



Cybersecurity

21.3 The Final Report

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.

Digittech uncovered evidence suggesting that Tracy and her brother Pat, along with their accomplices Carry and an associate named King, colluded to plan a heist at the National Gallery, D.C. The investigation revealed that Tracy used the alias Coral and corresponded using the email address 'coralbluetwo@hotmail.com', while Pat utilized the alias Perry and communicated through the email address 'perrypatsum@yahoo.com'. Our investigation also revealed that Tracy's participation in the heist was driven by financial motives, as evidenced by emails to her friend, Carry and ex-husband, Joe and through text messages to her daughter Terry and ex-husband Joe.

The Digitech team also found proof that Tracy was financially motivated by her friend Carry, to engage in the heist. Evidence indicated Carry's solicitations for Tracy to smuggle her tablet into the art gallery and share security-related information, both of which Tracy willingly complied with. Further investigation showed Tracy's brother engaging in blackmail against an associate, King, coercing him into participating in the heist. King communicated via the email address 'throne1966@hotmail.com', and he agreed to partake in the criminal endeavor, furnishing a list of required items in a text file labeled 'needs.txt', with Tracy being included in the email correspondence between Pat and King.

Equipment and Tools

The following equipment and tools were used to gather and analyze the evidence applicable to Tracy's iPhone investigation:

- Autopsy - used to analyze the directories - /mobile, /Applications, /Library, /root, /Logs and /logs
- SQLite DB Browser - used to analyze the exported directories offline (vol5/logs, call_history.db and INBOX.mbox)

- Kali Linux machine
- Google maps
- Epoch Unix Timestamp

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone1, 2	vol5/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelves iPhone	vol5/logs/lockdownd.log
OS Version	iPhone OS 4.2.1 (8C148)	vol5/logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	vol5/logs/AppleSupport/general.log
User Email	IMAP: tracysumtwelve@gmail.com POP: coralbluetwo@hotmail.com	vol5/mobile/Library/Mail/Envelope Index
Phone Number	1 (703) 340-9661	vol5/logs/lockdownd.log
Serial Number	86004482Y7H	vol5/logs/AppleSupport/general.log
ICCID	89014103225195342366	vol5/logs/lockdownd.log

IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	tracy-phone-2023-09-02.final.E01
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	tracy-phone-2023-09-02.final.E01

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, coralbluetwo@hotmail.com
 Work Email: tracy.sumtwelve@nationalgallerydc.org
 Relationship: Accused

Pat (Perry):

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

Terry:

Phone Number: (703) 829-6071
 Email:
 Relationship: Tracy's daughter

Joe:

Phone Number:
 Email: joe.sum.twelve@gmail.com
 Relationship: Tracy's ex-husband

Carry:

Phone Number: (202) 725-2124
Email: carrysum2012@yahoo.com
Relationship: Tracy's accomplice and friend

King:

Phone Number:
Email: throne1966@hotmail.com
Relationship: Pat's associate

The above information was gathered through careful examination of text and email correspondences. Through an analysis of various text messages and emails, it was verified that Pat (alias Perry) is Tracy's brother, as he referred to her as 'sis' both by emails and text messages.

Terry's relationship as Tracy's daughter was substantiated through a number of text exchanges discussing dinner, changing schools, and Terry's desire to live with her father. Correspondence between Tracy and her brother Pat, discussing Terry's well-being and literature class, further supported their familial connection.

Joe's association with Tracy was established by tracing the email address mentioned above, uncovering various email discussions about their daughter, Terry. Tracy sought financial assistance for Terry's tuition, and Joe agreed to contribute only if Terry resided with him.

A review of email exchanges between Tracy and Carry, discussing a lunch date and catching up, was also conducted. These messages included discussions about Tracy's assistance with taking a tablet into the gallery, while Carry also inquired about a shift change and security at the gallery.

King was introduced to Tracy by her brother Pat, who included her in an email to King, blackmailing him to collaborate or King's parole officer would be contacted and informed about his illegal activities. King agreed and provided a list of required items for the job. Pat then forwarded this email to Tracy.

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.

Findings on Tracy's iPhone provide evidence to support this. This includes: e-mail correspondence, SMS messages, photographs and other information that attest to collusion between Terry, Pat and King in the theft of high-value stamps from the NGDC, as shown in Appendix A. The investigation also reveals Terry's willingness to divulge sensitive information in support of the "flash mob", orchestrated for the purpose of damaging NGDC artwork, also shown in Appendix A.

The e-mail correspondence exposes Tracy and Pat's use of pseudonyms. Tracy called herself 'Coral', while Pat adopted the name 'Perry'.

Furthermore, it appears that Tracy was facing financial difficulties, as evidenced by her SMS messages and a personal note on her phone, explaining her difficulties in paying the school fees for her daughter, Terry, at Prufrock, as shown in Appendix A below.

The investigation clearly shows that Pat submitted to King, a proposition to join the heist to take place at the National Gallery, DC. It's obvious that Tracy knew about this proposition sent to King, since Pat copied her on it. The e-mail correspondence reveals that King accepted Pat's proposal to go and steal from the national gallery and sent Pat the list of tools needed for the theft.

Below, we have outlined further evidence relating to the theft of valuable stamps. This includes: the tools needed for the theft, memos on stamp insurance, and photos of the stamps. These reveal the ins and outs of the meticulous planning of the NGDC stamps heist. The exposure of the deterioration of the works of art at the NGDC is a direct result of the revelation of the theft.

```
-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)
```

FIGURE 1 - needs.txt email attachment

Figure 1 above shows photo evidence of an email sent from 'King kthings' at throne1966@hotmail.com with an attachment labeled 'needs.txt' listing the items required for the heist.

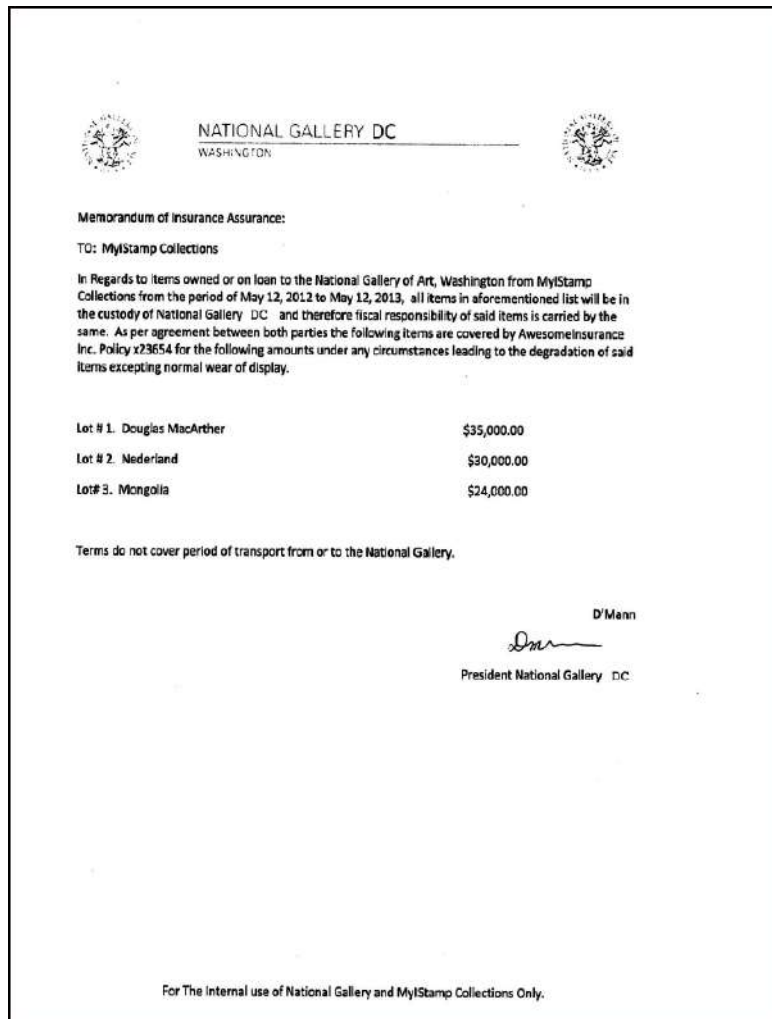


FIGURE 2 - Stamp_insurance3.pdf email attachment



FIGURE 3 - Stamps mentioned in figure 2 above

Figures 2 and 3 above show photo evidence of insurance documents and the corresponding stamps insured.

