

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.

Equipment and Tools

Using the Autopsy tool, evidence was gathered from Tracy's iPhone logs. Revealing those in question, along with times and locations. Other tools used:

- Kali Linux
- Google Maps
- SqliteBrowser

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone1, 2	VOL5/logs/apple support/general.log
Host Name	Tracy Sumtwelve's iPhone	VOL5/logs/lockdownd.log.1
OS Version	OS 4.2.1	VOL5/logs/apple support/general.log
Install Time	12:03 - 7:00	VOL5/logs/apple support/general.log
User Email	tracy.sumtwelve@gmail.com coralbluetwo@hotmail.com	VOL5/mail
Phone #	(703) 340-9661	VOL5/logs/mobile/Library/SMS/sms.db
Serial Number	8600482Y7H	VOL5/logs/apple support/general.log
ICCID	89014103255195342366	VOL5/logs/lockdownd.log.1
IMEI	012021003735398	VOL5/root/library/activation_records
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6 577ccb534ca0d1e83ffd27683e621607	

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
Email:	patsumtwelve@gmail.com
Alias:	perrypatsum@yahoo.com
Relationship:	Tracy's brother, the corrupted police officer.
Terry: Phone Number:	(703) 829-6071
Relationship:	Daughter of Tracy and Joe.
Joe: Email:	joe.sum.twelve@gmail.com
Relationship:	Tracy's ex-husband.
Carry: Phone Number:	(202) 725-2124
Email:	carrysum2012@yahoo.com
Relationship:	Acquaintance of Tracy, mastermind behind the "flash mob".

The above information was retrieved from the 'logs' and 'root' files of Tracy's iphone. Indicating communication with those above, along with details of the confiscated device.

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.

Within the email logs, Tracy (Coral) informed Pat (Perry) about the "buzz" going around the office about a new foreign exhibit they were getting that seemed like a big deal (Appendix A, Artifact 9). Pat seemed ecstatic with this information and replied "Hopefully this turns out to be our lucky break" (Appendix A, Artifact 10). The next day, Tracy did some digging and informed

Pat about the amount of money that was getting thrown into this exhibit, but couldn't find anything concrete and told him she'd continue looking (Appendix A, Artifact 11). A couple days later, Tracy found that the new exhibit contained highly valuable stamp collections and mentioned, "This could be our ticket" to Pat (Appendix A, Artifact 15). Pat seemed very pleased with this information as he replied, "That may just be exactly what we need. Try to collect as much information... the better. In the meantime, I will try to look into our options for actually pulling something like this off" (Appendix A, Artifact 16). Pat then reached out to an ex-con named King to help fulfill the heist, while also blackmailing him with his violation of parole for doing drugs, if he chose not to comply (Appendix A, Artifact 24). King seemingly agreed and requested a few items he'd need to pull it off. He asked for a rope, javelin, tactical turtle necks, spray paint, vibram five finger shoes, pack of smokes, and smoke grenades (Appendix A, Artifact 32). Pat forwards this email to Tracy (Appendix A, Artifact 33), and also sends her a text telling her that her friend Coral received an email that needed editing. Tracy replies, "Sure thing, I'll get on it" (Appendix A, Artifact 34).

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.

As Tracy posted about her financial problems, Carry, an old friend of Tracy, reached out and invited her to lunch (Appendix A, Artifact 18). After their lunch, Tracy thanks Carry for inviting her out, and mentions how they should get together more often (Appendix A, Artifact 20). Shortly after their initial get together, they seemed to meet up a few times for lunch (Appendix A, Artifact 26 & 27). On July 9th, Carry asks Tracy if she's able to get her tablet into the Gallery for her flash mob event that she told her about. She also mentions how she knows the security can be too "keen", and how she can "make it worth her while" by getting lunch or something else for her help (Appendix A, Artifact 28). Tracy agrees to help get her tablet into the Gallery and asks her what time she'd like to come in and take a look around (Appendix A, Artifact 29). Carry seemed appreciative and asked to come the next day at 9 (Appendix A, Artifact 30). The following day, Carry emails Tracy expressing how she wants to make the process as "painless as possible" since the security guards can be a bit much. She continues to ask Tracy for the shift changes that way Tracy doesn't have to know when she's going to do it. She also tells her that she has a good budget for the event if Tracy would like to get compensated for the info (Appendix A, Artifact 31). Tracy responds the next day and tells Carry that she will send it as long as nobody else sees. She asks her to be very careful as she could get in a lot of trouble, but will still help her because she could use the extra cash (Appendix A, Artifact 37). Carry responds and tells her to not worry so much and that it'll be fun (Appendix A, Artifact 38).

