

Case Report National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]
Prepared by David Chen

Table of Contents

Executive Summary	2
Equipment and Tools	2
Details of Tracy's iPhone	2
Evidence to Establish Personas	3
Evidence relating to theft of valuable stamps	4
Evidence relating to defacement of museum art	4
Plot Timeline	5
Conclusion	5
Appendix A: Correspondence Evidence	0
Appendix B: WiFi and GPS Location Information	9

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 was motivated by financial gain
- Emails exchanged between
- Pat and Tracy agreed to use aliases Perry and Coral, respectively
- Alias emails have been setup for communication (Pat:perrypatsum@yahoo.com and Tracy:coralbluetwo@hotmail.com)
- Pat and Tracy colluding to steal "highly valuable stamp collection"
- Pat blackmailing King by threatening to get in touch with King's parole officer
- Tracy had obtained the insurance documents to send to Pat
- Tracy arranged to help Carry sneak in a tablet for a flash mob event

Equipment and Tools

The tools used in the analysis were:

- Kali Linux 4.18.0-kali2-amd64
- Autopsy 4.10.0
- DB Browser for SQLite 3.10.1
- Google Maps for Geolocation

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 3G	/mobile/Library/Logs/AppleSupport/general.log EXIF data from photo
Host Name	Tracy Sumtwelves Iphone	/logs/lockdownd.log.1
OS Version	4.2.1	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	/mobile/Library/Logs/AppleSupport/general.log
User Email	tracy.sumtwelve@nationalgallerydc.org tracysumtwelve@gmail.com coralbluetwo@hotmail.com	vol5/mobile/Library/Mail/Envelop Index
Phone Number	1 (703) 340-9661	/logs/lockdownd.log.1
Serial Number	86004482Y7H	/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	/logs/lockdownd.log.1
IMEI	012021003735398	root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Provided
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d65 77ccb534ca0d1e83ffd27683e621607	Provided

Evidence to Establish Personas

Tracy:

Phone Number:	+17033409961
Personal Email:	tracysumtwelve@gmail.com
Alias Email:	coralbluetwo@hotmail.com
Work Email:	tracy.sumtwelve@nationalgallerydc.org
Relationship:	Accused

Pat:

Phone Number:	+15713083236
Email:	patsumtwelve@gmail.com
Alias Email:	perrypatsum@yahoo.com
Relationship:	Brother of the Accused

Terry:

Phone Number:	+17038296071
Email:	NA
Relationship:	Daughter of the Accused

Joe:

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

Carry:

Phone Number:	+12027252124
Email:	carrysum2012@yahoo.com catsumtwelve@gmail.com
Relationship:	Acquaintance of the Accused

King:

Email:	throne1966@hotmail.com
Relationship:	Parolee of Pat's parole officer friend

Both Tracy and her brother Pat are using more than one email to communicate with each other under the aliases Coral and Perry respectively.

Evidence relating to theft of valuable stamps

Artifact	Date Time	Evidence
Appendix A – Artifact 6	21/06/2012 17:43:15	Establishment of aliases to be used in communication
Appendix A – Artifact 13	03/07/2012 14:53:04	Tracy advises Pat that there is an exhibit with rare and highly valuable stamp collection and Pat replies asking Tracy to obtain more information about the stamps
Appendix A – Artifact 16	06/07/2012 15:49:31	Pat threatening King's parole and recommends King take on the heist
Appendix A – Artifact 18	09/07/2012 14:44:11	Tracy emails Pat insurance documents that she had obtained about the stamps
Appendix A – Artifact 21	10/07/2012 15:24:57	King replying to Pat and Coral, agreeing to do the heist, and requested equipment for the job
Appendix A – Artifact 41	10/07/2012 15:26:19	Pat sends Tracy an SMS with directions on changing the extension of the file sent by King to .pdf
Appendix A – Artifact 43	10/07/2012 16:37:09	Tracy attempted to share a location to Pat over MMS Location: 2600-2700 24th Rd S, Arlington, VA 22206
Appendix B – Artifact 12	10/07/2012 16:31:12	WiFi location from Tracy's iPhone puts her at the location she attempted to share with Pat on 24th Rd S, Arlington, VA 22206

