

# 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.

- Evidence that Tracy was financially motivated to conspire to the theft of Stamps at the National Gallery DC.
- Evidence that one Pat Sumtwelve, was a co-conspirator in the theft.
- Evidence that a person by the name of Carry (surname unknown) was colluding with Tracy to have a flashmob at the gallery. Unknown to Tracy this flashmob actually was there to deface art exhibits

## Equipment and Tools

- Autopsy Application
- Kali Linux Machine
- Sqlitebrowser

## Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	Iphone 1,2	General.log
Host Name	Tracy Sumtwelve's Iphone	Lockdownd.log.1
OS Version	Iphone OS 4.2.1 (8C148)	General.log
Install Time	6/6/2012 12:03:28 -0700	General.log
User Email	Tracy.sumtwelve@nationalgallerydc.org tracysumtwelve@gmail.com	image_Tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/mail

Phone Number	703-340-9661	Lockdownd.log.1
Serial Number	86004482Y7H	General.Log
ICCID	890141032551953 42366	Lockdownd.log.1
IMEI	12021003735398	wildcard_record.plist
MD5 Hash	Cde7ae3ac48c0345e9a1988b0e90715d	Data Source/ Tracy-phone/File Meta Data

## Evidence to Establish Personas

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

Tracy (AKA Coral):

Phone Number: (703) 340-9961  
 Personal Email: tracysumtwelve@gmail.com  
 Work Email: tracy.sumtwelve@nationalgallerydc.org  
 Relationship: Accused

Pat:

Phone Number: 571-308-3236  
 Email: perrypatsum@yahoo.com  
 Relationship: Brother

Terry:

Phone Number: 703-829-6071  
 Email:  
 Relationship: Daughter

Joe:

Phone Number: N/A  
Email: [Joe.sum.twelve@gmail.com](mailto:Joe.sum.twelve@gmail.com)  
Relationship: Ex-Husband

Carry:

Phone Number: 36380811  
Email: [carrysum2012@yahoo.com](mailto:carrysum2012@yahoo.com)  
Relationship: Co Conspirator

[Provide a summary of your conclusions here.]