Plot Timeline

- **June 28, 2012** - Tracy and Pat agree to only use their alias' and new emails for communication. He also mentions how money is "rough" for the both of them and how they should bounce ideas back and forth (Appendix A, Artifact 4).
- **July 3, 2012** - Tracy emails Pat informing him of a new exhibit at the National Gallery where there will be valuable stamps (Appendix A, Artifact 15).
- **July 5, 2012** - Carry emails Tracy about her recent post on having a hard time financially and asks her for lunch (Appendix A, Artifact 18).
- **July 6, 2012** - Pat emails a man named King and cc's Tracy, with a proposition for King to help assist with the heist (Appendix A, Artifact 24).
- **July 6, 2012** - Carry and Tracy meet for lunch for a second time (Appendix A, Artifact 27).
- **July 9, 2012** - Carry asks Tracy to help get her tablet into the National Gallery for her flashmob event (Appendix A, Artifact 28).
- **July 10, 2012** - Carry asks for the shift changes of the National Gallery and offers Tracy compensation for the info (Appendix A, Artifact 31)
- **July 10, 2012** - King replies agreeing to help and attaches a list of items he'll need to complete the heist (Appendix A, Artifact 32).
- **July 11, 2012** - Tracy asks Carry how the flash mob is going via sms (Appendix A, Artifact 36).
- **July 11, 2012** - Tracy sends Carry the shift change info (Appendix A, Artifact 37).

Conclusion

Evidence found on Tracy's iPhone indicated the following:

Tracy's confiscated evidence led to agreement and coherence in seeking opportunities to steal stamps from the National Gallery. Email and sms logs reveal Tracy going through financial hardships and in need of quick money to pay for her daughter's tuition. Email logs also reveal Tracy using an alias (Coral) while communicating with her brother Pat (Perry), who is also dealing with financial hardships and seeking avenues to find fast money. Emails between the two affirm Pat coinciding with Tracy to find opportunities for the heist. SMS logs also show communication with a person named Carry, who Tracy had been meeting with. Carry initially reached out due to a post Tracy made about her financial hardships and asked her to meet up for lunch. Going further into the investigation, it's safe to believe Carry reached out for her own agenda to conduct a potential "flash mob" at the National Gallery and needed Tracy's help. In the email logs between the two, Carry asked for security shifts, along with help to sneak a tablet into the Gallery. She informed Tracy that she would be fully compensated for her help. Although

Tracy agreed to help Carry, she seemed apprehensive as she expressed her concerns to be very careful and fearful of getting caught.

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.	June 13, 2012 5:30pm	Text thread between Terry and Tracy.	Terry: "I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook." Tracy: "Okay sounds good."	SMS
2.	June 19, 2012 2:39pm	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com	"Are you getting my emails? I've sent you two already. I thought to hear back from you by now..."	Protected Index
3.	June 19, 2012 5:02pm	To: coralbluetwo@hotmail.com From: perrypatsum@yahoo.com	"They are just now trickling in."	Protected Index

4.	June 28, 2012 12:31pm	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com	<p>“Great, now that we have everything set up it would be better to do most of our communication on here on your new email. This might keep us a little bit safer. I know money is rough for both of us, so we may have to push the envelope a bit. A few friends from around the office are really good about these types of things, If I find out anything interesting I will shoot you an email. In the meantime let’s try to shoot some ideas back and forth.</p> <p>Your friend, Perry”</p>	Protected Index
5.	June 28, 2012	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com	<p>“I know what you mean. If anything comes up around the office that we can maybe... get in on, please lets try to do so. Kiddo is getting really bent out of shape about possibly having to switch schools. I have been paying some more attention to the memos and papers that come across my desk. We get a bunch of insurance type documents that place values on certain objects. If anything stands out, I’ll let you know.</p> <p>Coral”</p>	Protected Index
6.	June 28, 2012 4:16pm	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com	<p>“Okay, we will work something out. I just need to be careful. IA has been sniffing around the office. Makes me nervous but I am sure we can still something happen.</p> <p>Perry”</p>	Protected Index
7.	June 29, 2012 7:31am	From: patsumtwelve@gmail.com To: tracysumtwelve@gmail.com	<p>“Hey sis, How have things been working at home? Did Terry sort out those problems she was having in</p>	Protected Index