Evidence relating to defacement of museum art

Artifact	Date Time	Evidence
Appendix A – Artifact 14	05/07/2012 15:51:31	Carry emails Tracy asking to meet up. Mentions she "saw on Facebook" that Tracy was "having a hard time lately"
Appendix A – Artifact 32	05/07/2012 18:18:23	Carry sets up a time and location to meet up with Tracy: 1pm at Bubba's grill
Appendix A – Artifact 33	05/07/2012 18:20:26	Tracy confirms meeting time and location with Carry
Appendix A – Artifact 39	06/07/2012 16:27:16	Carry at restaurant to meet up with Tracy
Appendix A – Artifact 40	06/07/2012 16:27:50	Tracy replying to Carry about the meet up
Appendix A – Artifact 19	09/07/2012 18:18:47	Tracy thanks Carry for lunch Carry requesting help from Tracy to assist with sneaking in a tablet for a flash mob Mentions that they had discussed the event earlier and that Tracy will be compensated for helping
Appendix A – Artifact 20	10/07/2012 13:48:40	Tracy agrees to sneak in tablet and asks when Carry would like to have a look in the gallery
Appendix A – Artifact 22	11/07/2012 17:06:19	Confirmed meetup at 9 "Can i come in tomorrow, around 9?"
Appendix A – Artifact 47	11/07/2012 12:41:45	Carry advising Tracy she's almost at the National Gallery
Appendix A – Artifact 48	11/07/2012 12:49:08	Tracy replying to Carry advising to meet at the front so she can bring the tablet in

Plot Timeline

Date and Time	
21/06/2012 17:43:15	Tracy and Pat establish aliases and
03/07/2012 14:53:04	Tracy pitches idea to Pat to steal valuable stamps from the gallery
05/07/2012 15:51:31	Carry reaches out to Tracy to catch up
09/07/2012 14:44:11	Pat reaches out to King regarding a job to steal the stamps
06/07/2012 16:27:16	Tracy meets up with Carry
09/07/2012 14:44:11	Tracy emails Pat insurance document for the valuable stamps
09/07/2012 18:18:47	Carry requesting Tracy's assistance to sneak in the tablet for a flash mob
10/07/2012 13:48:40	Tracy accepting Carry's proposal
10/07/2012 15:24:57	King agrees to doing the heist
11/07/2012 12:49:08	Tracy meets up with Carry at the front door of Gallery to sneak in tablet

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy was involved both the theft of valuable stamps and the defacement of museum art.
- The theft of the valuable stamps was organised by Tracy and her brother Pat and involved a third party, King, who would be pulling off the heist
- Tracy and Pat were communicating under the aliases Coral and Perry, respectively
- Tracy was financially motivated to complete these tasks as she needed the money to pay for daughters schooling
- Tracy was involved in the defacement of museum art by assisting an acquaintance, Carry, sneak in a tablet past the museum security to be used by Carry.

Appendix A: Correspondence Evidence

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

#	Timestamp GMT +0000	Header Information	Key Information	Evidence Location
1.	16/06/2012 20:06:33	From: patsumtwelve@gmail.com To: 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.	Email
2.	19/06/2012 20:26:47	From: perrypatsum@yahoo.com To: tracysumtwelve@gmail.com Subject: Look me up sometime	Pat (Perry) emails Tracy to ask her to communicate using her alias.	Email
3.	19/06/2012 21:38:59	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Email
4.	19/06/2012 21:39:34	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: Re: ???	Pat (Perry) replies to Tracy (Coral) confirming that he was getting her emails.	Email
5.	21/06/2012 17:43:15	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com	Pat (Perry) replies to Tracy (Coral) on a email thread about Virtual Machine installation saying that she should listen to some other songs as well.	Email

