

# 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, Pat, Coral and King conspired to plan a heist of the Nation gallery in July 2012. Tracy's Iphone revealed correspondence between the parties in relation to the heist.

## Equipment and Tools

- Autopsy
- Linux
- Nano
- SQLite
- Google Docs Google Maps
- Nessus

## Details of Tracy's iPhone

Case Name: 2012-07-15-National-Gallery

Case #: 1EZ215-P

---

## Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	Iphone 1,2	vol5/mobile/Library/Logs/Apple/Support/general.log
Host Name	Tracy Sumtwelve Iphone	vol5/logs/lockdown.log.1
OS Version	4.2.1	vol5/mobile/Library/Logs/Apple/Support/general.log
Install Time	06/06/2012	vol5/lockdownd.log.1
User Email	tracysumtwelve@gmail.com	vol5/mobile/Library/Mail/Envelope_Index
Phone Number	(703) 340-9661	vol5/lockdownd.log.1
Serial Number	86004482Y7H	vol5/mobile/Library/Logs/Apple/Support/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log.1
IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash		

## Evidence to Establish Personas

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

Tracy: (Also known as Coral Blue)

Phone Number: (703) 340-9961

Personal Email: tracysumtwelve@gmail.com  
Work Email: [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org)  
Heist Email: coralbluetwo@hotmail.com  
Relationship: Mother of Terry/ Ex wife of Joe

Pat: (Also know as Perry)  
Phone Number: (571) 308-3236  
Email: patsumtwelve@gmail.com  
Relationship: Brother of Tracy

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

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

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

King:  
Email: [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  
Relationship: Old acquaintance of Pat

The majority of data was collected from Tracey's Iphone and from her computer relating to a planned heist of the National Gallery. Tracy was working under the alias of Coral Blue to collude with her brother Pat, also known by the alias of Perry. They were blackmailing another party known as King to assist them with carrying out the heist. Carry who was a co worker of Tracy at the National Gallery was also assisting with the heist

## 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.

Evidence in Appendix A directly relates to email and SMS correspondence between the alleged parties Tracy, Pat, King and Carrey with some of the communications carried out using alias as shown in this report. Including log in details for one of the accounts. (Artifacts 1 - 4)

Financial motivation for all parties involved is reflected in the evidence provided. Specifically Tracey as she was struggling to pay for her daughter's school fees. (Artifact 5)

There is reference to an upcoming exhibition that looks to be of interest to the alleged parties (Artifacts 6 - 7)

Tracey and Carry conversate about sneaking a Tablet into the National Gallery (Artifact 14)

King was blackmailed with the threat of his parole being revoked and decided to partake in the heist, supplying a list of items needed to complete the heist (Artifact 12 and 22)

Copies containing information relating to the value of multiple items at the National Gallery which are believed to have been illegally obtained are documented in (Artifact 23 - 25)

Photographs that were taken of the surroundings at the National Gallery, including a photo of the front sign are shown in the following.  
(Artifacts 26 and 27)

Photographs showing images of certain stamps the alleged parties were interested in that reside at the national Gallery are shown in (Artifacts 28 - 33)

(Artifacts 34 and 35) shows geo locations that were translated from IP addresses contained in email correspondence.

(Artifacts 36 - 39) were geo locations that were gathered from Tracey's Iphone of possible important locations she visited around the time of the proposed heist.

## Plot Timeline

Plot Timeline	
June, 19th, 2012	Pat emails Tracey to confirm he is willing to participate and inform her that they should start using their alias email accounts.
June, 28th, 2012	Tracey and Pat both admit they are looking for an opportunity to get themselves out of financial hardship.
July, 7th, 2012	Tracey informs Pat that there is an exhibit that consists of rare stamps that are highly valuable. Pat replies asking her to gather intel.
July, 6th, 2012	Pat emails Tracey with the login details for her alias account for the second time. including username and password.
July 8th 2012	Images taken outside the National Gallery and of certain high value items of interest are captured by Tracey.
July 9th 2012	An email with an attachment including stamp values is sent from Tracey's normal email to her Alias email.
July 10th 2012	King has sent Pat an email with a list of tools that will be needed to successfully complete the heist.
July 11th 2012	Tracey and Carrey converse about sneaking a tablet into the National Gallery.