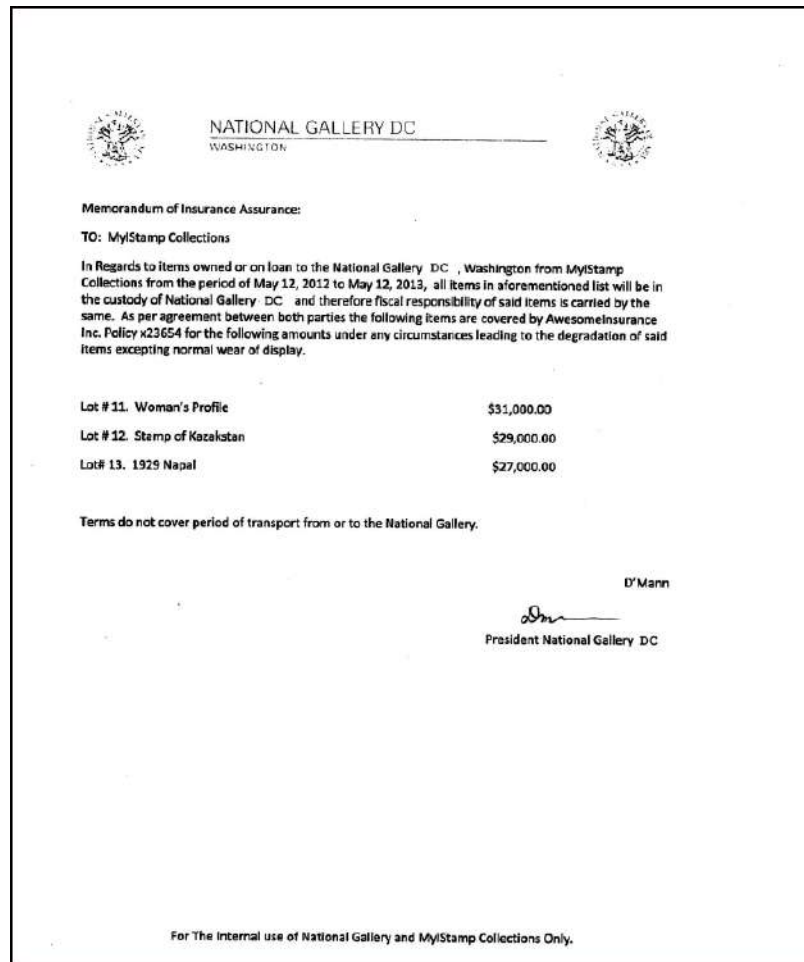


FIGURE 4 - Stamp_insurance2.pdf email attachment



FIGURE 5 - Stamps mentioned in figure 4 above

Figures 4 and 5 above show photo evidence of insurance documents and the corresponding stamps insured.

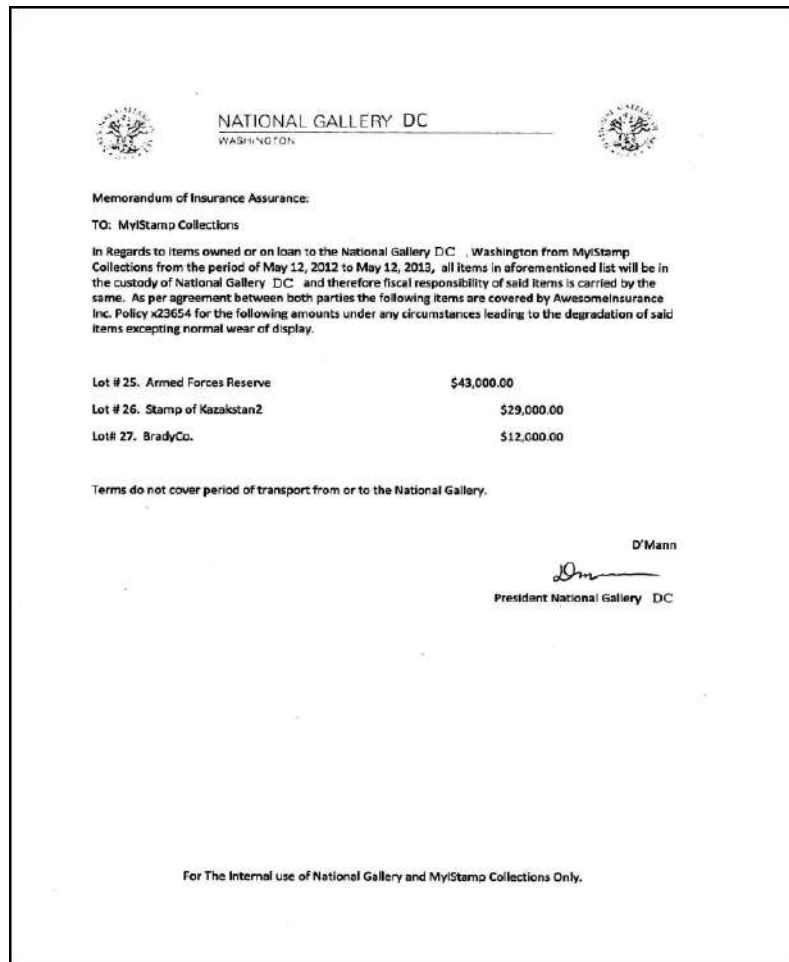


FIGURE 6 - Stamp_insurance1.pdf email attachment



FIGURE 7 - Stamps mentioned in figure 6 above

Figures 6 and 7 above show photo evidence of insurance documents and the corresponding stamps insured.

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.

There was no evidence related to vandalism of museum art in the iphone image, only evidence related to the theft of stamps.