## 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.

[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

## 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.

[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

# Plot Timeline

Artifact#	Timestamp	Header Information	Key Information	Evidence Location
1	6/12/2012 21:25:04	From: Pat To: Tracy	What are you up to this weekend?	SMS-Message Data
2	6/12/2012 10:04:50	From: (650) 887-0260 To: Tracy	This call lasted only 20 seconds from data received.	Call-Data
3	6/12/2012 20:52:14	From: (703) 829-6191 To: Tracy	This call lasted 56 seconds as shown on the chart.	Call-Data
4	6/13/2012 16:29:13	From: Tracy To: Pat	Tracy called Pat but there was no answer.	Call-Data
5	6/13/2012 17:30:28	From: Terry To: Tracy	I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook.	SMS-Message Data
6	6/13/2012 18:30:38	From: Tracy To: Pat	I don't have any big plans. How about you?	SMS-Message Data
7	6/13/2012 18:33:46	From: Tracy To: Terry	Ok, sounds good.	SMS-Message Data
8	6/19/2012 14:38:59	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com	Subject: Crazydave by the VMs	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.
9	6/22/2012 17:34:26	From: (571) 245-8517 To: Tracy	As you can see on the chart Tracy missed a call from (517)245-8517	Call-Data failed
10	7/3/2012 13:41:51	From: Tracy To: Terry	Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?	SMS-Message Data
11	7/3/2012 14:04:32	From: Terry To: Tracy	moving schools at this point would be the worst! I would rather live with dad and stay at prufrock then change schools :(	SMS-Message Data
12	7/5/2012 18:18:23	From: Carry To: Tracy	Sounds good let's shoot for one at Bubba's grill	SMS-Message Data
13	7/5/2012 18:20:26	From: Tracy To: Carry	Okay that sounds great. See you there	SMS-Message Data
14	7/6/2012 11:49:31	From: patsumtwelve@gmail.com To: 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.	EMAIL-MailBox Data
15	7/6/2012 15:02:19	From: Tracy To: Pat	Hey can you give me a call	SMS-Message Data
16	7/6/2012 15:08:37	From: Pat To: Tracy	Sis I'm really busy can we can do this later	SMS-Message Data
17	7/6/2012 15:11:54	From: Tracy To: Pat	No pat this is important I need you to call me soon	SMS-Message Data
18	7/6/2012 15:13:31	From: Pat To: Tracy	Ok ok I'll call in 5	SMS-Message Data
19	7/6/2012 15:18:50	From: Carry To: Tracy	Pat calls Tracy and as you can see from the data they spoke for approximately 4 minutes and 4 seconds.	Call-Data
20	7/6/2012 16:27:16	From: Carry To: Tracy	I have a table inside	SMS-Message Data
21	7/6/2012 16:27:50	From: Tracy To: Carry	Okay brt	SMS-Message Data
22	7/7/2012 19:36:35	Congratulations, your entry in last months drawing won you a FREE \$1,000 Target Giftcard! Enter "703" at	www.target.com.trdt.biz to tell us where to ship it	SMS-Message Data
23	7/9/2012 10:44:11	From: tracysuntwelve@gmail.com To: coralbluetwo@hotmail.com	Subject: things	docs.zip is an encrypted ZIP folder containing 3 insurance documents related to stamps. documents.zip is a compressed ZIP folder that contains the un-encrypted docs.zip which contains 3 insurance documents related to stamps.
24	7/10/2012 11:19:00	From: patsumtwelve@gmail.com To: coralbluetwo@hotmail.com	Subject: FWD: can't pass up Attachment: needs.txt Email Thread: can't 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.	EMAIL-MailBox Data
25	7/10/2012 15:26:19	From: Pat To: Tracy	hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know	SMS-Message Data
26	7/10/2012 15:58:04	From: Tracy To: Pat	Sure thing I'll get on it	SMS-Message Data
27	7/10/2012 16:37:09	From: Tracy To: Pat	Message failed	SMS-MMS-Message Data
28	7/10/2012 17:18:38	From: Tracy To: Terry	Going to lunch. You want to go?????	SMS-Message Data
29	7/10/2012 18:19:24	From: Tracy To: Terry	Back at work	SMS-Message Data
30	7/10/2012 18:58:24	From: Terry To: Tracy	I'm busy. Maybe this weekend if dad isn't busy	SMS-Message Data
31	7/11/2012 12:41:45	From: Carry To: Tracy	I'm almost there where should I meet you?	SMS-Message Data
32	7/11/2012 12:49:08	From: Tracy To: Carry	Just meet me out front, I'll take the tablet in.	SMS-Message Data
33	7/12/2012 17:06:45	From: Tracy To: Carry	How's the flashmob going	SMS-Message Data
34	7/13/2012 1:02:10	From: Terry To: Tracy	I really want to go to Dad's this weekend. He said he'll take me shopping for school	SMS-Message Data