## Conclusion

Evidence found on Tracy's iPhone indicated the following:

The evidence supports the allegations that Tracey, Pat, King and Carey all worked together to plan a heist on the Nation Gallery. They went to effort to try and conceal their identities with the use of email aliases and covert communication techniques.

The evidence also shows motive as they were in financial trouble. The email communication proves that Tracey used the Alias Coral and Pat used the Alias Perry.

## Appendix A: Correspondence Evidence

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

### Correspondence Evidence Worksheet

Cameron Wright

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
001	Jun 19, 2012, 20:06:33	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:tracey whole@gmail.com">tracey whole@gmail.com</a> Subject: Paris Speak...	Pat emails Tracey to inform her that he is willing to carry out the task and asks her to start using their email alias for further communication	vol_5/mobile/Library/Mail/*
002	Jun 19, 2012, 21:38:59	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:tracey whole@gmail.com">tracey whole@gmail.com</a> Subject: Crazy Dave to the VM's	Pat emails Tracey to tell her to check out an audio file that is attached.	vol_5/mobile/Library/Mail/*
003	Jun 28, 2012, 19:31:33	From: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> To: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject: whats going on coral	Pat is confirming with Tracey that moving forward all communication should be done through their alias accounts and the Virtual Machine.	vol_5/mobile/Library/Mail/*
004	Jul 6, 2012, 11:42	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:tracey whole@gmail.com">tracey whole@gmail.com</a>	Pat is giving his sister Tracey the login details for the alias account <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Password: legalBee.	vol_5/mobile/Library/Mail/Protected_Index
005	Jun 28, 2012, 04:16	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:tracey whole@gmail.com">tracey whole@gmail.com</a> Subject: whats going on coral	Both parties are looking for an opportunity to make some money as both parties are experiencing financial difficulties. They are worried about IA sniffing around.	vol_5/mobile/Library/Mail/Protected_Index

006	Jun 29, 2012, 15:21:35	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:traceysumtwelve@gmail.com">traceysumtwelve@gmail.com</a> Subject: whats going on coral	Pat informs Tracey that he is certain that he can get the job done	vol_5/mobile/Library/Mail/Protected_Index
007	Jul 02, 2012, 16:13:18	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:traceysumtwelve@gmail.com">traceysumtwelve@gmail.com</a> Subject: Re: Some good news	Tracy emails Pat to let him know that there is an interesting foreign exhibit coming up and she is going through the information to see if it would be worth their effort. Pat is excited about this.	vol_5/mobile/Library/Mail/*
008	Jul 03, 2012, 14:53:04	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:traceysumtwelve@gmail.com">traceysumtwelve@gmail.com</a> Subject: Re: Some good news	Tracy informs Pat that the exhibit consists of stamps that are rare and highly valuable.  Pat replies asking her to gather as much intel possible and he would look into how they would pull off the heist.	vol_5/mobile/Library/Mail/*
009	Jul 05, 2012, 15:51:31	From: <a href="mailto:carrysum2012@yahoo.com">carrysum2012@yahoo.com</a> To: <a href="mailto:traceysumtwelve@gmail.com">traceysumtwelve@gmail.com</a> Subject: Long time no see	Carry contacts Tracey to catch up for lunch. Carry also states that she noticed on Facebook Tracy was having a hard time lately.	vol_5/mobile/Library/Mail/*
010	Jul 06, 2012, 15:27:51	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:traceysumtwelve@gmail.com">traceysumtwelve@gmail.com</a> Subject: Re: Good news	Tracy emails Pat to let him know she spoke with Coral and she has some great news about her job. suggests Pat catches up with Coral.  Pat replies saying that he knows a guy called King	vol_5/mobile/Library/Mail/*
011	July 9, 2012, 14:44:11	From: <a href="mailto:traceysumtwelve@gmail.com">traceysumtwelve@gmail.com</a> To: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject: things	“somethings” was the message body and attached was a file name “document.zip”	vol_5/mobile/Library/Mail/*
012	July 10, 2012, 11:19	From: <a href="mailto:throne1966@hotmail.com">throne1966@hotmail.com</a> To: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> CC: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a>	The email from king to Pat was indicating which tools he would need to complete the job. Pat was also blackmailing King with the threat of giving his parole officer information that would lead to him being sent	vol_5/mobile/Library/Mail/*