Plot Timeline

- On Tuesday, June 19, 2012 at 02:38 PM, Pat sent an email to Tracy with an MP3 audio recording attachment (Crazydave1.mp3) that contained voice instructions on how to install a VirtualBox VM.
- On July 5, 2012 06:18:23 PM, Tracy and Carry spoke about meeting for lunch at Bubba's Grill.
- On Friday, July 6, 2012, at 11:49:31 AM, Pat sent an email to King at 'throne1966@hotmail.com' with the subject 'can't pass up'. In the email, Pat coerced King into joining the team planning to perform the heist at the National Gallery. Pat's sister, Tracy, was also copied on the email.
- On Friday, July 6, 2012 at 04:27:16 PM, Tracy and Carry confirmed the lunch meeting at Bubba's Grill via SMS.
- On Saturday, July 7 2012 at 07:36:35 PM, Tracy received an SMS from an unknown number advising that she had received a Target Gift Card valued at \$1000.
- On Monday, July 9, 2012 at 10:44:11 AM, Tracy sent an email to herself with the valuable stamps she had in mind to steal. This email also had the amount the stamps were insured for.
- On Monday, Jul 9, 2012 at 10:44:11 AM, King, who had agreed to take part in the theft at the gallery, sent an email to Pat with an attachment 'needs.txt', which outlined all the required tools to perform the heist.
- On Tuesday, July 10, 2012 at 11:24 AM, Pat forwarded the email from King with the attachment 'needs.txt' to his sister, Tracy.
- On Wednesday, July 11, 2012 at 12:49:08 PM, Carry and Tracy made arrangements via SMS for Tracy to smuggle Carry's tablet into the gallery.
- On Thursday, July 12, 2012 at 05:06:45 PM, Tracy sent a text message to Carry inquiring how the flashmob was going.

Persons of interest are shown in figure 8 below:

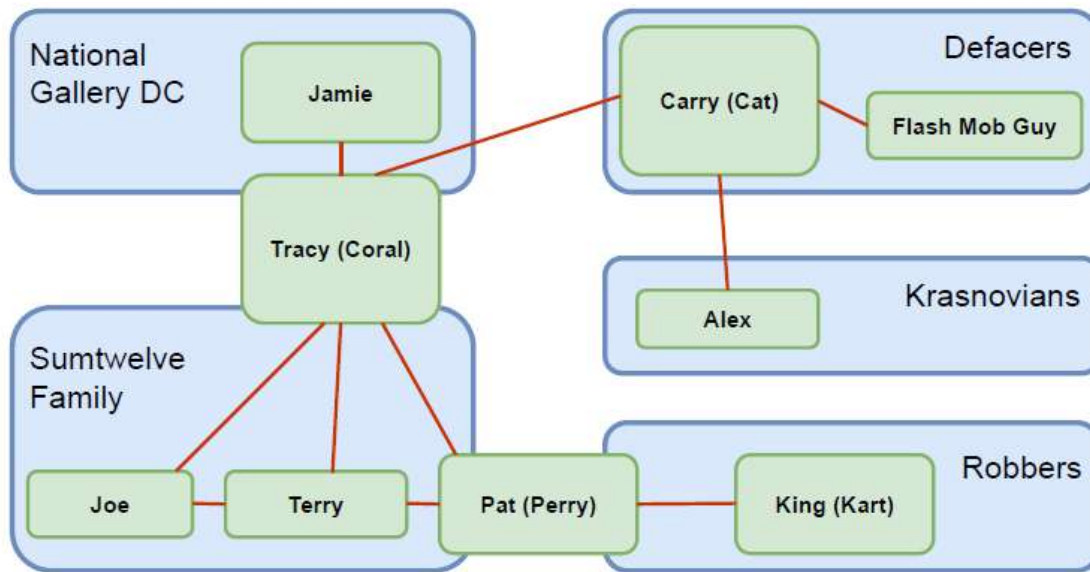


FIGURE 8 - Possible connections to the heist

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy and Pat conspired with each other - Pat used the alias 'Perry' and communicated via patsumtwelve@gmail.com and his temporary email address perrypatsum@yahoo.com. Tracy used the alias 'Coral' and communicated via her temporary email address coralbluetwo@hotmail.com, as well as her regular email address tracysumtwelve@gmail.com in some instances.
- Pat colluded with King, blackmailing him into joining the heist on the National Gallery, DC. He sent an email to King at throne1966@hotmail.com requesting his assistance or he would contact King's parole officer and advise them of King's current criminal activities that possibly violate his parole conditions.
- Tracy and Carry made arrangements for Carry to deliver a tablet with data owned by a flashmob distracting the museum's security guards, while King would commit the theft.
- Tracy sent documents to herself pertaining to the stamps to be stolen, as well as the value they were insured for.

- Tracy was advised that a 'Gift Card' for \$1000 was set up for her. This was most possibly payment for her part in the job made from Carry via an individual named Alex or made directly from Alex.

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
1.1	Tuesday, June 12, 2012 at 09:25:04 PM	SMS from Pat (Perry) at 1(571)308-3236	What are you up to this weekend?	vol5/mobile/Library/SMS/sms.db
1.2	Wednesday, June 13, 2012 at 05:30:28 PM	SMS from Terry at 1(703)829-6071	I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook.	vol5/mobile/Library/SMS/sms.db
1.3	Wednesday, June 13, 2012 at 06:30:38 PM	SMS from Pat (Perry) at 1(571)308-3236	I don't have any big plans. How about you?	vol5/mobile/Library/SMS/sms.db
1.4	Wednesday, June 13, 2012 at 18:33:46 PM	SMS to Terry at 1(703)829-6071	Ok, sounds good	vol5/mobile/Library/SMS/sms.db

1.5	Tuesday, June 19, 2012 02:38:59 PM	Email from: Pat (Perry) at perrypatsum@yahoo.com To: Tracy (Coral) at coralbluetwo@hotmail.com	Hey Coral, Just got your email. That took longer than expected! Oh well! You've got to check out this new song by the VMs. I love the base. Tell me what you think! Note: This email had an attachment 'Crazydave1.mp3' explaining how to install virtualbox.	vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
1.6	Tuesday, July 3, 2012 at 09:34 AM	Email from Pat (Perry) at	Hey sis i know a guy...he's known as king	/vol5/mobile/Library/Mail/Protected Index
1.7	Tuesday, July 3, 2012 at 01:41:51 PM	SMS to Terry at 1(703)829-6071	Hey honey, I'm not sure if we can afford Prufrock anymore... What do you think about switching to someplace else?	vol5/mobile/Library/SMS/sms.db
1.8	Tuesday, July 03 2012 at 02:04:32 PM	SMS from Terry at 1(703)829-6071	Moving schools at this point would be the worst! I would rather live with dad and stay at Prufrock than change schools :(vol5/mobile/Library/SMS/sms.db
1.9	Thursday, July 05, 2012 at 06:18:23 PM	SMS from Carry at 1 (202) 725-2124	Sounds good let's shoot for one at Bubba's grill	vol5/mobile/Library/SMS/sms.db

1.10	Thursday July 05, 2012 at 06:20:26 PM	SMS to Carry at 1 (202) 725-2124	Okay that sounds great. See you there	vol5/mobile/Library/SMS/sms.db
1.11	Thursday, July 5, 2012 at 12:58:41 PM	Email from Woina.Honril@m57.biz to Tracy (Coral) at coralbluetwo@hotmail.com	I didn't Note: This email contains attachments that appear to be official government documents	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
1.12	Friday, July 06, 2012 at 03:02:19 PM	SMS to Pat at 1 (571) 308-3236	Hey can you give me a call	vol5/mobile/Library/SMS/sms.db
1.13	Friday, July 06, 2012 at 03:08:37 PM	SMS from Pat (Perry) at 1(571)308-3236	Sis I'm really busy can we do this later	vol5/mobile/Library/SMS/sms.db
1.14	Friday, July 6, 2012 at 03:11:54 PM	SMS to Pat at 1 (571) 308-3236	No Pat this is important I need you to call me soon	vol5/mobile/Library/SMS/sms.db
1.15	Friday, July 06, 2012 at 03:13:31 PM	SMS from Pat (Perry) at 1(571)308-3236	Ok ok I'll call in 5	vol5/mobile/Library/SMS/sms.db