## Conclusion

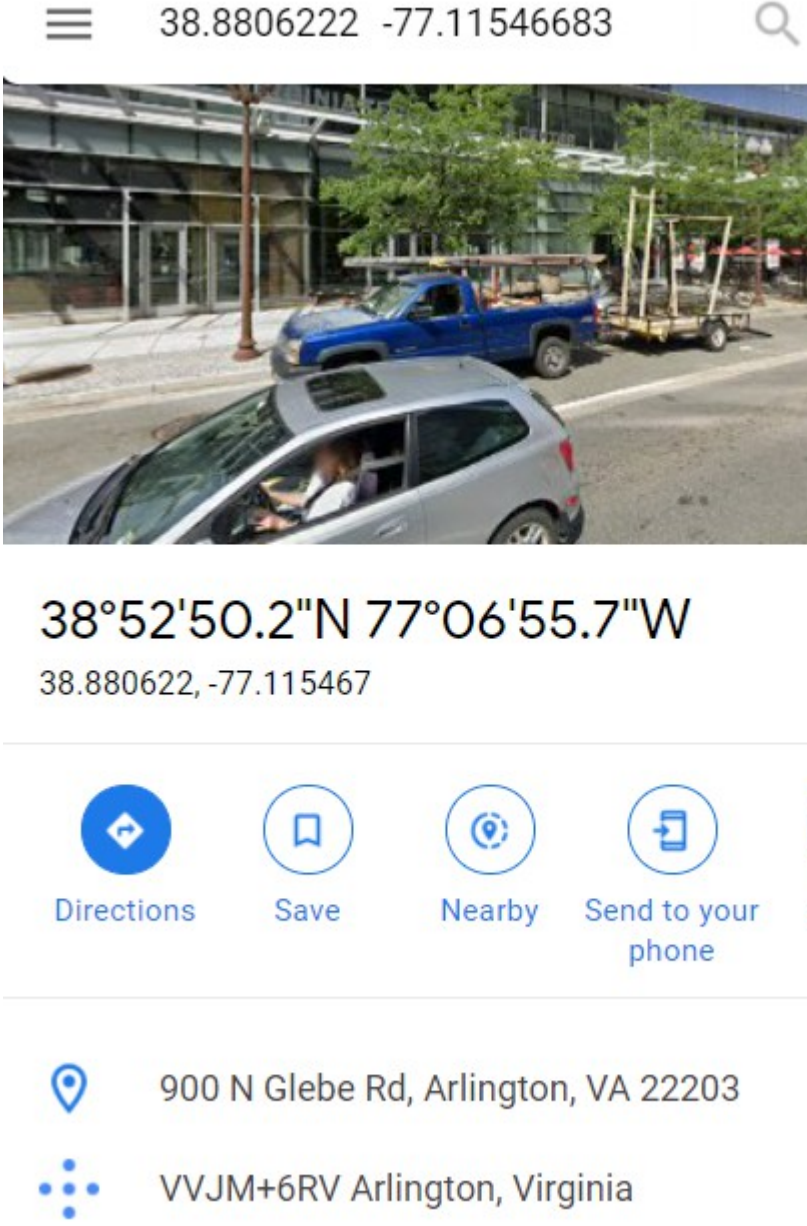
Evidence found on Tracy's iPhone indicated the following:

- Tracy used the alias Coral
- Pat used the alias Perry
- Tracy and Pat coluded to steal a stamp collection from the National Gallery
- Pat was blackmailing a person by the name of King for help with the theft
- Tracy met Cary at Bubba's Grill