		Subject: Re: Crazydave by the VMs	In the email thread Tracy (Coral) confirms that the instructions sent earlier in the audio file helped her.	
6.	28/06/2012 19:31:33	From: perrypatsum@yahoo.com To: 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.	Email
7.	29/06/2012 14:21:56	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: Re: Whats going on	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 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.	Email
8.	29/06/2012 14:31:36	From: perrypatsum@yahoo.com To: 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.	Email

9.	29/06/2012 15:21:35	From: perrypatsum@yahoo.com To: 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.	Email
10.	02/07/2012 16:13:18	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: Re: Some good news	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 a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	Email
11.	02/07/2012 20:00:31	From: perrypatsum@yahoo.com To: 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.	Email
12.	03/07/2012 13:29:37	From: joe.sum.twelve@gmail.com To: 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.	Email

13.	03/07/2012 14:53:04	From: 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.	Email
14.	05/07/2012 15:51:31	From: carriesum2012@yahoo.com To: 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.	Email
15.	06/07/2012 15:27:51	From: patsumtwelve@gmail.com To: 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.	Email
16.	06/07/2012 15:49:31	From: patsumtwelve@gmail.com To: throne1966@hotmail.com Cc:coralbluetwo@hotmail.com	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

		Subject: can't pass up		
17.	06/07/2012 17:59:24	From: patsumtwelve@gmail.com To: 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	Email
18.	09/07/2012 14:44:11	From: tracysumtwelve@gmail.com To: 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/Librar y/Mail/POP-coralbluetwo @hotmail.com @pop3.live.co m/INBOX.mbox/Messages/8 A3BD06F- CDB1-4453- 9C69- 77E06823F2A E.emlx
19.	09/07/2012 18:18:47	From: carriesum2012@yahoo.com To: 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.	Email
20.	10/07/2012 13:48:40	From: carriesum2012@yahoo.com To: 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.	Email

			Carry replies saying that this would be a big help and asks if she could come around 9 tomorrow.	
21	10/07/2012 15:24:57	From: patsumtwelve@gmail.com To: 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/Librar y/Mail/POP-coralbluetwo @hotmail.com @pop3.live.co m/INBOX.mbox/Messages/9 F0508B8- 04FB-490E- A7F0- 3E23B0E7C5 9B.emlx
22.	11/07/2012 17:06:19	From: carrysum2012@yahoo.com To: 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 Tracy not to worry and says "It will be gun".	Email
23.	11/07/2012 19:28:53	From: "Google+" <noreply-5dd47ca1@plus.google.com> To: 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.	Email

24.	11/07/2012 23:22:03	From: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> To: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+ informing Tracy that Carry had shared an album.	Email
25.	12/07/2012 16:12:07	From: "Carry Carsumtwotwelve (Google+)" <replyto-748d3d22@plus.google.com> To: tracysumtwelve@gmail.com Subject: Carry Carsumtwotwelve is sharing with you on Google+	Notification from Google+ informing Tracy that Carry had shared an album.	Email
26.	12/07/2012 18:03:51	From: carriesum2012@yahoo.com To: 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".	Email
27.	12/06/2012 21:25:04	From: Pat To: Tracy	Pat asks Tracy about her plans for the weekend	SMS
28.	13/06/2012 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. T	SMS
29.	13/06/2012 18:30:38	From: Tracy To: Pat	Tracy replies to Pats message saying that she has no big plans and enquires about his plans.	SMS