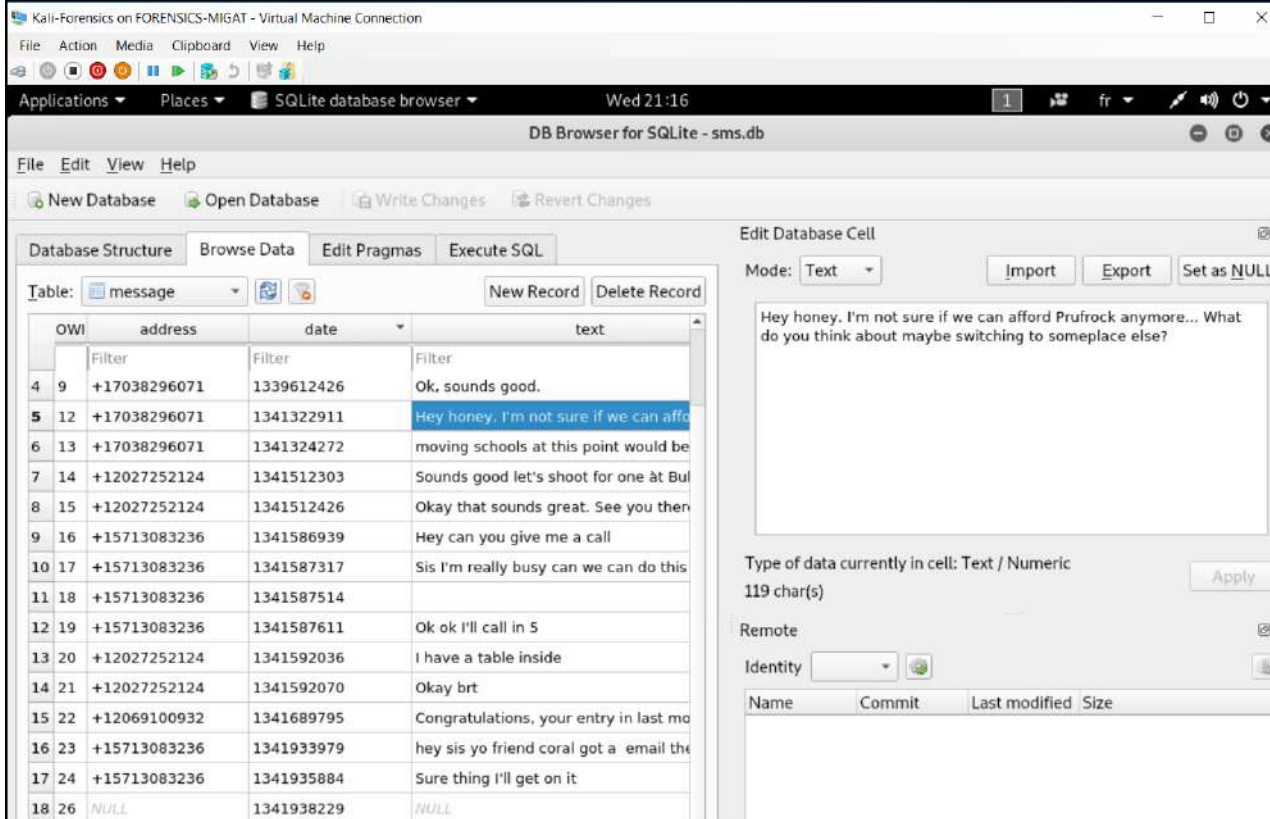
1.16	Friday, July 6, 2012 at 11:49:31 AM	Email from Pat (Perry) at patsumtwelve@gmail.com to King at throne1966@hotmail.com Cc: coralbluetwo@hotmail.com	King, Long time no see... I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. 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'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.	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
1.17	Friday, July 06, 2012 at 04:27:16 PM	SMS from Carry at 1(202) 725-2124	I have a table inside	vol5/mobile/Library/SMS/sms.db
1.18	Friday, July 06, 2012 at 04:27:50 PM	SMS to Carry at 1 (202) 725-2124	Okay brt	vol5/mobile/Library/SMS/sms.db

1.19	Saturday, July, 07 2012 at 07:36:35 PM	SMS from unknown at 1(206)910-0932	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	vol5/mobile/Library/SMS/sms.db
1.20	Monday, July 9, 2012 at 10:44:11 AM	Email from Tracy to herself: From tracysumtwelve@gmail.com to coralbluetwo@hotmail.com	Somethings Note: Attachments 'docs.zip' and 'documents.zip' contain stamp insurance documents in pdf format.	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
1.21	Tuesday, July 10, 2012 11:19 AM	From: King kthings throne1966@hotmail.com To: patsumtwelve@gmail.com Subject: RE: can't pass up	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 Note: Email contained attachment 'needs.txt'	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
1.22	Tuesday, July 10, 2012 11:24:58 AM	From Pat: patsumtwelve@gmail.com To Tracy: coralbluetwo@hotmail.com Subject: Fwd: can't pass up	"This is what we need to get for the guy that's going to make our job happen" Note: Email contained attachment 'needs.txt'	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com/pop3.live.com/INBOX.mbox/Messages/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
1.23	Tuesday, Jul 10, 2012, 03:26:19 PM	SMS from Pat (Perry) at 1(571)308-3236	hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know	/vol5/mobile/Library/SMS/sms.db
1.24	Tuesday, July 10, 2012 at	SMS to Pat (Perry) at 1(571)308-3236	Sure thing I'll get on it	/vol5/mobile/Library/SMS/sms.db

	03:58:04 PM			
1.25	Tuesday, July 10, 2012 at 05:18:38 PM	SMS to Terry at 1(703)829-6071	Going to lunch. You want to go?????	/vol5/mobile/Library /SMS/sms.db
1.26	Tuesday, July 10, 2012 at 06:19:24 PM	SMS to Terry at 1(703)829-6071	Back at work	/vol5/mobile/Library /SMS/sms.db
1.27	Tuesday, July 10, 2012 at 06:58:24 PM	SMS from Terry at 1(703)829-6071	I'm busy. Maybe this weekend if dad isn't busy	/vol5/mobile/Library /SMS/sms.db
1.28	Wednesday, July 11, 2012 at 12:41:45 PM	SMS from Carry at 1(202) 725-2124	I'm almost there where should I meet you?	/vol5/mobile/Library /SMS/sms.db
1.29	Wednesday, July 11, 2012 at 12:49:08 PM	SMS to Carry at 1(202) 725-2124	Just meet me out front, I'll take the tablet in.	/vol5/mobile/Library /SMS/sms.db
1.30	Wednesday, July 11, 2012 at 02:53 PM	Email from Carry at carrysum2012@yahoo.com	Hey so i'm putting together this event we talked about and i want to make it 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 know the shift changes so you dont 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.	/vol5/mobile/Library /Mail/Protected Index
1.31	Thursday July 12, 2012 at 01:24 PM	Email to Carry at carrysum2012@yahoo.com	Okay Carrie I'm going to send you this but you need to make sure no one else sees it okay I could get in a	/vol5/mobile/Library /Mail/POP-coralblue two@hotmail.com/pop3.live.com/INBO

			bunch of trouble. I want to help you and I could really use some extra cash too but please please be careful.	X.mbox/Messages/01FE9965-A923-40CF-A78A-72CEBD26571.emlx
1.32	Sunday, Jul 15, 2012 03:20:05 PM	SMS to Carry at 1(202) 725-2124	How's the flashmob going	/vol5/mobile/Library/SMS/sms.db
1.33	Monday, Jul 16, 2012 06:48:50	SMS from Terry at 1(703)829-6071	I really want to go to Dad's this weekend. He said he'll take me shopping for school	/vol5/mobile/Library/SMS/sms.db

The table below shows some screenshots to support the Correspondence Evidence in Appendix A.

