Tracy colluded with Perry and his accomplice, King to steal stamps at the National Gallery. She received pictures from a tablet from Carry.

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.

- Tracy, Pat and King were in correspondence to steal valuable stamps from the National Gallery. Tracy's phone contained photos of the stamps they wanted to steal.
- A blackmail email was sent from Pat to King to gain his help in the heist.
- King sent an email with an attached document listing the tools he needs for the heist.
 - Pat forwarded this email to Tracy.
- Tracy emails herself pdf attachments. The attachments are memos for stamp insurance – it lists the amount each stamp is insured for.

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.

- Tracy was in correspondence with Carry to assist with a flash mob. She gave sensitive information about the National Gallery to Carry.
- SMS Messages – Tracy and Carry meet at Bubba's Grill.
- SMS Messages – Tracy and Carry to meet with Carry's tablet.

Plot Timeline

<u>Date</u>	<u>Information</u>
Tue, June 19, 2012	Pat sent Tracy info about Virtual Machine
Thurs, July 5, 2012	SMS Messages between Tracy and Carry to meet at Bubba's Grill
Fri, July 6, 2012	Tracy meets with Carry at Bubba's Grill
Fri, July 6, 2012 to Tue, July 10, 2012	Correspondence with Tracy, Pat and King about tools needed for stamp heist
Sun, July 08, 2012	Tracy photographs stamps at National Gallery they want to steal
Mon, July 09, 2012	Tracy sent copies of insurance policy for valuable stamps at National Gallery
Wed, July 11, 2012	Tracy met with Carry and brought along her tablet
Thurs, July 12, 2012	Tracy asks Carry about status of flash mob

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Terry colluded with Pat and King to steal valuable stamps from the National Gallery.
- Terry gave sensitive information to Carry to execute a flash mob.
- Tracy and Pat use aliases – Coral and Perry, respectively.
- Terry has financial issues.
- Attachment file labeling tools needed for heist - a conspiracy to deface artwork at the National Gallery.
- Memos for stamp insurance and photos detailing plans to steal valuable stamps.

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
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	Pat (Perry) emails Tracy (Coral) with instructions to install a	Mailbox Data Structure

		Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Virtual Machine hidden in an audio file.	
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	Mailbox Data Structure

			<p>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.</p>	
7.	6/29/2012 14:21:56	<p>F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going on</p>	<p>This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money.</p> <p>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.</p>	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	Mailbox Data Structure

			<p>foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal.</p> <p>Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.</p>	
11.	7/2/2012 20:00:31	<p>F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com</p> <p>Subject: Re: Some good news</p>	<p>Email thread: Some good news</p> <p>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.</p> <p>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.</p>	Mailbox Data Structure
12.	7/3/2012 13:29:37	<p>F: joe.sum.twelve@gmail.com T: tracysumtwelve@gmail.com</p>	<p>Email Thread: Regarding Terry</p> <p>Tracy emails Joe asking whether he could help her with</p>	Mailbox Data Structure

		Subject: Re: Regarding Terry	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.	
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	Email Thread: Good News	Mailbox Data Structure

		<p>T: tracysumtwelve@gmail.com</p> <p>Subject: Re: Good News</p>	<p>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.</p> <p>Pat replied back saying that he knows a guy called King.</p>	
16.	7/6/2012 15:49:31	<p>F: patsumtwelve@gmail.com T: throne1966@hotmail.com Cc: coralbluetwo@hotmail.com</p> <p>Subject: can't pass up</p>	<p>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.</p>	Mailbox Data Structure
17.	7/6/2012 17:59:24	<p>F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com</p> <p>Subject: Re: Good News</p>	<p>Email Thread: Good News</p> <p>Tracy suggests they (meaning King, Tracy and Pat) should hang out sometime.</p> <p>Pat emails Tracy with account login information for: coralblue@hotmail.com Password: legalBee</p>	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/Libra r y/Mail/POP- coralbluetwo @hotmail.co m @pop3.live.co m/INBOX.mb o 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	Mailbox Data Structure

			she could come around 9 tomorrow.	
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/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9 F0508B8-04FB-490E-A7F0-3E23B0E7C59B.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	Mailbox Data Structure