30.	13/06/2012 18:33:46	From: Tracy To: Terry	Ok, sounds good.	SMS
31.	03/07/2012 14:04:32	From: Terry To: 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.	05/07/2012 18:18:23	From: Carry To: Tracy	Carry sets up the time and location as 1pm at Bubba's grill for meeting with Tracy	SMS
33.	05/07/2012 18:20:26	From: Tracy To: Carry	Tracy confirms the meeting time and location	SMS
34.	06/07/2012 15:02:19	From: Tracy To: Pat	Tracy asks Pat to give her a call	SMS
35.	06/07/2012 15:08:37	From: Pat To: Tracy	Pat says he is busy and suggests calling later	SMS
36.	06/07/2012 15:11:54	From: Tracy To: Pat	Tracy says its important and insists that pat call her soon	SMS
37.	06/07/2012 15:13:31	From: Pat To: Tracy	Pat says he will call in 5 min	SMS
38.	06/07/2012 15:18:50	From: Pat To: Tracy	Pat calls Tracy and they speak for 4 min 4 secs.	SMS
39.	06/07/2012 16:27:16	From: Carry To: Tracy	Carry messages saying she has a table inside	SMS
40.	06/07/2012 16:27:50	From: Tracy To: Carry	Tracy replies back saying that she will be there.	SMS
41.	10/07/2012 15:26:19	From: Pat To: 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.	10/07/2012 15:58:04	From: Tracy To: Pat	Tracy acknowledges the email and message.	SMS


43.	10/07/2012 16:37:09	From: Tracy To: 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.	10/07/2012 17:18:38	From: Tracy To: Terry	Tracy messages Terry for Lunch	SMS
45.	10/07/2012 18:19:24	From: Tracy To: Terry	Tracy messages Terry that she is back at work.	SMS
46.	10/07/2012 18:58:24	From: Terry To: Tracy	Terry messages Tracy saying she is busy and suggests meeting up over the weekend if her dad isn't busy.	SMS
47.	11/07/2012 12:41:45	From: Carry To: Tracy	Carry messages Tracy informing that she is almost there (National Gallery)	SMS
48.	11/07/2012 12:49:08	From: Tracy To: Carry	Tracy replies to Carry asking her to meet out front. She says that she will take the tablet in.	SMS
49.	13/07/2012 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

Appendix B: WiFi and GPS Location Information

#	Timestamp	Header Information	Body	Map Screenshot
1	13/06/2012 19:01:22	GPS	38.87767624 -77.11546951	
2	13/06/2012 19:01:22	WIFI	38.88055896 -77.11553561	

