Cybersecurity

21.3 The Final Report

Case Report
National Gallery DC

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

By: Steve Parker, [redacted]

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.

After going through Tracy's phone, we were able to discover that Tracy is guilty of conspiring to steal stamps from the National Gallery. Tracy worked with Pat, her brother, and Carry in order to steal the stamps for financial gain. Pat blackmailed a guy referred to as "King", to perform the heist. Through emails, you can see that King agrees to perform the heist and requests materials. Pat, Carry, and Tracy coordinate a flash mob to use as a distraction. The crime was committed for financial reasons. The accused has a daughter who wants to stay at her current school. Tracy cannot afford the school for her daughter anymore due to a divorce. Tracy, however, did not know that Carry had ulterior motives.

Equipment and Tools

We used Autopsy to examine the contents of the phone and recover relevant information. We extracted some of this information and viewed it using SQLiteBrowser and Kali Linux Terminal.

Details of Tracy's iPhone

Name	**Findings**	**Location in iPhone image file**
Model	iPhone 1,2	img_tracy-phone-2012-07-15-final.E01/Vol5/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	img_tracy-phone-2012-07-15-final.E01/Vol5/logs/lockdownd.log.1

OS Version	iPhone OS 4.2.1 (8C148)	img_tracy-phone-2012-07-15-final.E01/Vol5/mobile/Library/Logs/AppleSupport/general.log
Install Time	06.06.2012 12:03:28 -0700	img_tracy-phone-2012-07-15-final.E01/Vol5/mobile/Library/Logs/AppleSupport/general.log
User Email	Tracysumtwelve@nationalgallerydc.org Tracysumtwelve@gmail.com Coralbluetwo@hotmail.com	mg_tracy-phone-2012-07-15-final.E01/Vol5/$CatalogFile
Phone Number	17033409661	img_tracy-phone-2012-07-15-final.E01/Vol5/logs/lockdownd.log.1
Serial Number	86004482Y7h	img_tracy-phone-2012-07-15-final.E01/Vol5/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	img_tracy-phone-2012-07-15-final.E01/Vol5/logs/lockdownd.log.1
IMEI	012021003735398	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/root/Library/Lockdown/activation_records/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
Work Email:	tracy.sumtwelve@nationalgallerydc.org
Relationship:	Accused

Pat:

Phone Number: 571-308-3236
Personal Email: perrypatsum@yahoo.com
Work Email: patsumtwelve@gmail.com
Relationship: Tracy's brother

Terry:

Phone Number: 17038
Email: tracysumtwelve@gmail.com
Relationship: daughter of Tracy and Joe

Joe:

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

Carry:

Phone Number: 202-725-2124
Email: carrysum2012@yahoo.com
Relationship: friend/accomplice of Tracy

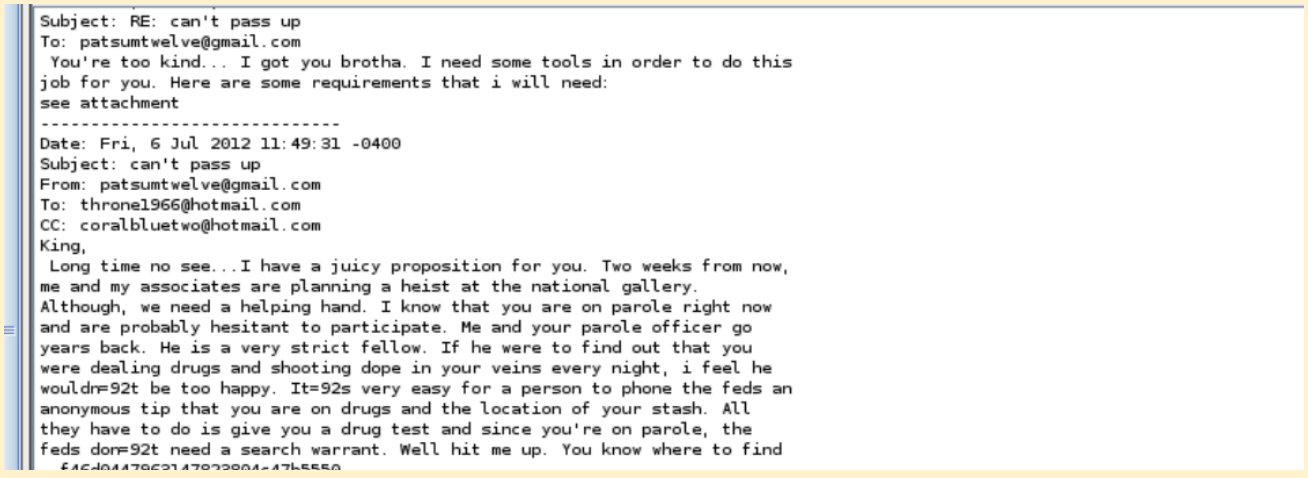
We were able to piece together the phone numbers and emails of each person by using the data we found by using Autopsy.