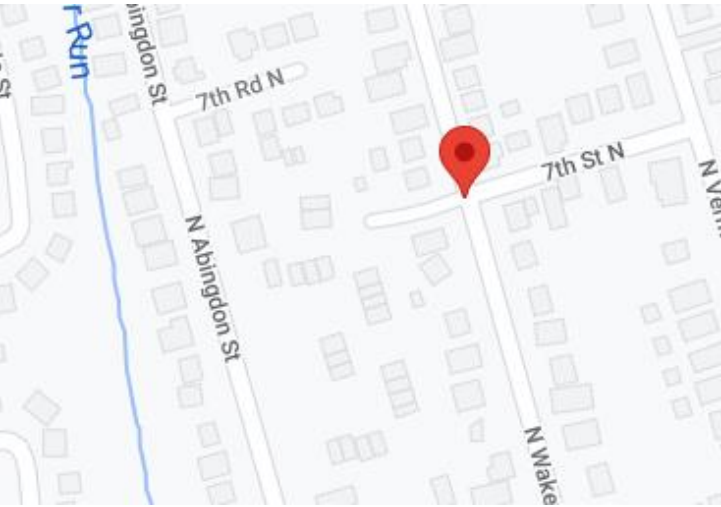
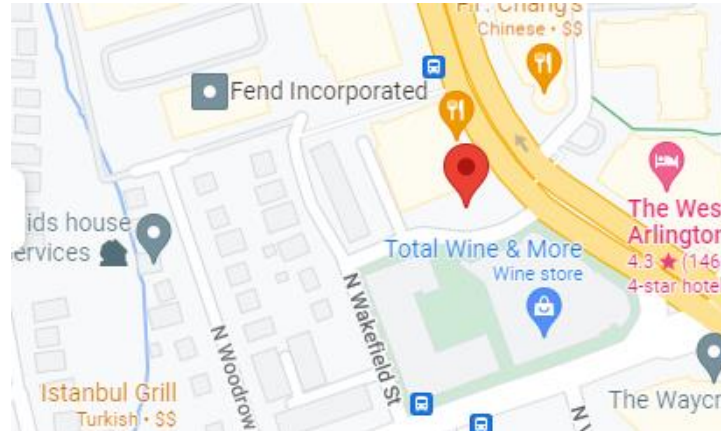
			Tracy not to worry and says "It will be gun".	
23.	7/11/2012 19:28:53	F: "Google+" <noreply-5dd47ca1@plus.google.com> T: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve added you on Google+	Email Thread: Long time no see Previous email from the thread from Carry asking for the security shift 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	Email Thread: Long time no see... Tracy emailed Carry asking her what she	Mailbox Data Structure


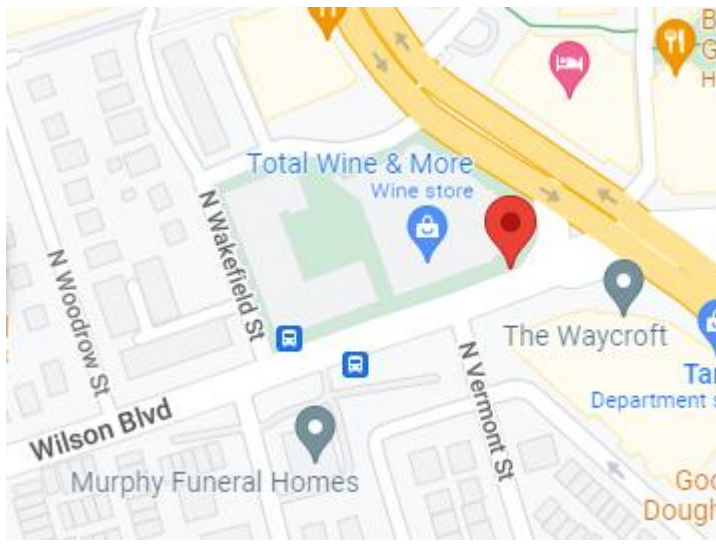

		Subject: Re: Long time no see...	meant by "It will be gun". Carry replies saying that it was a typographical error and she meant "It will be fun".	
27.	6/12/2012 21:25:04	F: Pat T: Tracy	Pat asks Tracy about her plans for the weekend	SMS
28.	6/13/2012 17:30:28	F: Terry T: Tracy	I'm going out with dad 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