3 13/06/2012 19:01:22 WIFI 38.87969988 -77.11591041

38.87969988 -77.11591041



38°52'46.9"N 77°06'57.3"W

38.879700, -77.115910

Directions

Save

Nearby

Send to your phone

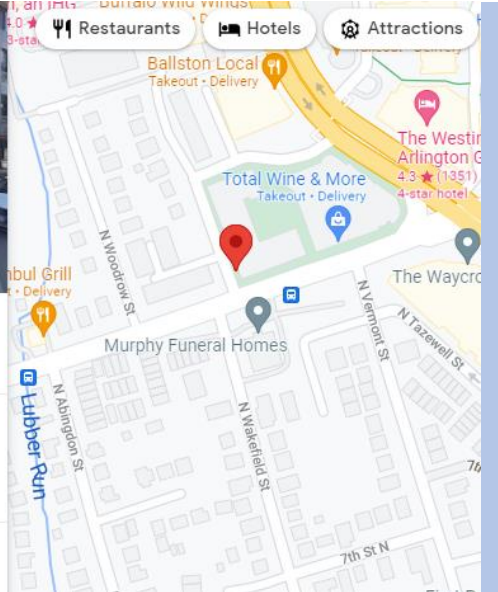
Share

801 N Wakefield St, Arlington, VA 22203, USA

Restaurants


Hotels

Attractions



4 13/06/2012 19:04:04 WIFI 38.88170194 -77.11397719

38.88170194 -77.11397719



38°52'54.1"N 77°06'50.3"W

38.881702, -77.113977

Directions

Save

Nearby

Send to your phone

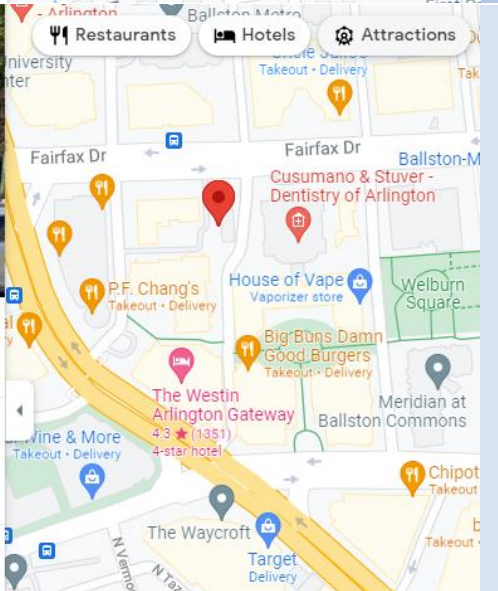
Share

4420 Fairfax Dr, Arlington, VA 22203, USA

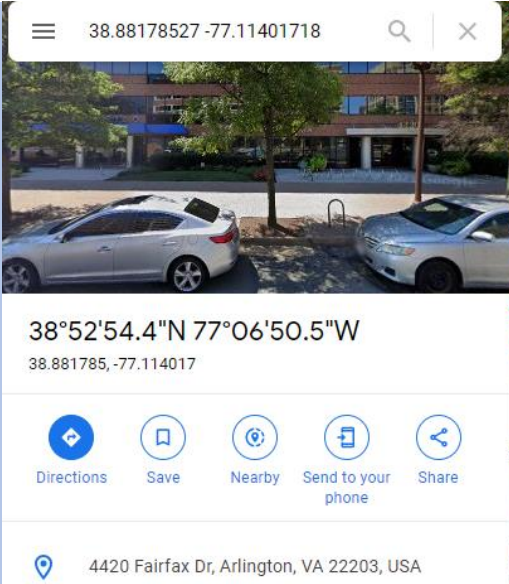
Restaurants

Hotels

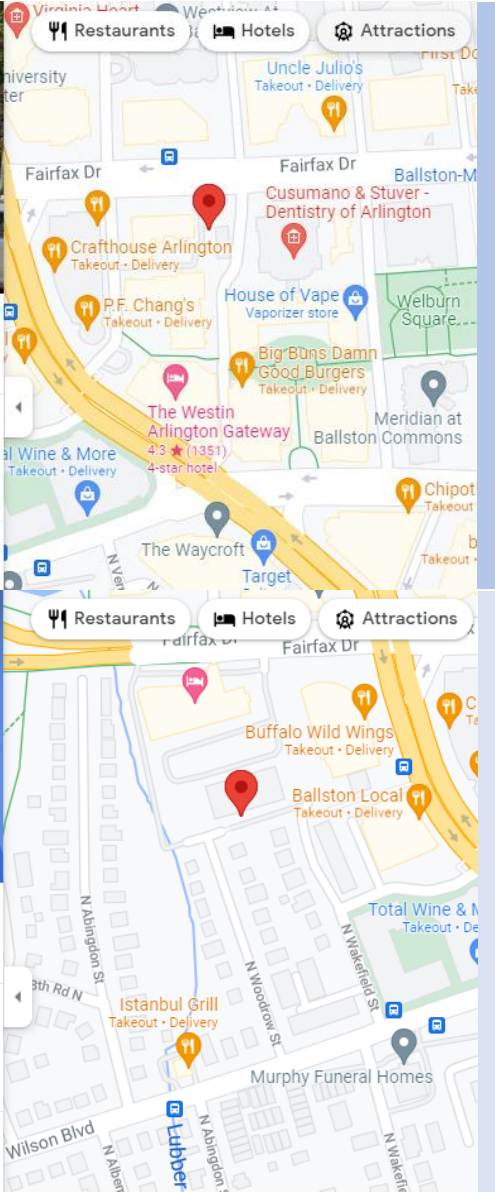
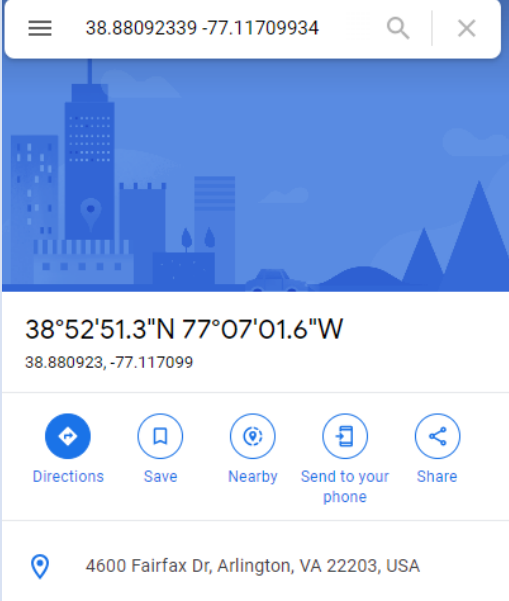
Attractions