SMS-screenshots																																																																	
Artifact #	Screenshots																																																																
2.1	 <p>The screenshot displays the DB Browser for SQLite application. The main window shows a table named 'message' with the following data:</p> <table><tr><th>OWI</th><th>address</th><th>date</th><th>text</th></tr><tr><td>9</td><td>+17038296071</td><td>1339612426</td><td>Ok, sounds good.</td></tr><tr><td>12</td><td>+17038296071</td><td>1341322911</td><td>Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?</td></tr><tr><td>13</td><td>+17038296071</td><td>1341324272</td><td>moving schools at this point would be</td></tr><tr><td>14</td><td>+12027252124</td><td>1341512303</td><td>Sounds good let's shoot for one at Bul</td></tr><tr><td>15</td><td>+12027252124</td><td>1341512426</td><td>Okay that sounds great. See you then</td></tr><tr><td>16</td><td>+15713083236</td><td>1341586939</td><td>Hey can you give me a call</td></tr><tr><td>17</td><td>+15713083236</td><td>1341587317</td><td>Sis I'm really busy can we can do this</td></tr><tr><td>18</td><td>+15713083236</td><td>1341587514</td><td></td></tr><tr><td>19</td><td>+15713083236</td><td>1341587611</td><td>Ok ok I'll call in 5</td></tr><tr><td>20</td><td>+12027252124</td><td>1341592036</td><td>I have a table inside</td></tr><tr><td>21</td><td>+12027252124</td><td>1341592070</td><td>Okay brt</td></tr><tr><td>22</td><td>+12069100932</td><td>1341689795</td><td>Congratulations, your entry in last mo</td></tr><tr><td>23</td><td>+15713083236</td><td>1341933979</td><td>hey sis yo friend coral got a email the</td></tr><tr><td>24</td><td>+15713083236</td><td>1341935884</td><td>Sure thing I'll get on it</td></tr><tr><td>26</td><td>NULL</td><td>1341938229</td><td>NULL</td></tr></table> <p>The right pane shows the 'Edit Database Cell' dialog with the text content: 'Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?'. The 'Type of data currently in cell' is 'Text / Numeric' and '119 char(s)'. The 'Remote' section shows 'Identity' and 'Name' fields.</p>	OWI	address	date	text	9	+17038296071	1339612426	Ok, sounds good.	12	+17038296071	1341322911	Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?	13	+17038296071	1341324272	moving schools at this point would be	14	+12027252124	1341512303	Sounds good let's shoot for one at Bul	15	+12027252124	1341512426	Okay that sounds great. See you then	16	+15713083236	1341586939	Hey can you give me a call	17	+15713083236	1341587317	Sis I'm really busy can we can do this	18	+15713083236	1341587514		19	+15713083236	1341587611	Ok ok I'll call in 5	20	+12027252124	1341592036	I have a table inside	21	+12027252124	1341592070	Okay brt	22	+12069100932	1341689795	Congratulations, your entry in last mo	23	+15713083236	1341933979	hey sis yo friend coral got a email the	24	+15713083236	1341935884	Sure thing I'll get on it	26	NULL	1341938229	NULL
OWI	address	date	text																																																														
9	+17038296071	1339612426	Ok, sounds good.																																																														
12	+17038296071	1341322911	Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?																																																														
13	+17038296071	1341324272	moving schools at this point would be																																																														
14	+12027252124	1341512303	Sounds good let's shoot for one at Bul																																																														
15	+12027252124	1341512426	Okay that sounds great. See you then																																																														
16	+15713083236	1341586939	Hey can you give me a call																																																														
17	+15713083236	1341587317	Sis I'm really busy can we can do this																																																														
18	+15713083236	1341587514																																																															
19	+15713083236	1341587611	Ok ok I'll call in 5																																																														
20	+12027252124	1341592036	I have a table inside																																																														
21	+12027252124	1341592070	Okay brt																																																														
22	+12069100932	1341689795	Congratulations, your entry in last mo																																																														
23	+15713083236	1341933979	hey sis yo friend coral got a email the																																																														
24	+15713083236	1341935884	Sure thing I'll get on it																																																														
26	NULL	1341938229	NULL																																																														

Kali-Forensics on FORENSICS-MIGAT - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places SQLite database browser Wed 21:47

DB Browser for SQLite - sms.db

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragas Execute SQL

Table: message New Record Delete Record

	address	date	text	
	Filter	Filter	Filter	Filter
7	+12027252...	1341512303	Sounds good let's shoot for one at Bubba's grill	2
8	+12027252...	1341512426	Okay that sounds great. See you there	3
9	+15713083...	1341586939	Hey can you give me a call	3
10	+15713083...	1341587317	Sis I'm really busy can we can do this later	2
11	+15713083...	1341587514		3
12	+15713083...	1341587611	Ok ok I'll call in 5	2
13	+12027252...	1341592036	I have a table inside	2
14	+12027252...	1341592070	Okay brt	3
15	+12069100...	1341689795	Congratulations, your entry in last months dr...	2
16	+15713083...	1341933979	hey sis yo friend coral got a email the attach...	2
17	+15713083...	1341935884	Sure thing I'll get on it	3
18	NULL	1341938229	NULL	33
19	+17038296...	1341940718	Going to lunch. You want to go?????	3
20	+17038296...	1341944364	Back at work	3
21	+17038296...	1341946704	I'm busy. Maybe this weekend if dad isn't busy	2