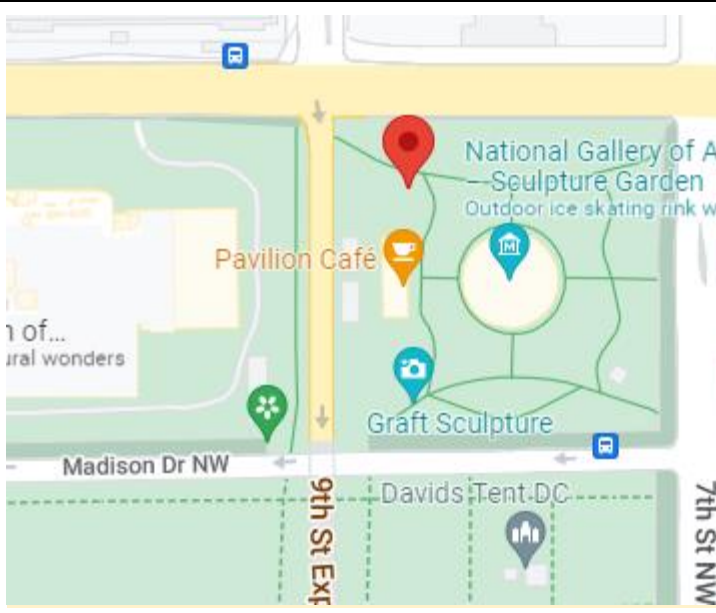
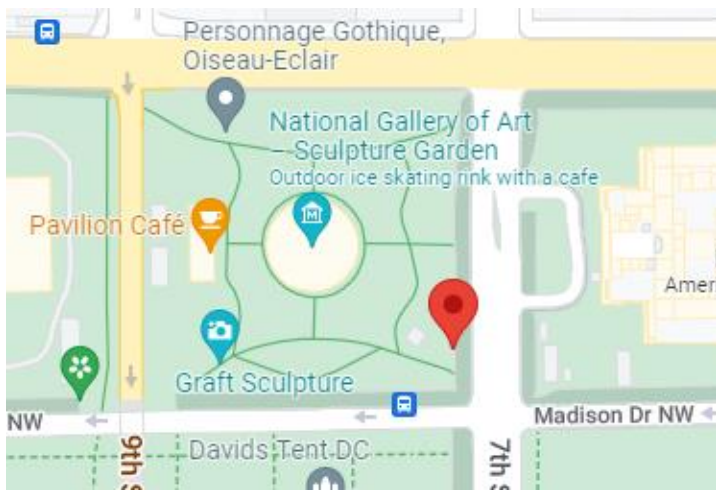
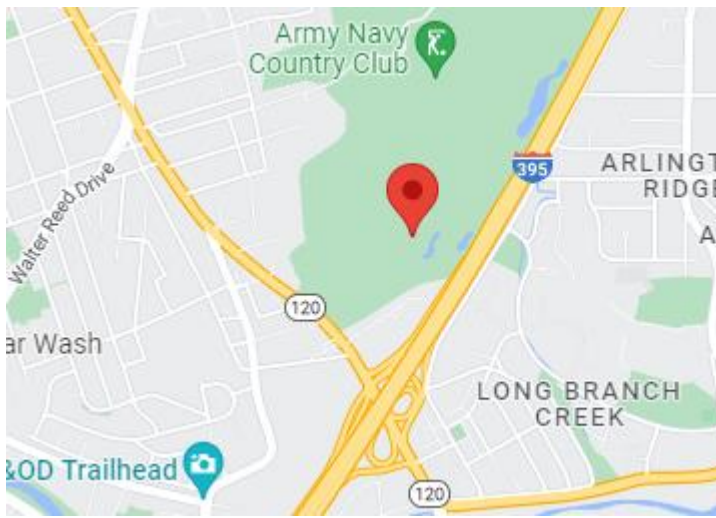
43.	7/10/2012 16:37:09	F: Tracy T: Pat *Failed	Tracy tried to share the following location with Pat over MMS message but it failed. Location: 2600-2700 24th Rd S, Arlington, VA 22206	SMS
44.	7/10/2012 17:18:38	F: Tracy T: Terry	Tracy messages Terry for Lunch	SMS
45.	7/10/2012 18:19:24	F: Tracy T: Terry	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