			back to jail. Attached was a list of tools under the name needs.txt	
013	July 10, 2012, 15:24:57	From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject: cant pass up	coral blue was included in the above email thread relating to the tools needed to complete the heist.	vol_5/mobile/Library/Mail/*
014	Jul 11, 2012, 17:06:19	From: <a href="mailto:carrysum2012@yahoo.com">carrysum2012@yahoo.com</a> To: <a href="mailto:tracysumtwelve@gmail.com">tracysumtwelve@gmail.com</a> Subject: Long time no see	Tracey and Carry converse about sneaking in a tablet to the National Gallery. They agree to work together and figure out a plan relating to the shift change of the security officers that are working. Tracy confirms with carry they will meet at 9 tomorrow	vol_5/mobile/Library/Mail/*

## SMS Correspondence Evidence Worksheet

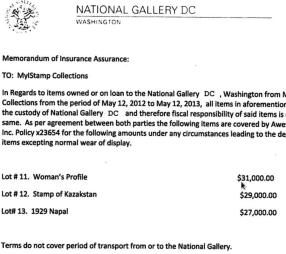
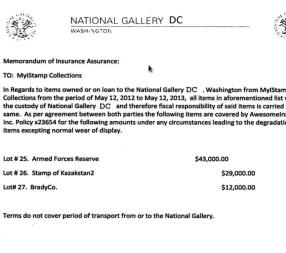
Cameron Wright

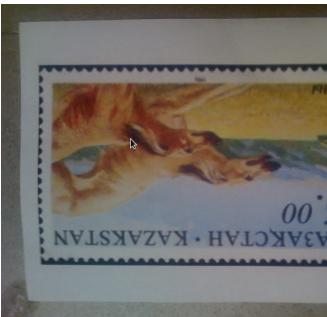
---

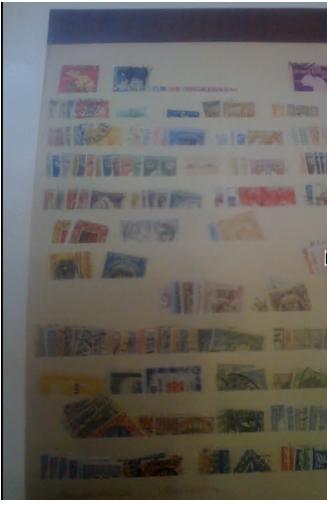
Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
015	Jul 03, 2012, 13:41:51	From: Tracy To: Terry	Tracey explains to her daughter that she cant keep attending Prufrock as they cant afford it. Shows evidence towards financial hardship and motive,	vol_5/mobile/SMS/sms.db
016	Jul 05, 2012, 18:18:23	From: Carry To: Tracey	Confirm that they will meet at Bubbas grill at 1pm	vol_5/mobile/SMS/sms.db
017	Jul 06, 2012, 15:11:54	From: Tracey To: Pat	Tracey replies to Pats message which said he was busy, Tracey insists that it is important and she needs to speak straight away.	vol_5/mobile/SMS/sms.db
018	Jul 06, 2012,	From: Pat To: Tracey	Pat agrees to call in 5 minutes	vol_5/mobile/SMS/sms.db

	15:13:31			
019	Jul 10, 2012, 15:26:19	From: Pat To: Tracey	Pat texts Tracey asking her to inform "Coral" that the email attachment needs to be changed to a pdf before it can be opened.	vol_5/mobile/ SMS/sms.db
020	Jul 11, 2012, 12:49:08	From: Tracey To: Carry	Tracey texts Carry informing her to meet out the front and she will take the tablet into the Nation Gallery as planned.	vol_5/mobile/ SMS/sms.db
021	Jul 12, 2012, 17:06:45	From: Tracey To: Carry	Tracey messages akings about the flash mob.	vol_5/mobile/ SMS/sms.db