Edit Database Cell

Mode: Text Import Export Set as NULL

hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know

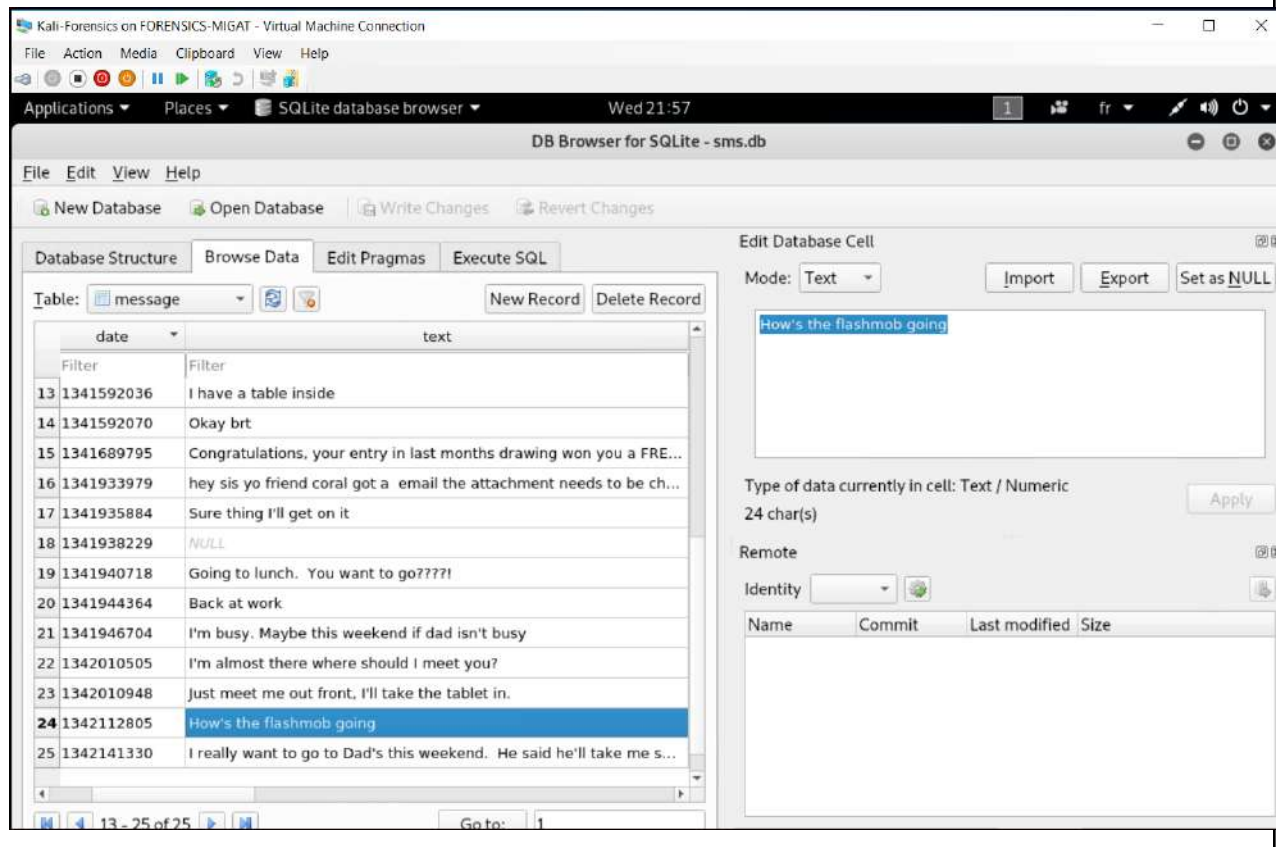
Type of data currently in cell: Text / Numeric
91 char(s) Apply

Remote

Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

2.3



2.4

Kali-Forensics on FORENSICS-MIGAT - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places SQLite database browser Wed 22:01

DB Browser for SQLite - sms.db

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragas Execute SQL

Table: message New Record Delete Record

	OWI	address	date	text
		Filter	Filter	Filter
13	20	+12027252124	1341592036	I have a table inside
14	21	+12027252124	1341592070	Okay brt
15	22	+12069100932	1341689795	Congratulations, your entry in last months draw
16	23	+15713083236	1341933979	hey sis yo friend coral got a email the attachm
17	24	+15713083236	1341935884	Sure thing I'll get on it
18	26	NULL	1341938229	NULL
19	27	+17038296071	1341940718	Going to lunch. You want to go?????
20	28	+17038296071	1341944364	Back at work
21	29	+17038296071	1341946704	I'm busy. Maybe this weekend if dad isn't busy
22	30	+12027252124	1342010505	I'm almost there where should I meet you?
23	31	+12027252124	1342010948	Just meet me out front, I'll take the tablet in.
24	32	+12027252124	1342112805	How's the flashmob going
25	33	+17038296071	1342141330	I really want to go to Dad's this weekend. He

Go to: 1

Edit Database Cell

Mode: Text Import Export Set as NULL

I really want to go to Dad's this weekend. He said he'll take me shopping for school

Type of data currently in cell: Text / Numeric
85 char(s)