			<p>her literature class? I'm sorry I haven't been able to check in with you guys more often... I have been busy trying to sort some things with your friend Coral. We should all go out for dinner as friends some time! Check in with her.</p> <p>Pat “</p>	
8.	July 2, 2012 4:06pm	<p>From: tracysumtwelve@gmail.com To: joe.sum.twelve@gmail.com</p>	<p>“Joe, Sorry to bother you, but I have a serious question about Terry and her school. Her tuition is getting a bit too much for me right now and I could use a little help. I hate to impose on you for this, but is there any way you would be willing to help me out with her tuition this year? Please get back to me, Tracy “</p>	Protected Index
9.	July 2, 2012 12:05pm	<p>From: coralbluetwo@gmail.com To: perrypatsum@yahoo.com</p>	<p>“Perry, I think I may have come across something interesting. Everybody around the office seems to be buzzed about a foreign exhibit that is supposed to be coming over. There hasn't been any official release in writing but we have been through quite an ordeal with all this paperwork. From what I can tell, this exhibit has to be a big deal. I'll let you know if I found out anything else. Coral”</p>	Protected Index
10.	July 2, 2012	<p>From: perrypatsum@yahoo.com To: coralbluetwo@gmail.com</p>	<p>“Awesome. Hopefully this turns out to be our lucky break.”</p>	Protected Index
11.	July 2, 2012	<p>From: coralbluetwo@gmail.com To: perrypatsum@yahoo.com</p>	<p>“Okay, so there has been a lot of money being thrown around to get this exhibit over to us. I've been swimming through paperwork and memos all day, but none of it seems to have any solid information that could help us. I had to scan and</p>	Protected Index

			verify some shipping information, and compared to what it usually costs to ship exhibits.. this ones seems relatively cheap. I'm not sure if this is good or bad for us (or even an error) but hopefully I will be able to find out more later in the week."	
12.	July 2, 2012	From: perrypatsum@yahoo.com To: coralbluetwo@gmail.com	"That is weird. Hopefully it just means that it is something small, and that could be a very good thing for us. "	Protected Index
13.	July 3, 2012 6:29am	From: joe.sum.twelve@gmail.com To: tracysumtwelve@gmail.com	"Sorry Tracy. I'm not going to be paying for Terry's school if shes not living with me. I hope things take an upturn for you. Joe"	Protected Index
14.	July 3, 2012 9:34am	From: tracysumtwelve@gmail.com To: patsumtwelve@gmail.com	"I just talked to Coral, she sounded ecstatic. She mentioned she just got some great news about her job. You should catch up with her. Tracy"	Protected Index
15.	July 3, 2012	From: coralbluetwo@gmail.com To: perrypatsum@yahoo.com	"I was told that we are supposed to be receiving a rare collection of stamps. That would explain why the shipping information looked a bit out of the ordinary to me. I'm not certain of the specifics for the stamps, but they seem to be very highly valued by somebody. Maybe this is our ticket."	Protected Index
16.	July 3, 2012, 12:32pm	From: perrypatsum@yahoo.com To: coralbluetwo@gmail.com	"That may just be exactly what we need. Try to collect as much information... the better. In the meantime, I will try to look into our options for actually pulling something like this off."	Protected Index
17.	July 3, 2012	Text thread between Terry and Tracy.	Tracy: "Hey honey. I'm not sure if we can afford Prufrock anymore... What	SMS