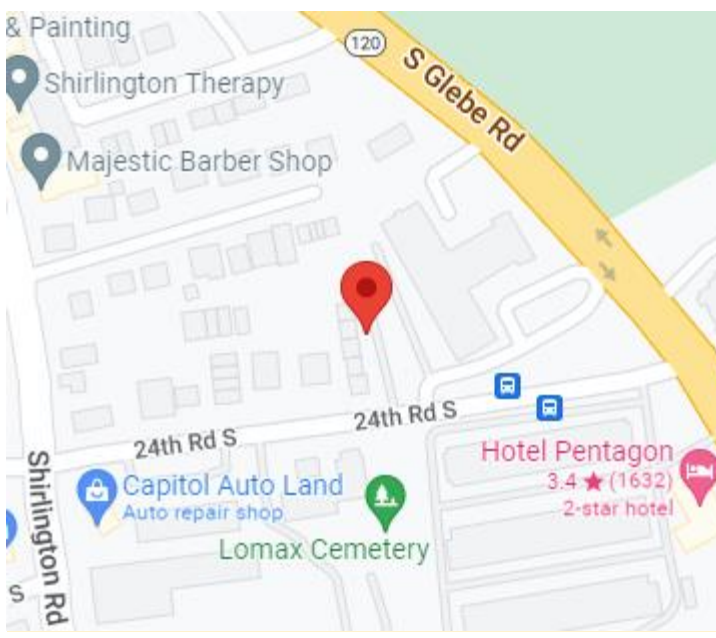

Appendix B: WiFi and GPS Location Information

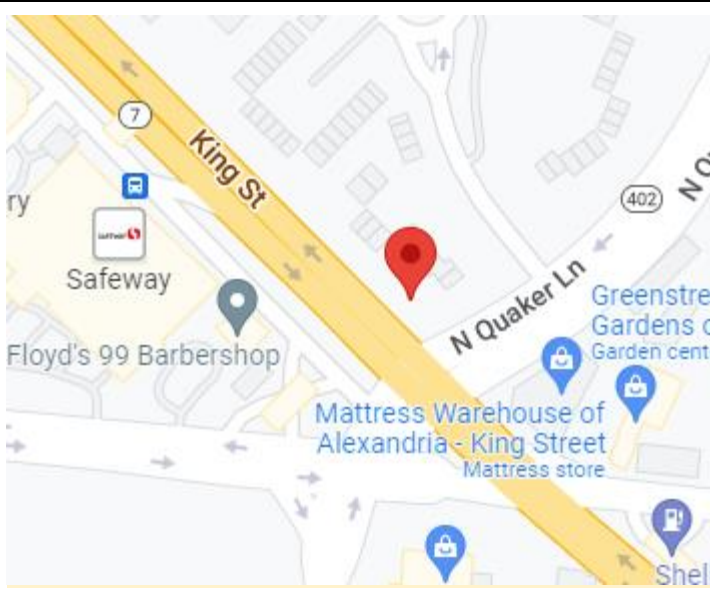
Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	Wed, Jun 13, 2012 7:01:21 PM	38°52'39.6"N 77°06'55.7"W	Virginia Tech Research Center – Arlington (900 N Glebe Rd, Arlington, VA 22203, USA)	
2	Sun, Jun 13, 2012 7:01:22 PM	38°52'50.0"N 77°06'55.9"W	Virginia Tech Research Center – Arlington (900 N Glebe Rd, Arlington, VA 22203, USA)	

3	Mon, July 2, 2012, 4:19:23 PM	38°52'51. 3"N 77°07'01. 6"W	4600 Fairfax Dr, Arlington, VA 22203, USA	
4	Mon, July 2, 2012, 4:19:24 PM	38°52'47. 7"N 77°06'52. 6"W	800 N Glebe Rd, Arlington, VA 22203, USA	
5	Tue, July 3, 2012, 1:42:42 PM	38°52'50. 3"N 77°06'56. 1"W	900 N Glebe Rd, Arlington, VA 22203, USA	

6	Thurs, July 5, 2012, 4:32:46 PM	38°52'46. 2"N 77°06'52. 6"W	Arlington, VA 22203, USA	
7	Thurs, July 5, 2012, 4:32:47 PM	38°52'49. 9"N 77°06'52. 0"W	801 N Glebe Rd, Arlington, VA 22203, USA	

8	Sun, July 8, 2012, 12:33:36 PM	38°53'30.0"N 77°01'24.6"W	National Gallery of Art, Washington DC 20408, USA	
9	Sun, July 8, 2012 12:41:41 PM	38°53'27.0"N 77°01'19.8"W	Northwest Washington, Washington DC 20408, USA	
10	Tue, July 10, 2012, 4:31:10 PM	38°51'05.1"N 77°04'41.7"W	1700 Army Navy Dr, Arlington, VA 22202, USA	

11	Tue, July 10, 2012, 4:31:12 PM	38°50'54. 0"N 77°04'55. 9"W	2693 24 th Rd S, Arlington, VA 22206, USA	
12	Tue, July 10, 2012 4:45:00 PM	38°49'37. 4"N 77°05'10. 0"W	1737 W Braddock Pl, Alexandria, VA 22302, USA	

13	Tue, July 10, 2012, 4:45:01 PM	38°49'39. 5"N 77°05'17. 0"W	4104 36 th St S, Arlingto n, VA 22206, USA	
14	Tue, July 10, 2012, 4:46:29 PM	38°49'44. 7"N 77°05'05. 1"W	1701 Centre Plaza, Alexand ria, VA 22302, USA	