Apply

Remote


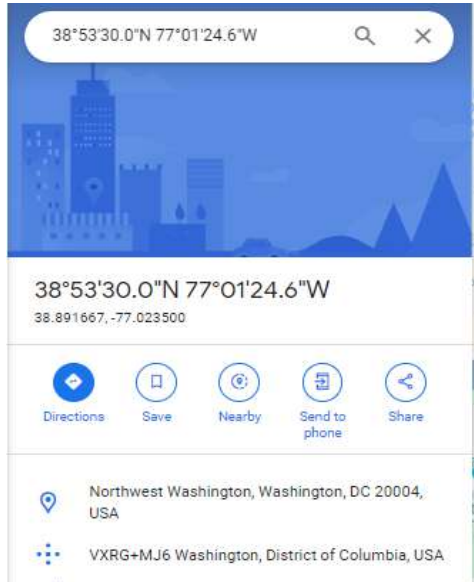
Identity


Name	Commit	Last modified	Size
------	--------	---------------	------

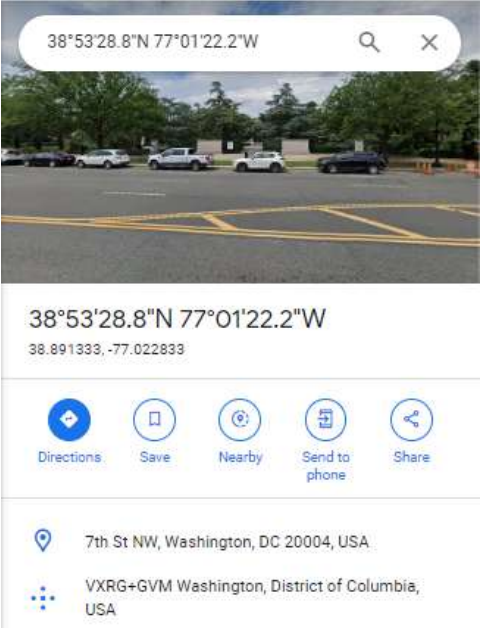

2.5

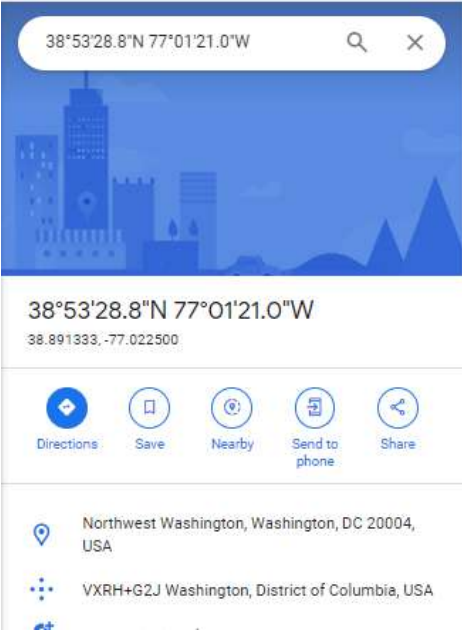

ID	Address	Date	Text
+15713083236	2012-06-14 20:05:04	What are you up to this weekend?	
+17038296071	2012-06-15 14:17:08	I'm going out with dad after school for pizzaz thought I'd let you know if you planned to cook.	
+15713083236	2012-06-15 16:57:18	I don't have any big plans. How about you?	
+17038296071	2012-06-15 17:07:06	Ok, sounds good.	
+17038296071	2012-07-03 08:21:51	Hey honey, I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?	
+17038296071	2012-07-03 08:57:52	Moving schools at this point would be the worst! I would rather live with dad and stay at Prufrock then change schools :(
+12027252124	2012-07-05 14:38:23	Sounds good let's shoot for one at Bubba's grill	
+12027252124	2012-07-05 14:40:26	Okay that sounds great. See you there	
+15713083236	2012-07-06 06:35:39	Hey, can you give me a call	
+15713083236	2012-07-06 06:41:57	Sis, I'm really busy can we do this later	
+15713083236	2012-07-06 06:45:14	No Pat, this is important. I need you to call me soon	
+15713083236	2012-07-06 06:46:51	Ok, ok. I'll call in 5	
+12027252124	2012-07-06 20:47:16	I have a table inside	
+12027252124	2012-07-06 20:47:50	Okay, be right there	
+12069100932	2012-07-08 12:56:35	Congratulations, your entry in last month's drawing won you a FREE \$1,000 Target Giftcard! Enter "703" at www.target.com.trdt.biz to tell us where to ship it	
+15713083236	2012-07-11 04:19:39	Hey sis, your friend Coral got an email; the attachment needs to be changed to pdf. Let her know.	
+15713083236	2012-07-11 04:51:24	Sure thing, I'll get on it	
+17038296071	2012-07-11 14:38:38	Going to lunch. You want to go?????	
+17038296071	2012-07-11 23:26:04	Back at work	
+17038296071	2012-07-12 08:51:44	I'm busy. Maybe this weekend if dad isn't busy	
+12027252124	2012-07-12 23:55:05	I'm almost there. Where should I meet you?	
+12027252124	2012-07-13 00:42:28	Just meet me out front, I'll take the tablet in.	
+12027252124	2012-07-15 15:20:05	How's the flashmob going?	
+17038296071	2012-07-16 06:48:50	I really want to go to Dad's this weekend. He said he'll take me shopping for school	

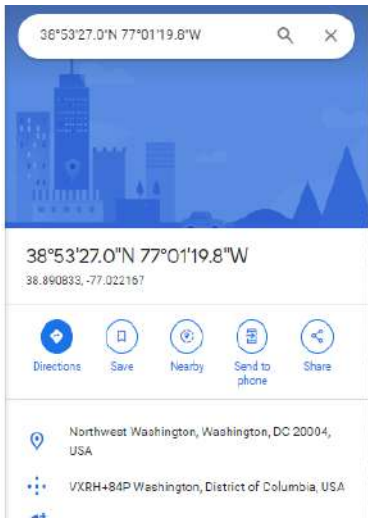

Appendix B: WiFi and GPS Location Information

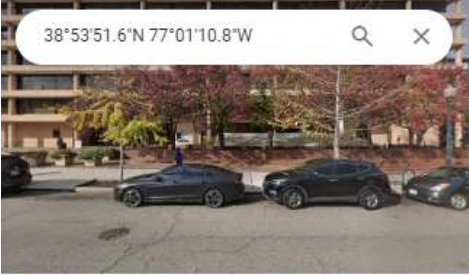

Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
4.1	Jul 8, 2012 at 16:33:36	IMG_0042.JPG	<p>Subject: Shrubs</p> <p>Location: National Gallery of Art Sculpture Garden</p> <p>Northwest Washington, Washington, DC 20004, USA</p>	 
4.2	Jul 8, 2012 at 16:34:31	IMG_0043.JPG	<p>Subject: Plant with pink flowers</p>	As depicted in artifact 4.1 above

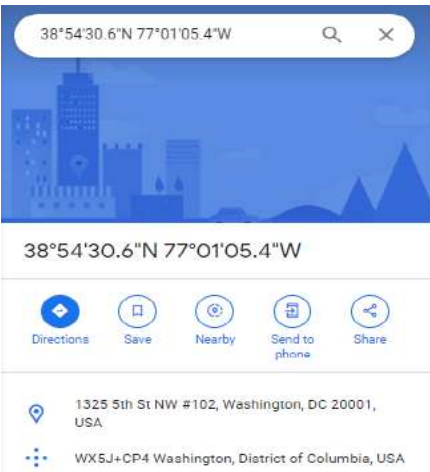
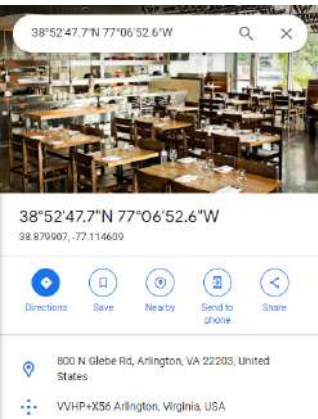
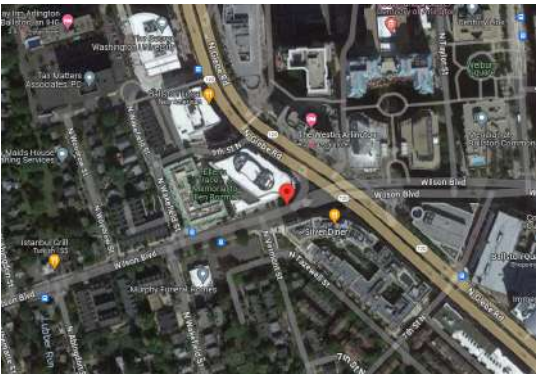
			<p>Location: National Gallery of Art Sculpture Garden</p> <p>Northwest Washington, Washington, DC 20004, USA</p>	
4.3	Jul 8, 2012 at 16:34:49	IMG_0044.JPG	<p>Subject: Seating Area</p> <p>Location: National Gallery of Art Sculpture Garden</p> <p>Northwest Washington, Washington, DC 20004, USA</p>	As depicted in artifact 4.1 above
4.4	Jul 8, 2012 at 16:35:50	IMG_0045.JPG	<p>Subject: Trash Can</p> <p>Location: National Gallery of Art Sculpture Garden</p> <p>Northwest Washington, Washington, DC 20004, USA</p>	


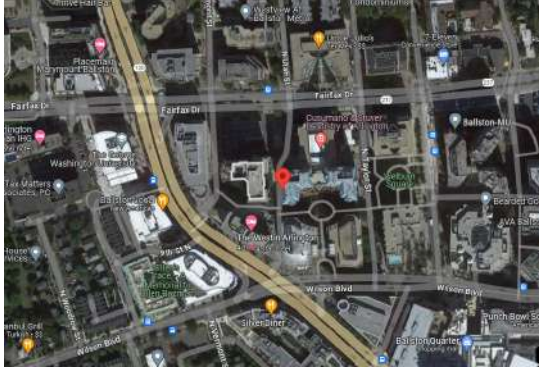



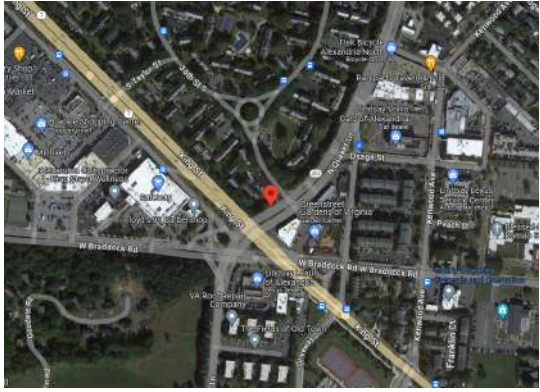
				
4.5	Jul 8, 2012 at 16:36:30	IMG_0046.JPG	<p>Subject: Plant with white flowers</p> <p>Location: National Gallery of Art Sculpture Garden</p> <p>Northwest Washington, Washington, DC 20004, USA</p>	