	1:41pm		<p>do you think about maybe switching to someplace else?"</p> <p>Terry: "moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools"</p>	
18.	July 5, 2012 11:51am	<p>From: carrysum2012@yahoo.com To: tracysumtwelve@gmail.com</p>	<p>"I saw on facebook that you were having a hard time lately, and I realized that we haven't spoken face to face in quite a while. I was really hoping that we could get together and have lunch. Does this Friday sound good? Let me know."</p>	INBOX.mbox
19.	July 5, 2012 6:18pm	Text thread between Carry and Tracy.	<p>Tracy: "Sounds good let's shoot for one at Bubba's grill"</p> <p>Carry: "Okay that sounds great. See you there"</p>	SMS
20.	July 6, 2012 10:55am	<p>From: tracysumtwelve@gmail.com To: carrysum2012@yahoo.com</p>	<p>"Hey Carry, Just wanted to say thanks for lunch. I had a great time and it was good catching up with you. We should do lunch more often."</p>	INBOX.mbox
21.	July 6, 2012 11:27am	<p>From: patsumtwelve@gmail.com To: tracysumtwelve@gmail.com</p>	<p>"hey sis i know a guy...he's known as king"</p>	Protected Index
22.	July 6, 2012 11:42am	<p>From: tracysumtwelve@gmail.com To: patsumtwelve@gmail.com</p>	<p>"Oh cool, we should hang out sometime."</p>	Protected Index
23.	July 6, 2012	<p>From: perrypatsum@yahoo.com To: coralbluetwo@gmail.com</p>	<p>"Hey sis here is the login info for the other account we talked about - AGAIN coralblue@hotmail.com"</p>	Protected Index
24.	July 6, 2012 11:49am	<p>Subject: can't pass up From: patsumtwelve@gmail.com to : throne966@hotmail.com CC: coralbluetwo@hotmail.com</p>	<p>"King, Long time no see...I have a juicy proposition for you. Two weeks from now, me and my associates are planning a</p>	INBOX.mbox

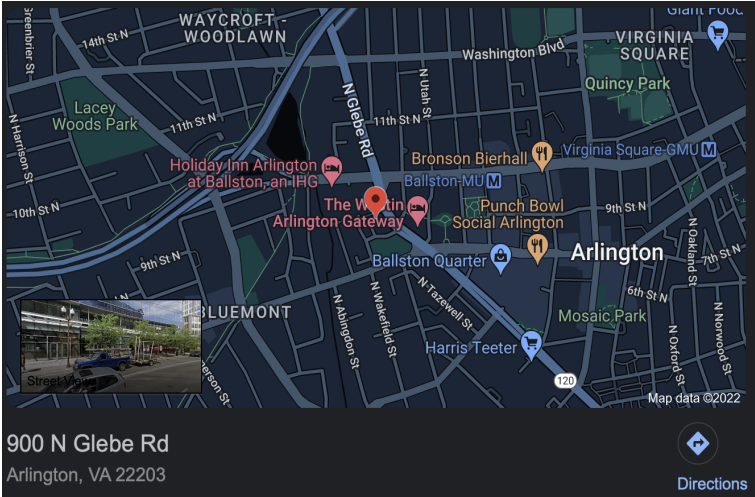
			<p>heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole officer go years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, i feel he wouldn't be too happy. It's 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't need a search warrant. Well hit me up. You know where to find me"</p>	
25.	July 6, 2012 3:02pm	Text thread between Pat and Tracy.	<p>Tracy: "Hey can you give me a call"</p> <p>Pat: "Sis I'm really busy can we can do this later"</p> <p>Tracy: "No pat this is important I need you to call me soon"</p> <p>Pat: "Ok ok I'll call in 5"</p>	SMS
26.	July 6, 2012 3:18pm	Phone call between Pat and Tracy.	Duration 2 min 44 sec.	Call History
27.	July 6, 2012 4:27pm	Text thread between Carry and Tracy.	<p>Carry: "I have a table inside"</p> <p>Tracy: "Okay brt"</p>	SMS
28.	July 9, 2012 2:18pm	<p>From: carrysum2012@yahoo.com</p> <p>To: tracysumtwelve@gmail.com</p>	"if there was any way you could help me get my tablet into the gallery. I know security isn't too keen on computers and the like in the gallery, but maybe you could pull some strings and get it in for me? I can make it worth your while :) But really I would happy to get lunch again or	INBOX.mbox