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Image
22	July 10, 2012, 11:19	From: throne1966@hotmail.com To: patsumtwelve@gmail.co m CC: coralbluetwo@hotmail.co m	In relation to artifact 12, this is a copy of the file that was attached to the email.	<ul style="list-style-type: none"> <li>-A rope and javelin (using alternative me</li> <li>-tactical turtlenecks ( what i will be wearin</li> <li>-spray paint (for the cameras)</li> <li>-vibram five finger shoes (in order to wal</li> <li>-pack of smokes (detecting lasers)</li> <li>-smoke grenades (use as a means of es</li> </ul>
23	July 9, 2012, 14:44:11	From: traceysumtwelve@gmail. com To: coralbluetwo@hotmail.co m Subject: things	In relation to artifact 11, this is a copy of the attachment 1 of 3 referred to in the email as document.zip  These documents are in reference to the stamps values	 <b>NATIONAL GALLERY DC</b> WASHINGTON  Memorandum of Insurance Assurance: TO: MyStamp Collections In Regards to Items owned or on loan to the National Gallery of Art, Washington Inc. Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned are under the custody of National Gallery DC and therefore fiscal responsibility of said items same. As per agreement between both parties the following items are covered by the Inc. Policy #X3654 for the following amounts under any circumstances leading to the loss of the items excepting normal wear of display.  Lot # 1. Douglas MacArthur \$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.

24	July 9, 2012, 14:44:11	<p>From: traceysumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: things</p>	<p>In relation to artifact 11, this is a copy of the attachment 2 of 3 referred to in the email as document.zip</p> <p>These documents are in reference to the stamps values</p>	 <p><b>NATIONAL GALLERY DC</b> WASHINGTON</p> <p><b>Memorandum of Insurance Assurance:</b></p> <p>To: MyStamp Collections</p> <p>In Regards to items owned or on loan to the National Gallery DC - Washington from MyStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list is same. As per agreement between both parties the following items are covered by Awe Inc. Policy #2654 for the following amounts under any circumstances leading to the de-items excepting normal wear of display.</p> <table border="1"> <tr> <td>Lot # 11. Woman's Profile</td> <td>\$31,000.00</td> </tr> <tr> <td>Lot # 12. Stamp of Kazakhstan</td> <td>\$29,000.00</td> </tr> <tr> <td>Lot# 13. 1929 Nepal</td> <td>\$27,000.00</td> </tr> </table> <p>Terms do not cover period of transport from or to the National Gallery.</p>	Lot # 11. Woman's Profile	\$31,000.00	Lot # 12. Stamp of Kazakhstan	\$29,000.00	Lot# 13. 1929 Nepal	\$27,000.00
Lot # 11. Woman's Profile	\$31,000.00									
Lot # 12. Stamp of Kazakhstan	\$29,000.00									
Lot# 13. 1929 Nepal	\$27,000.00									
25	July 9, 2012, 14:44:11	<p>From: traceysumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: things</p>	<p>In relation to artifact 11, this is a copy of the attachment 3 of 3 referred to in the email as document.zip</p> <p>These documents are in reference to the stamps values</p>	 <p><b>NATIONAL GALLERY DC</b> WASHINGTON</p> <p><b>Memorandum of Insurance Assurance:</b></p> <p>To: MyStamp Collections</p> <p>In Regards to items owned or on loan to the National Gallery DC - Washington from MyStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list is same. As per agreement between both parties the following items are covered by Awe Inc. Policy #2654 for the following amounts under any circumstances leading to the degradation of items excepting normal wear of display.</p> <table border="1"> <tr> <td>Lot # 25. Armed Forces Reserve</td> <td>\$43,000.00</td> </tr> <tr> <td>Lot # 26. Stamp of Kazakhstan2</td> <td>\$29,000.00</td> </tr> <tr> <td>Lot# 27. BradyCo.</td> <td>\$12,000.00</td> </tr> </table> <p>Terms do not cover period of transport from or to the National Gallery.</p> <p><i>D</i> President National Gal</p>	Lot # 25. Armed Forces Reserve	\$43,000.00	Lot # 26. Stamp of Kazakhstan2	\$29,000.00	Lot# 27. BradyCo.	\$12,000.00
Lot # 25. Armed Forces Reserve	\$43,000.00									
Lot # 26. Stamp of Kazakhstan2	\$29,000.00									
Lot# 27. BradyCo.	\$12,000.00									
26	July 8, 2012, 12:34:50 pm	<p>Traceys Iphone</p> <p>Image taken outside the National Gallery</p>	<p>Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0044</p>							
27	July 08, 2012, 12:37:37 pm	<p>Traceys Iphone</p> <p>Image taken of the front Nation Gallery wall signage</p>	<p>Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0048</p>							
28	July 08, 2012, 12:41:41 pm	<p>Traceys Iphone</p> <p>Image taken of Stamps inside the National Gallery</p>	<p>Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0049</p>							