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.

Emails and text messages were exchanged between Pat, Tracy, and Carry and an accomplice using the alias "King" using the email throne1966@hotmail.com.
Pat emails Tracy on 7/2/12 with "Some Good News". The email states how the upcoming expensive exhibit has items being shipped at a low cost. This means that the items are small and easier to steal.

See the email below:



```
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
------------------------------
Date: Fri, 6 Jul 2012 11:49:31 -0400
Subject: can't pass up
From: patsumtwelve@gmail.com
To: throne1966@hotmail.com
CC: coralbluetwo@hotmail.com
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 that you
were dealing drugs and shooting dope in your veins every night, i feel he
wouldn=92t be too happy. It=92s very easy for a person to phone the feds an
anonymous tip that you are on drugs and the location of your stash. All
they have to do is give you a drug test and since you're on parole, the
feds don=92t need a search warrant. Well hit me up. You know where to find
```

Below throne1966@hotmail.com responds via email with a list of items he will need in order to complete the heist.

```
-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)
```

Photos of the stamps were also found that were taken at the museum prior to the heist.

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 reached out to Tracy to meet for lunch at the Russian Tea Room. Carry asks Tracy to sneak in a tablet for a flash mob event that was to be used as a distraction. She also asks Tracy for information regarding guard changes. Tracys agrees to help since she will be compensated. They agree to meet at 9. Tracy gets a Google+ notification letting her know that Carry shared something with her. One of the

notifications was to add Alex, someone Carry knows. Unbeknownst to Tracy, Alex is a Krassinovian supporter.

Plot Timeline

6/19/12: Pat sends Tracy an email letting her know that he has accepted her proposal and asks her to email using her alias for further instructions.
6/19/12: Perry sends an email to Coral with instructions on how to install a virtual machine. The instructions are sent as an audio file. Pat is now going by the alias Perry and Tracy is now using the alias Coral. The audiofile is name: Crazydave1.mp3
6/21/12: Tracy confirms via email that the instructions sent via audiofile were helpful to her, and she was able to successfully install the virtual machine.
6/28/12 Pat sends Tracy an email saying they shall only use their aliases henceforth. He also states they might have to get into riskier businesses since both are having financial issues. Pat also informs Tracy he has a few workplace friends who might be able to help them.
6/29/12: Tracy states in an email to Pat that they should also look into other opportunities so that her child doesn't have to switch schools.
7/2/12 Tracy emails Pat about an upcoming exhibit that has expensive items that have lower shipping costs. This means that the items will be smaller and therefore easier to steal.
7/3/12 Tracy emails her husband asking for help in tuition for their daughter. Joe responds saying that since Terry is no longer living with him, he will not contribute to her tuition. Terry also texts Tracy saying she would rather live with her Dad so she can continue going to her current school.
7/6/12 Pat mentions that he may know someone that can help named King.Pat emails King and CCs Tracy. He says he has a lucrative proposition. He also blackmails King, saying he would put his parole in jeopardy.
7/9/12 Tracys sends herself insurance claims on the stamps. Carry asks Tracy to help sneak a tablet into the National Gallery. Carry says Tracy will be compensated for helping.
7/10/12 Tracy agrees to help and asks when Carry would like to come to the National Gallery to have a look around. Carry responds saying 9 tomorrow works. King agrees to help with the heist and sends an attachment with a list of items he needs.
7/11/12 Carry asks Tracy for information regarding guard shift changes and says that Tracy will be compensated. Tracy agrees to give the information over. Carry sends a text to Tracy saying she is on the way to the National Gallery. Tracy responds telling Carry to meet out front and that she will take the tablet in.

Conclusion

- Tracy and Pat were co-conspirators. They both used an alias. Pat used 'patsumtwelve@gmail.com' and Tracy used 'coralbluetwo@hotmail.com'.
- The main motive for the conspirators was financial gain. Tracy had previously emailed Joe asking whether he could help her with 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.
- Pat also emailed throne1966@hotmail.com to steal stamps from the National Gallery. Throne1966@hotmail.com is a guy referred to as "King".
- Tracy and Carry coordinate a flash mob to use as a distraction while the stamps are being stolen.