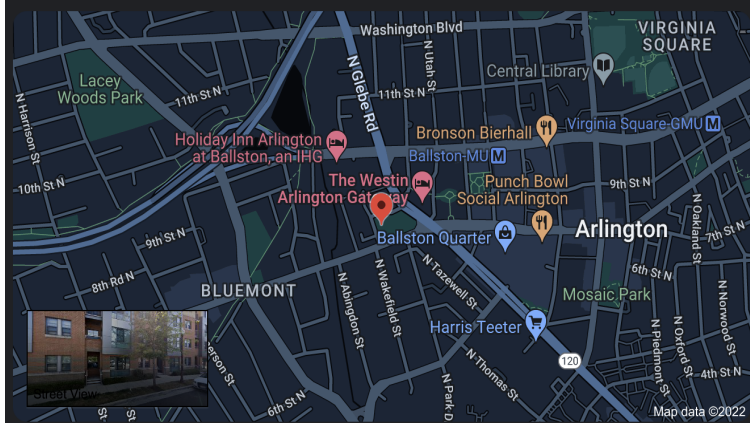
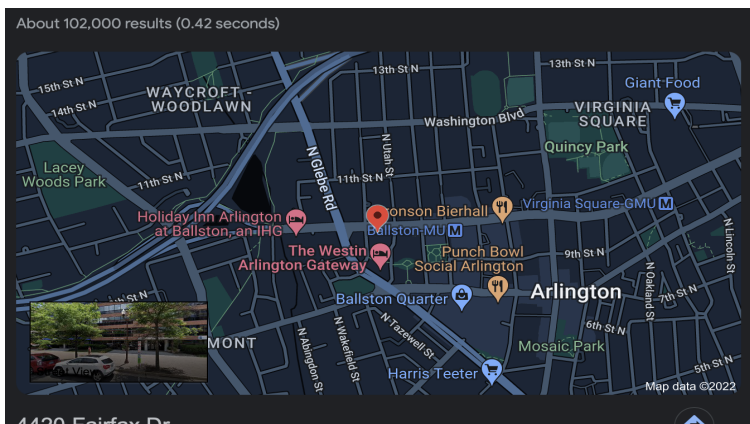
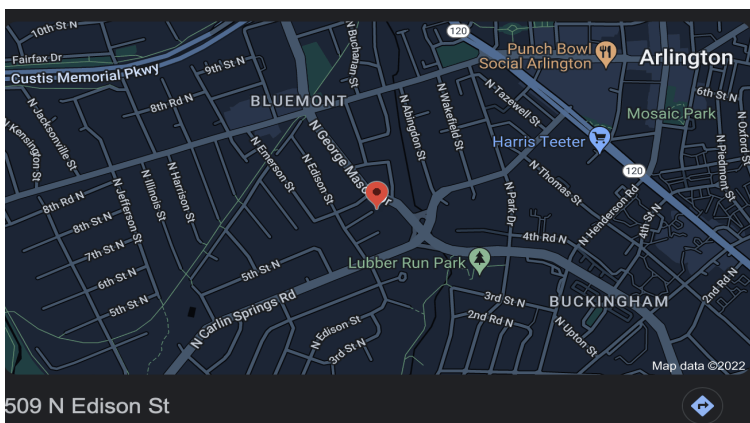
			something else for your help. I want to get some pictures for my flash mob event I told you about. Let me know."	
29.	July 10, 2012 6:29am	From: tracysumtwelve@gmail.com To: carrysum2012@yahoo.com	"I can definitely help get your tablet in. Our security guards can be pretty ridiculous sometimes! When would you want to get in and take a look around? Tracy"	INBOX.mbox
30.	July 10, 2012 6:48am	From: carrysum2012@yahoo.com To: tracysumtwelve@gmail.com	"Awesome this will be a big help. Can i come in tomorrow, around 9?"	INBOX.mbox
31.	July 10, 2012 8:15am	From: carrysum2012@yahoo.com To: tracysumtwelve@gmail.com	"Hey so i'm putting together this event we talked about and i want to make it as painless as possible. I know that your security folk sometimes get a little out of sorts. Is there a good time or maybe you could just let me know the shift changes so you don't have to know when i am going to do this. I have a pretty good budget for the event if you would like a little something for the info"	INBOX.mbox
32.	July 10th, 2012 11:19am	Subject: can't pass up From: throne966@hotmail.com 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: -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	INBOX.mbox