29	July 08, 2012, 12:41:53	Traceys Iphone  Image taken of Stamps inside the National Gallery	Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0050	
30	July 08, 2012, 12:42:03 pm	Traceys Iphone  Image taken of Stamps inside the National Gallery	Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0051	
31	July 08, 2012, 12:49:25 pm	Traceys Iphone  Image taken of Stamps inside the National Gallery	Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0054	

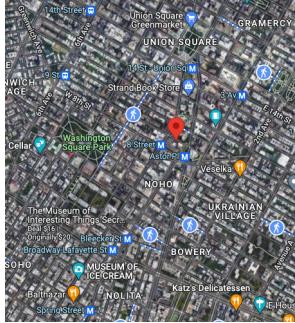
32	July 08, 2012, 12:49:49	Traceys Iphone  Image taken of Stamps inside the National Gallery	Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0056	
33	July 08, 2012, 12:50:20 pm	Traceys Iphone  Image taken of Stamps inside the National Gallery	Evidence Location: vol_5/mobile/Library/Media/DCIM /100APPLE/IMG_0058	

# Appendix B: WiFi and GPS Location Information

## Correspondence Evidence Worksheet

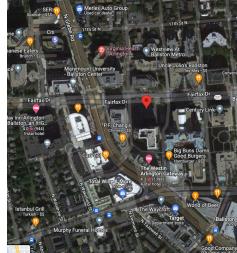
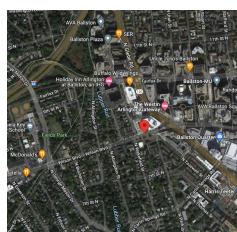
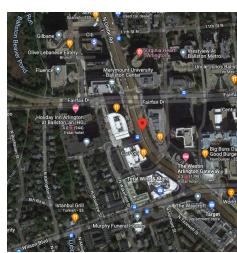
Group members:

---

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Ariel Photo (Google Maps)
034	19 Jun, 2012, 21:39:04	To: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> From: perrypatsum@yahoo.com	email header shows the senders IP address as 98.138.89.197.  The IP address was calculated to give the approximate location of 40.73084, -73.99140. As shown in the picture on the right.	
035	09 Jul, 2012 14:44:11	To: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> From: traceysumtwelve@gmail.com	email header shows traceys IP to be 174.254.176.91  The IP address was calculated to give the approximate location of 39.0437, -77.4875. As shown in the picture to the right	

---

Artifact #	Location	Key Information	Evidence Location	Ariel Photo (Google Maps)

036	38°52'54.9"N 77°06'51.7"W	4420 Fairfax Dr, Arlington, VA 22203, USA	vol_5/root/Library/Caches/I ocationd/consolidated.db	
037	38°52'46.9"N 77°06'55.8"W	801 N Wakefield St, Arlington, VA 22203, USA	vol_5/root/Library/Caches/I ocationd/consolidated.db	
038	38°52'53.0"N 77°06'56.1"W	851-977 N Glebe Rd, Arlington, VA 22203, USA	vol_5/root/Library/Caches/I ocationd/consolidated.db	
039	38°52'50.0"N 77°06'55.9"W	900 N Glebe Rd, Arlington, VA 22203, USA	vol_5/root/Library/Caches/I ocationd/consolidated.db	