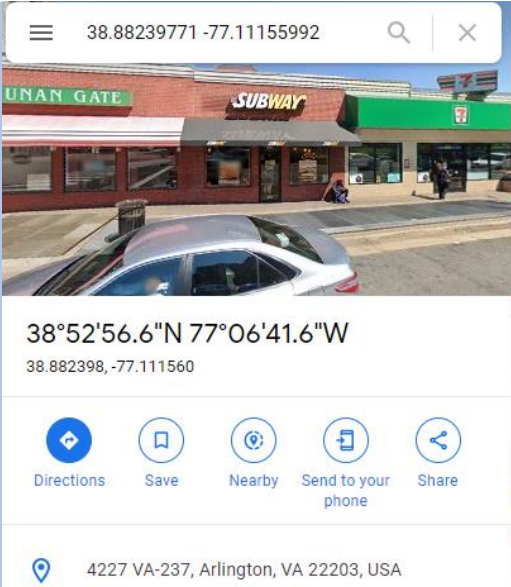
5 13/06/2012 19:04:04 WIFI 38.88178527 -77.11401718



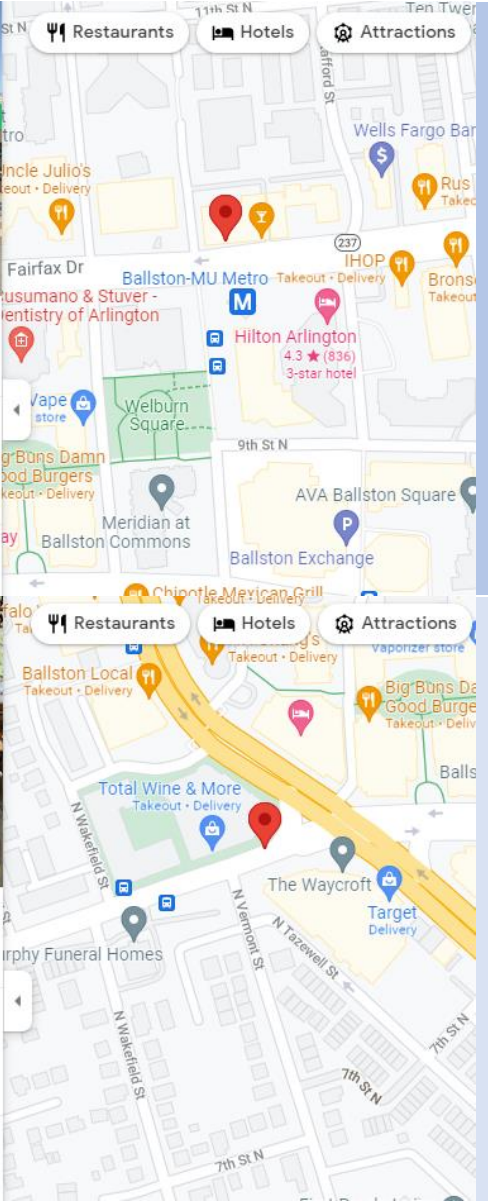
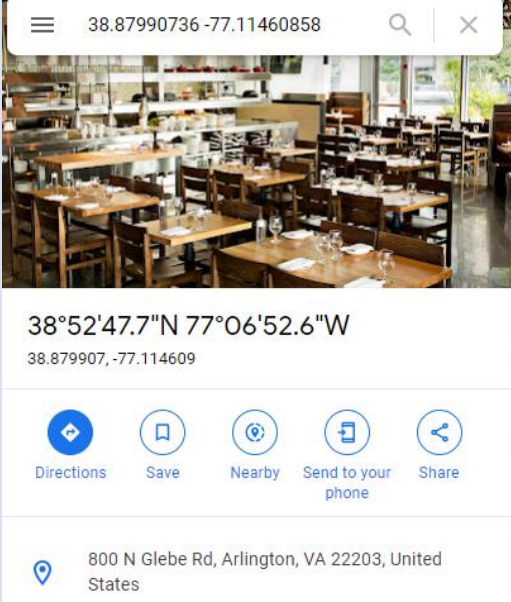
6 02/07/2012 16:19:23 GPS 38.88092339 -77.11709934