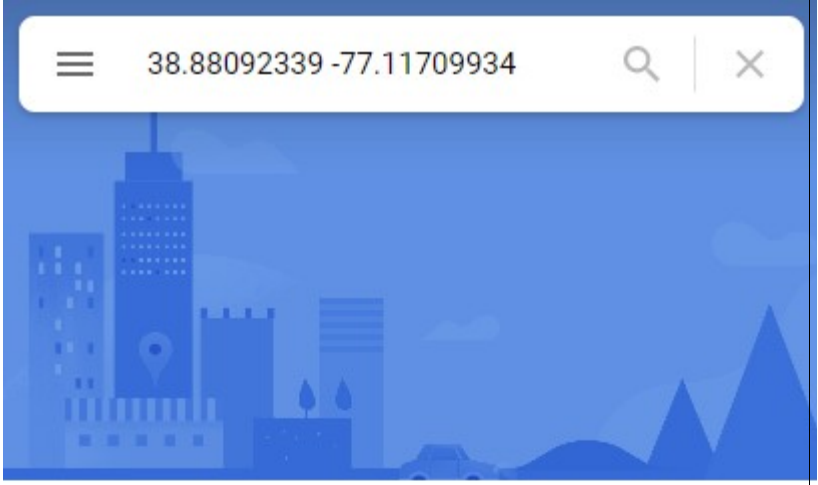
## Appendix A: Correspondence Evidence

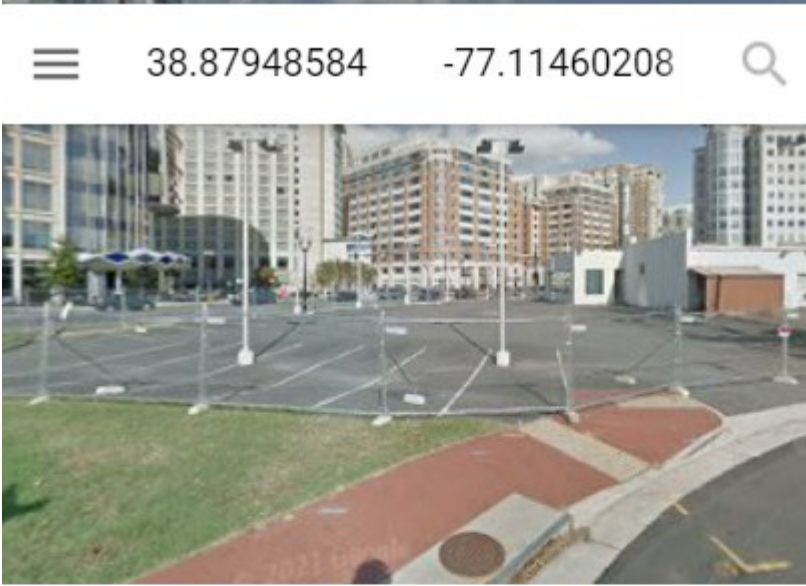
See Plot timeline for the Correspondence Evidence

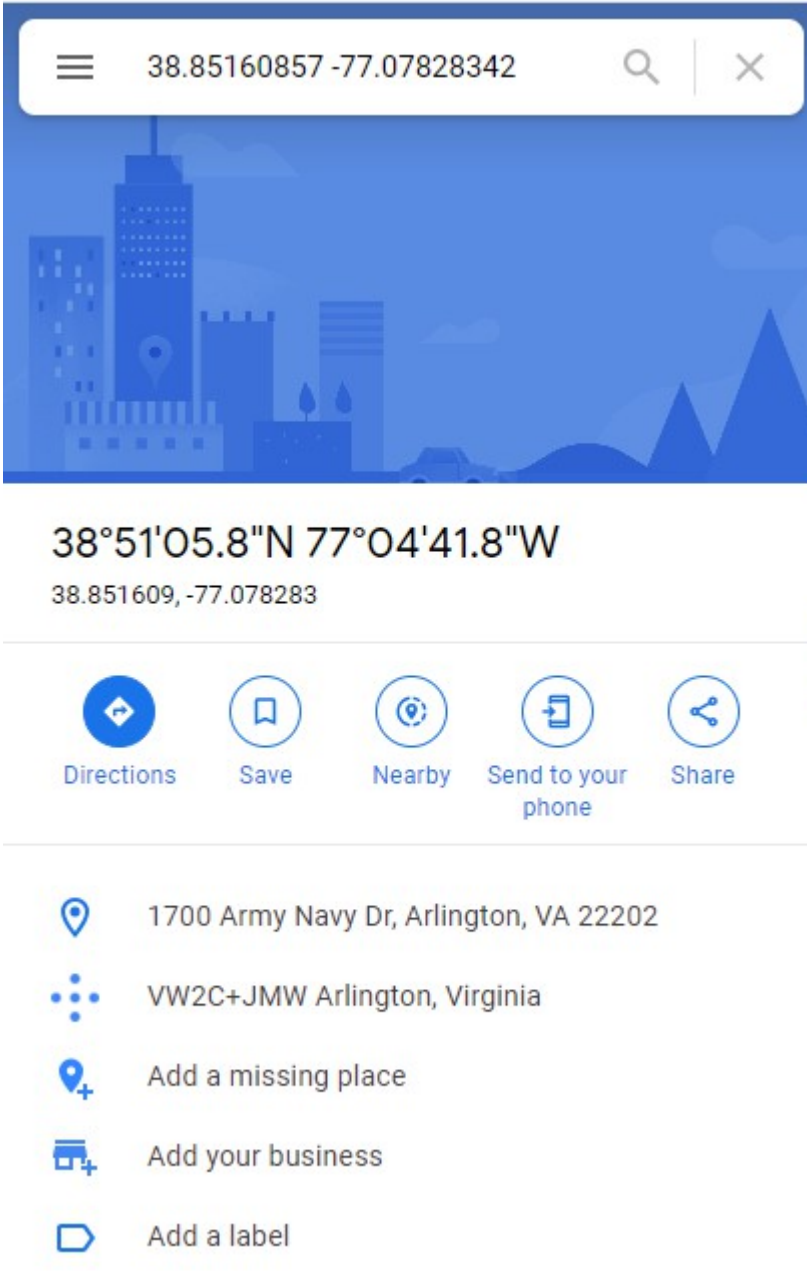
## Appendix B: WiFi and GPS Location Information