Appendix A: 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:	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Mailbox Data Structure

		coralbluetwo@hotmail.com Subject: Crazydave by the VMs Attachment: Crazydave1.mp3		
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 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.	Mailbox Data Structure
7.	6/29/2012 14:21:56	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Whats going	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money. To Pat's suggestion that they use the Virtual Machines and aliases to	Mailbox Data Structure

		on	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.	
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	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be	Mailbox Data Structure

		news	a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	
11.	7/2/2012 20:00:31	F: perrypatsum@yahoo.com T: coralbluetwo@hotmail.com Subject: Re: Some good news	Email thread: Some good news 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. 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.	Mailbox Data Structure
12.	7/3/2012 13:29:37	F: joe.sum.twelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Regarding Terry	Email Thread: Regarding Terry Tracy emails Joe asking whether he could help her with 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.	Mailbox Data Structure
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	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	Mailbox Data Structure

		Subject: Long time no see...	realized that Tracy was having a hard time recently.	
15.	7/6/2012 15:27:51	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News 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. Pat replied back saying that he knows a guy called King.	Mailbox Data Structure
16.	7/6/2012 15:49:31	F: patsumtwelve@gmail.com T: throne1966@hotmail.com Cc:coralbluetwo@hotmail.com Subject: can't pass up	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.	Mailbox Data Structure
17.	7/6/2012 17:59:24	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy suggests they (meaning King, Tracy and Pat) should hang out sometime. Pat emails Tracy with account login information for: coralblue@hotmail.com Password: legalBee	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/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbo

				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 she could come around 9 tomorrow.	Mailbox Data Structure
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	Email Thread: Long time no see Tracy confirms the meet at 9 tomorrow. Carry wants Tracy to pass her	Mailbox Data Structure

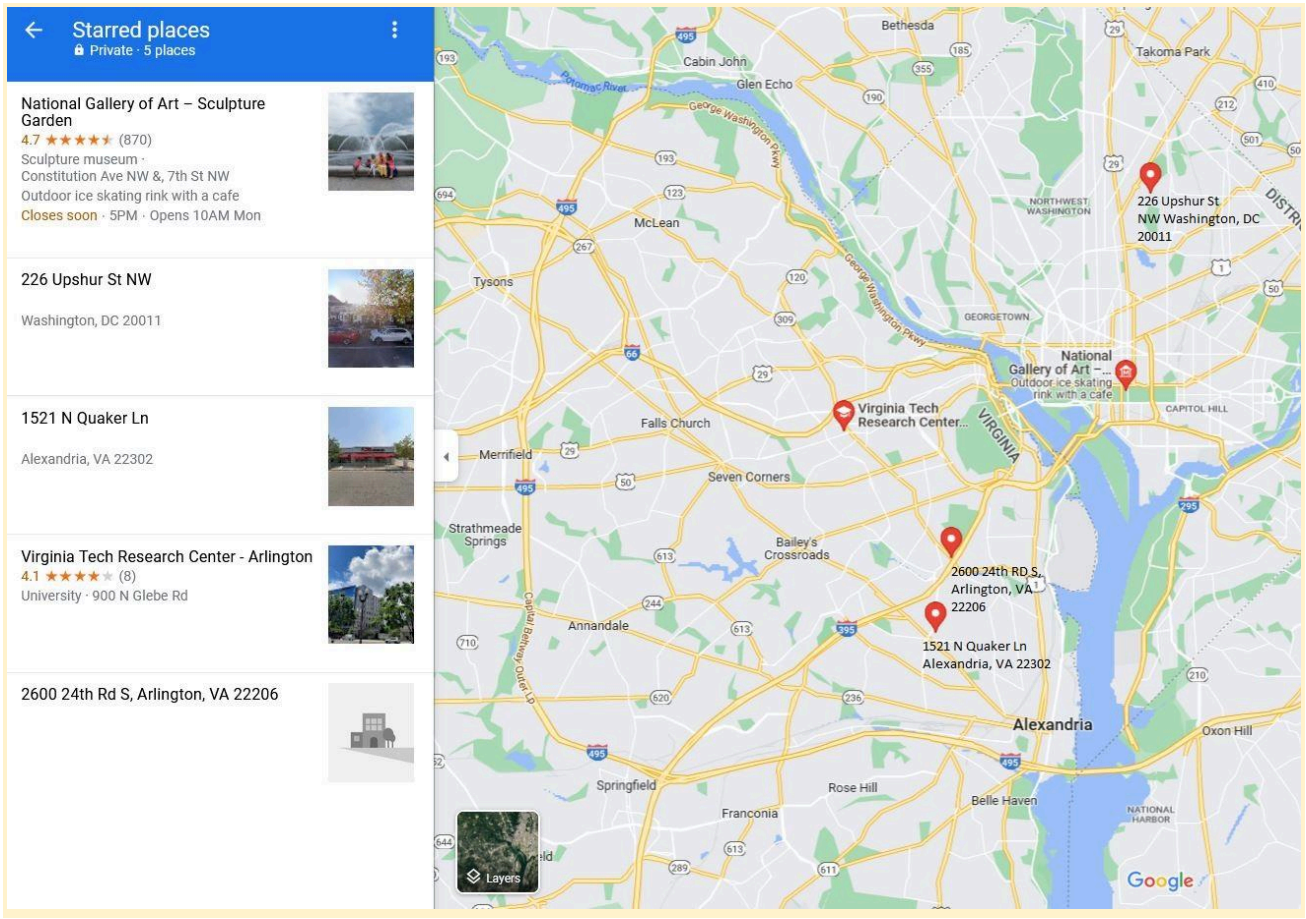
		Subject: Re: Long time no see...	information regarding shift changes of security. She suggests that Tracy would be well compensated for the information. Tracy confirms that she will give the security shift information Carry requested in exchange for money but asks Carry to be careful with it. Carry replies asking 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 Subject: Re: Long time no see...	Email Thread: Long time no see... Tracy emailed Carry asking her what she meant by “It will be gun”. Carry replies saying that it was a typographical error and she meant “It will be fun”.	Mailbox Data Structure