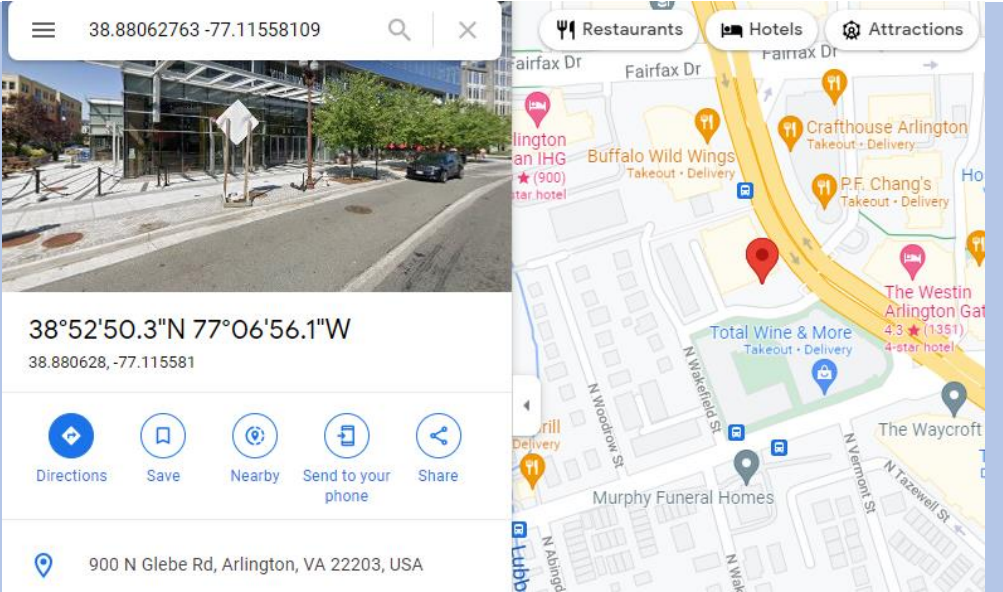
7 02/07/2012 16:19:23 GPS 38.88239771 -77.11155992