Timestamp	Relative path	Map Screenshot
2012-06-13 19:01:21	root/Library/Caches/locationd/consolidated.db	 <p>38.8806222 -77.11546683</p> <p>38°52'50.2"N 77°06'55.7"W 38.880622, -77.115467</p> <p>Directions Save Nearby Send to your phone</p> <p>900 N Glebe Rd, Arlington, VA 22203</p> <p>VVJM+6RV Arlington, Virginia</p>

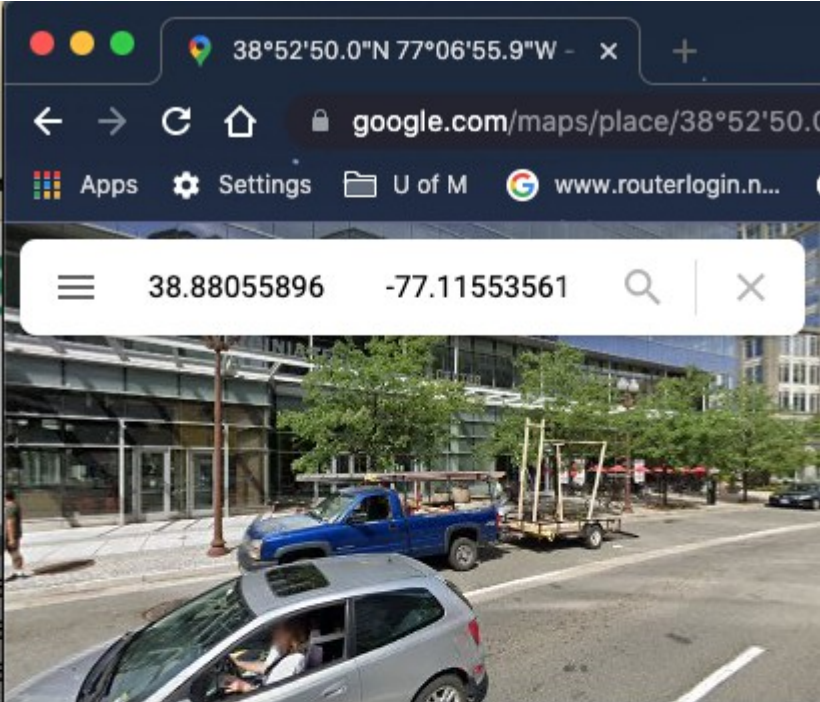









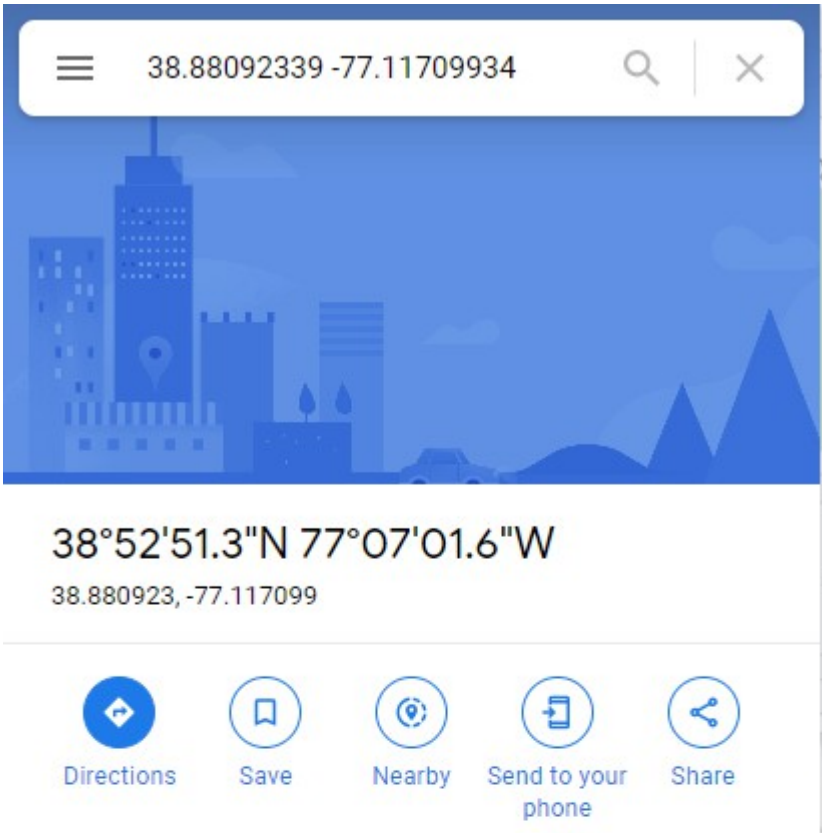
Timestamp	Relative path	Map Screenshot
2012-07-02 16:19:23	root/Library/Caches/locationd/consolidated.db	 <p data-bbox="657 871 1161 955">38°52'51.3"N 77°07'01.6"W 38.880923, -77.117099</p> <div data-bbox="657 1018 1347 1176"><p>Directions Save Nearby Send to your phone Share</p></div> <div data-bbox="657 1239 1218 1606"><p>4600 Fairfax Dr, Arlington, VA 