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact #	**Timestamp**	**Header Information**	**Body**	**Map Screenshot**
1.	6/13/2012 19:01:21	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	
2.	6/13/2012 19:01:22	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	
3.	6/13/2012 19:04:03	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	
4.	7/2/2012 16:19:23	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	
5.	7/2/2012 16:19:24	WifiLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	
6.	7/5/2012 16:32:46	CellLocation	Location: Virginia Tech Research Center - Arlington (900 N Glebe Rd, Arlington, VA 22203)	
7.	7/5/2012	WifiLocation	Location: Virginia Tech Research Center -	

	16:32:47		Arlington (900 N Glebe Rd, Arlington, VA 22203)	
8.	7/5/2012 16:42:27	CellLocationLocal	226 Upshur St NW Washington, DC 20011	
9.	7/8/2012 16:39:10	CellLocationLocal	Location: National Gallery of Art Sculpture Garden	
10.	7/10/2012 16:31:10	CellLocation	Location: 2600-2700 24th Rd S, Arlington, VA 22206	
11.	7/10/2012 16:31:12	WifiLocation	Location: 2600-2700 24th Rd S, Arlington, VA 22206	
12.	7/10/2012 16:44:59	CellLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	
13.	7/10/2012 16:45:01	WifiLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	
14.	7/10/2012 16:46:29	WifiLocation	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	
15.	7/10/2012 16:47:12	CellLocationLocal	1521 North Quaker Lane, Alexandria, VA 22302 (CVS Pharmacy)	


Starred places
Private · 5 places
National Gallery of Art – Sculpture Garden
4.7 ★★★★½ (870)
Sculpture museum ·
Constitution Ave NW &, 7th St NW
Outdoor ice skating rink with a cafe
Closes soon · 5PM · Opens 10AM Mon
226 Upshur St NW
Washington, DC 20011
1521 N Quaker Ln
Alexandria, VA 22302
Virginia Tech Research Center - Arlington
4.1 ★★★★☆ (8)
University · 900 N Glebe Rd
2600 24th Rd S, Arlington, VA 22206
Bethesda
Takoma Park
Cabin John
Glen Echo
Potomac River
George Washington Pkwy
McLean
Tysons
NORTHWEST WASHINGTON
226 Upshur St NW Washington, DC 20011
GEORGETOWN
National Gallery of Art –... Outdoor ice skating rink with a cafe
CAPITOL HILL
Virginia Tech Research Center...
Falls Church
VIRGINIA
Merrifield
Seven Corners
Strathmeade Springs
Bailey's Crossroads
2600 24th RD S, Arlington, VA 22206
Annandale
1521 N Quaker Ln Alexandria, VA 22302
Capital Beltway Outer Lp
Alexandria
Oxon Hill
Springfield
Rose Hill
Franconia
Belle Haven
NATIONAL HARBOR
Layers
Google