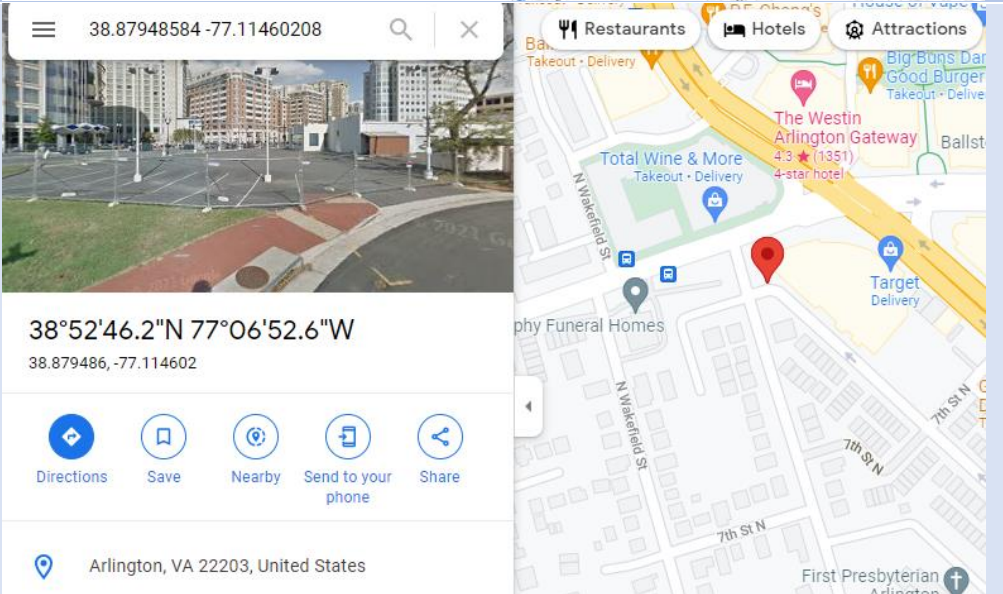
8 02/07/2012 16:19:25 WIFI 38.87990736 -77.11460858



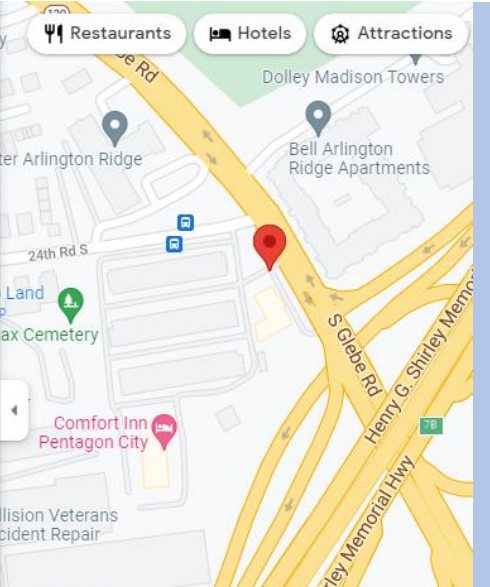
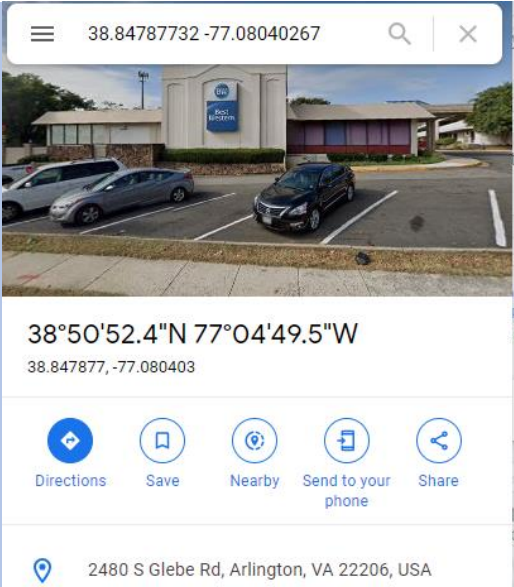
9 03/07/2012 13:42:43 WIFI 38.88062763 -77.11558109



10 05/07/2012 16:32:46 GPS 38.87948584 -77.11460208



13 10/07/2012 16:31:13 WIFI 38.84787732 -77.08040267



14 10/07/2012 16:45:00 GPS 38.90048003 -76.99235898