22203</p><p>VVJM+956 Arlington, Virginia</p><p>Add a missing place</p><p>Add your business</p><p>Add a label</p></div>

Timestamp	Relative path	Map Screenshot
2012-07-05 16:32:46	root/Library/Caches/locationd/consolidated.db	 <p data-bbox="631 982 1279 1094"> <b>38°52'46.2"N 77°06'52.6"W</b>  38.879486, -77.114602 </p> <div data-bbox="646 1171 1419 1360"> <div>Directions</div> <div>Save</div> <div>Nearby</div> <div>Send to your phone</div> </div> <div data-bbox="631 1444 1227 1703"> <div>Arlington, VA 22203</div> <div>VVHP+Q5R Arlington, Virginia</div> <div>Add a missing place</div> </div>

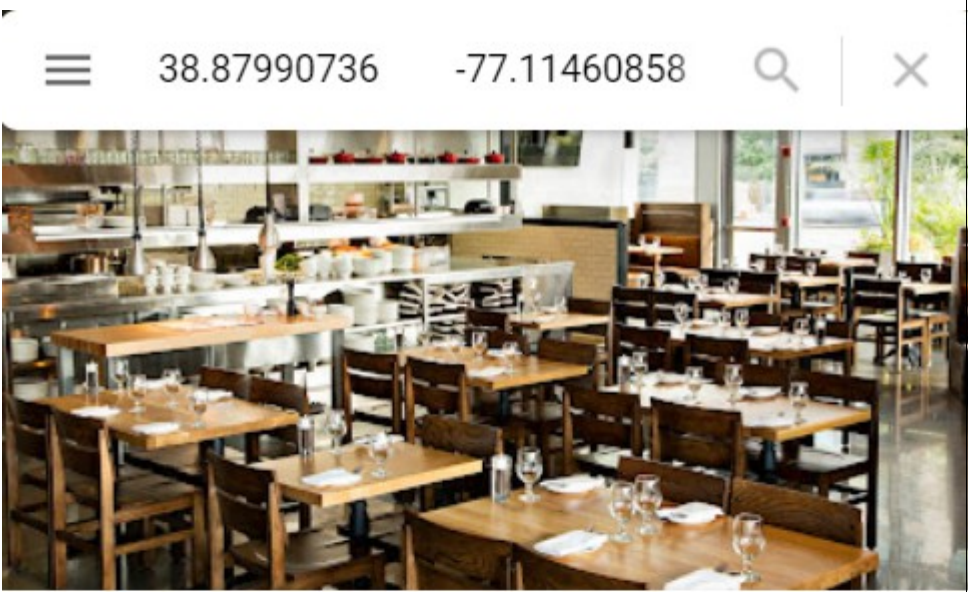










Timestamp	Relative path	Map Screenshot
2012-07-10 16:31:10	root/Library/Caches/locationd/consolidated.db	