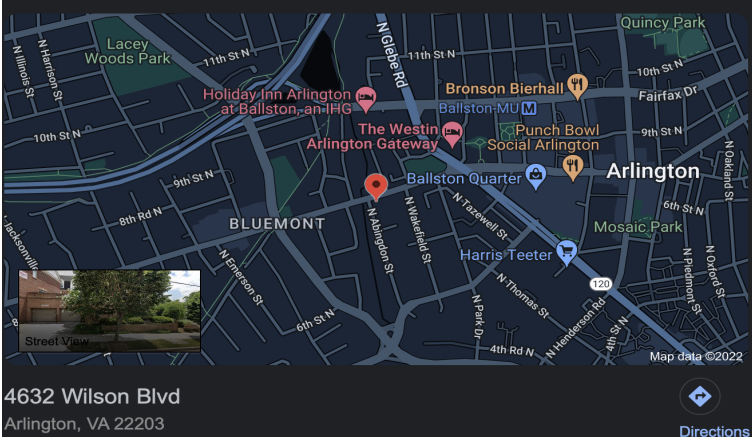
			walk silently) -pack of smokes (detecting lasers) -smoke grenades (use as a means of escape if caught)	
33.	July 10, 2012 11:24am	Subject: FWD: can't pass up From: patsumtwelve@gmail.com To: coralbluetwo@hotmail.com	"This is what we need to get for the guy that's going to make our job happen"	INBOX.mbox needs.txt
34.	July 10, 2012 3:26pm	Text thread between Pat and Tracy.	Pat: 'hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know' Tracy: "Sure thing I'll get on it"	SMS
35.	July 10, 2012 5:18pm	Text thread between Terry and Tracy.	Tracy: "Going to lunch. You want to go????" Tracy: "Back at work" - 6:19pm Terry: "I'm busy. Maybe this weekend if dad isn't busy" -6:58pm	SMS
36.	July 11, 2012 12:41pm	Text thread between Carry and Tracy.	"I'm almost there where should I meet you?" "Just meet me out front, I'll take the tablet in" "How's the flashmob going"	SMS
37.	July 11, 2012 2:53pm	To: tracysumtwelve@gmail.com From: carrysum2012@yahoo.com	"Okay carrie I'm going to send this but you need to make sure no one else sees it okay I could get in a bunch of trouble. I want to help you and I could really use some extra cash too but please please be careful."	INBOX.mbox
38.	July 11, 2012	To: tracysumtwelve@gmail.com From: carrysum2012@yahoo.com	"Don't. Worry so much. It will be gun Tracy"	INBOX.mbox
39.		From: perrypatsum@yahoo.com	"Tracy,	INBOX.mbox

		To: tracysumtwelve@gmail.com	Talked to your brother about an email. You should have your friend, Alias, send me an email. Thanks Perry."	
40.	July 13, 2012 1:02am	Text thread between Terry and Tracy.	Terry: "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.	361306882.473715	WiFi Location - Virginia Tech Center	38.88055896 -77.11553561	

2.	361306882 .473715	WiFi Location - Apartment Building	38.88005346 -77.11595332	 <p>801 N Wakefield St Arlington, VA 22203</p> <p>Directions</p>
3.	361306882 .473715	WiFi Location - Physical Therapy	38.88154673 -77.11469429	<p>About 102,000 results (0.42 seconds)</p>  <p>4420 Fairfax Dr Arlington, VA 22203</p> <p>Directions</p>
4.		Cell Location - House	38.87493735 -77.11815351	 <p>509 N Edison St Arlington, VA 22203</p> <p>Directions</p>

5.		Cell Location - House	38.87869298 -77.11703056	 <p>4632 Wilson Blvd Arlington, VA 22203</p>
6.				