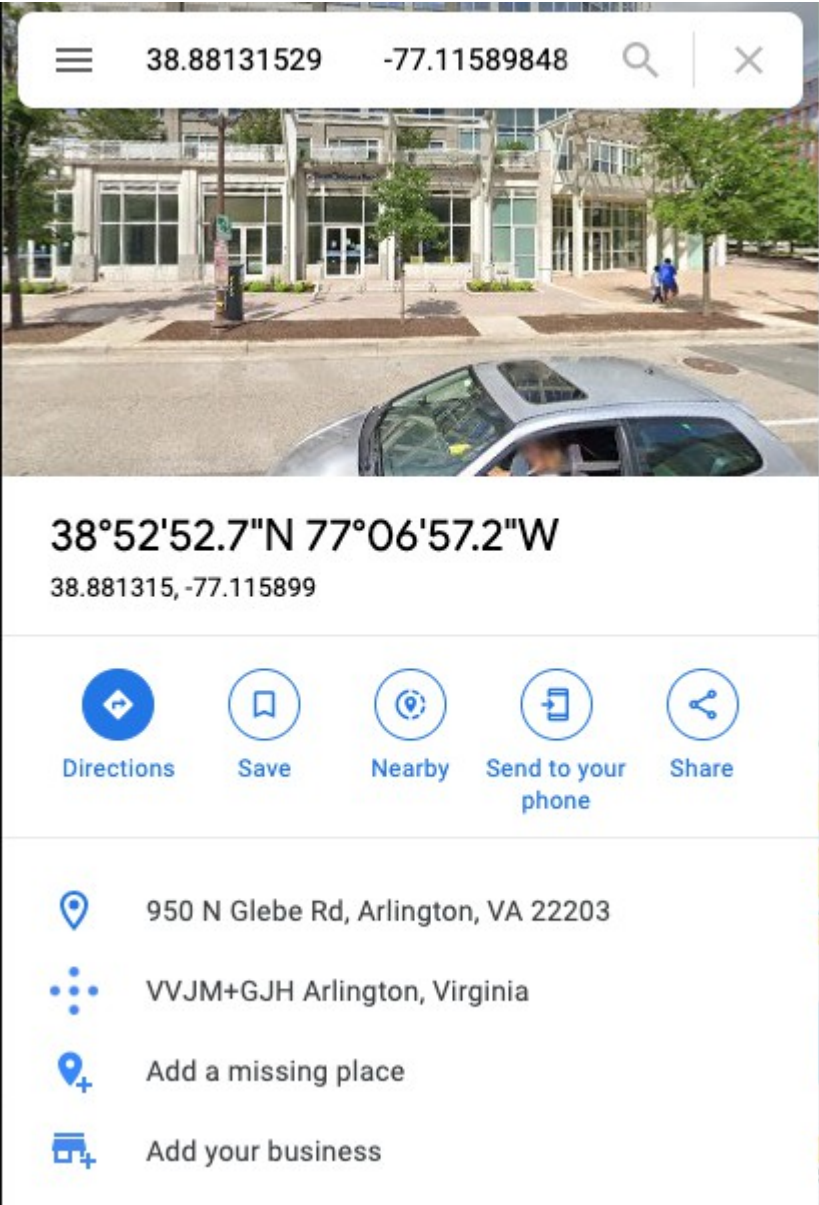
## Location Information (Wifi location)

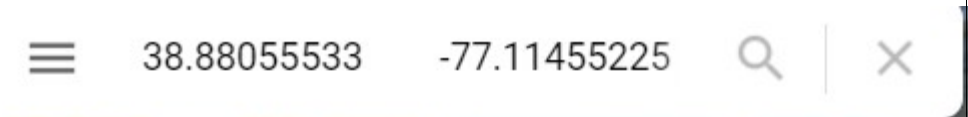









Timestamp	Relative path	Map Screenshot
2012-06-13 19:01:22	root/Library/Caches/locationd/consolidated.db	 <p data-bbox="656 1184 1182 1276"><b>38°52'50.0"N 77°06'55.9"W</b> 38.880559, -77.115536</p> <div data-bbox="656 1335 1344 1486"><div>Directions</div><div>Save</div><div>Nearby</div><div>Send to your phone</div><div>Share</div></div> <p data-bbox="656 1562 1218 1604"> 900 N Glebe Rd, Arlington, VA 22203</p> <p data-bbox="656 1638 1136 1680"> VVJM+6QG Arlington, Virginia</p>

Timest amp	Relative path	Map Screenshot
		
2012-07-02 16:19:24	root/Library/Caches/locationd/consolidated.db	<ul style="list-style-type: none"> <li>4600 Fairfax Dr, Arlington, VA 22203</li> <li>VVJM+956 Arlington, Virginia</li> <li>Add a missing place</li> <li>Add your business</li> <li>Add a label</li> </ul>












Timest amp	Relative path	Map Screenshot
2012- 07-03 13:42:4 2	root/Library/ Caches/loc ationd/cons olidated.db	 <p data-bbox="605 926 1570 1119">38°52'47.7"N 77°06'52.6"W 38.879907, -77.114609</p> <div data-bbox="605 1119 1570 1373"> Directions  Save  Nearby  Send to your phone  Share</div> <div data-bbox="605 1373 1570 1908"> 800 N Glebe Rd, Arlington, VA 22203  VVHP+X56 Arlington, Virginia  Add a missing place  Add your business  Add a label</div>

Timestamp	Relative path	Map Screenshot
2012-07-03 13:42:42	root/Library/Caches/locationd/consolidated.db	

Timestamp	Relative path	Map Screenshot
2012-07-05 16:32:47	root/Library/Caches/locationd/consolidated.db	<div data-bbox="605 342 1568 457"></div> <div data-bbox="605 457 1568 919"></div> <div data-bbox="623 961 1284 1073"><p>38°52'50.0"N 77°06'52.4"W</p><p>38.880555, -77.114552</p></div> <div data-bbox="638 1150 1484 1339"><div> Directions</div><div> Save</div><div> Nearby</div><div> Send to your phone</div><div> Share</div></div> <div data-bbox="623 1423 1325 1654"><div> 801 N Glebe Rd, Arlington, VA 22203</div><div> VVJP+65G Arlington, Virginia</div><div></div></div>



Timest amp	Relative path	Map Screenshot
2012- 07-10 16:31:1 2	root/Library/ Caches/loc ationd/cons olidated.db	<div data-bbox="605 342 1557 464"></div> <div data-bbox="605 464 1557 924"></div> <div data-bbox="605 924 1557 1119"><p data-bbox="605 924 1557 1024">38°52'51.3"N 77°06'51.3"W</p><p data-bbox="605 1024 1557 1077">38.880905, -77.114241</p></div> <div data-bbox="605 1119 1557 1373"><div data-bbox="605 1119 1557 1373"><div data-bbox="605 1119 779 1373"><p data-bbox="634 1268 774 1302">Directions</p></div><div data-bbox="779 1119 953 1373"><p data-bbox="850 1268 922 1302">Save</p></div><div data-bbox="953 1119 1127 1373"><p data-bbox="1016 1268 1120 1302">Nearby</p></div><div data-bbox="1127 1119 1339 1373"><p data-bbox="1159 1268 1339 1344">Send to your phone</p></div><div data-bbox="1339 1119 1557 1373"><p data-bbox="1386 1268 1474 1302">Share</p></div></div></div> <div data-bbox="605 1373 1557 1650"><div data-bbox="605 1373 1557 1650"><div data-bbox="605 1373 1557 1501"><p data-bbox="737 1444 1318 1486">801 N Glebe Rd, Arlington, VA 22203</p></div><div data-bbox="605 1501 1557 1650"><p data-bbox="737 1543 1198 1585">VVJP+986 Arlington, Virginia</p></div></div></div>