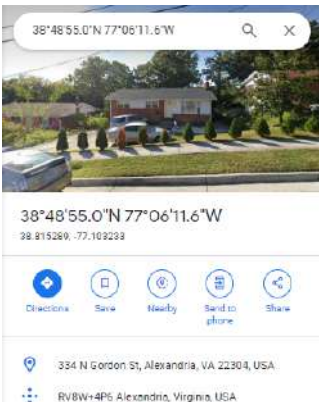

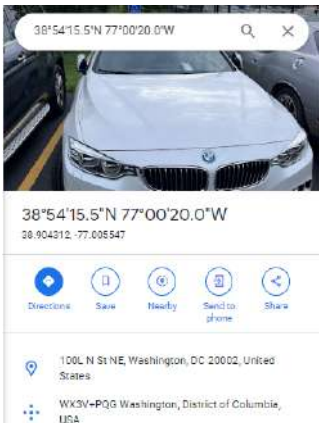
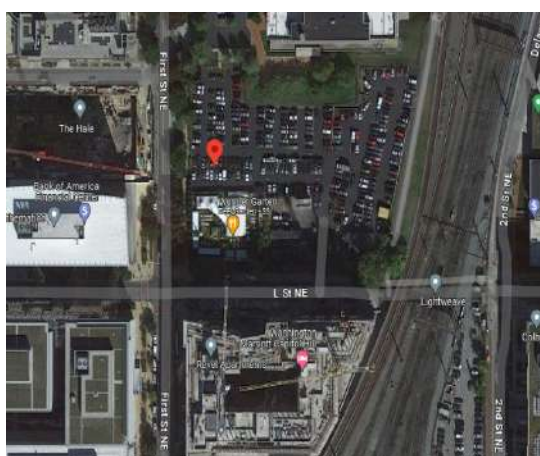
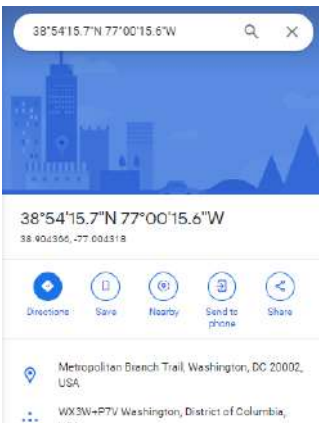
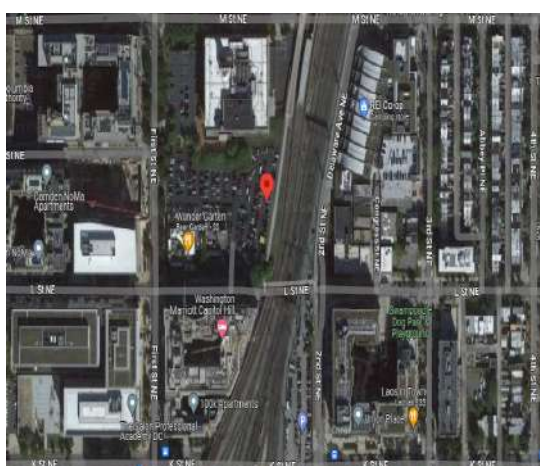
				
4.6	Jul 8, 2012 at 16:37:15	IMG_0047.JPG	<p>Subject: Pedestrian Crossing</p> <p>Location: Near the National Gallery of Art Sculpture Garden</p> <p>Northwest Washington, Washington, DC 20004, USA</p>	

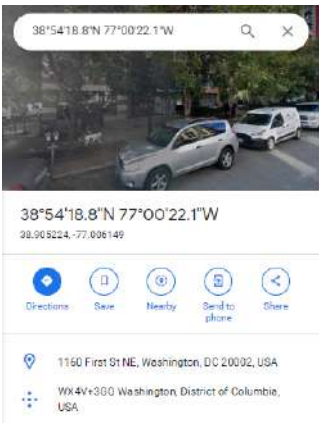

				 <p>36°53'27.0"N 77°01'19.8"W</p> <p>38°53'27.0"N 77°01'19.8"W 38.890833, -77.022167</p> <p>Directions Save Nearby Send to phone Share</p> <p>Northwest Washington, Washington, DC 20004, USA</p> <p>VXRH+84P Washington, District of Columbia, USA</p>
4.7	Jul 8, 2012 at 16:37:36	IMG_0048.JPG	<p>Subject: Entrance Sign National Gallery of Art Sculpture Garden</p> <p>Location: National Gallery of Art Sculpture Garden</p>	As depicted in artifact 4.6 above
4.8	Jul 8, 2012 at 16:41:30	<p>IMG_0049.JPG</p> <p>IMG_0050.JPG</p> <p>IMG_0051.JPG</p>	<p>Subject: Photos of Stamps</p> <p>Location: National Gallery of Art Sculpture Garden</p>	As depicted in artifact 4.1 above
4.9	Jul 8, 2012 at 16:49:20	IMG_0054.JPG	<p>Subject: Photo of Stamp</p> <p>Location: 600 5th St NW, Washington, DC 20001, USA</p>	

				 <p>38°53'51.6"N 77°01'10.8"W</p> <p>38°53'51.6"N 77°01'10.8"W</p> <p> Directions Save Nearby Send to phone Share </p> <p> 600 5th St NW, Washington, DC 20001, USA VXXJ+348 Washington, District of Columbia, USA </p>
4.10	Jul 8, 2012 at 16:49:20	IMG_0055.JPG IMG_0056.JPG IMG_0057.JPG IMG_0058.JPG	Subject: Photos of Stamps Location: 600 5th St NW, Washington, DC 20001, USA	As depicted in artifact 4.9 above
4.11	Jul 8, 2012 at 16:51:39	IMG_0064.JPG	Subject: Photo of bathroom sink Location: 1325 5th St NW #102, Washington, DC 20001, USA	

				
4.12	Jul 8, 2012 at 16:59:51	IMG-0065.JPG IMG-0066.JPG IMG-0067.JPG IMG-0068.JPG IMG-0069.JPG	Subject: Photos of Stamps Location: National Gallery of Art Sculpture Garden	As depicted in artifact 4.1 above
4.13	July 2, 2012 11:19:24	WIFI Location	Location: 	

4.14	July 5, 2012 11:32:47	WIFI Location	<p>Location:</p>  <p>38°52'52.1"N 77°06'49.8"W 38.881132, -77.113841</p> <p>Directions Save Nearby Send to phone Share</p> <p>900 N Taylor St, Arlington, VA 22203, USA VVJP+FF3 Arlington, Virginia, USA</p>	
4.15	July 10, 2012 11:31:12	WIFI Location	<p>Location:</p>  <p>38°50'50.9"N 77°04'50.8"W 38.847469, -77.080787</p> <p>Directions Save Nearby Send to phone Share</p> <p>Green Valley, Arlington, VA, USA RWW9+XMP Arlington, Virginia, USA</p>	
4.16	July 10, 2012 11:45:01	WIFI Location	<p>Location:</p>  <p>38°49'39.5"N 77°05'15.4"W 38.827624, -77.087619</p> <p>Directions Save Nearby Send to phone Share</p> <p>4100 36th St S, Arlington, VA 22206, USA RWH6+2XR Arlington, Virginia, USA</p>	



4.17	July 10, 2012 11:44:59	CellLocation	<p>Location:</p>  <p>38°48'55.0"N 77°06'11.6"W 98.815269, -77.102239</p> <p>Directions Save Nearby Send to phone Share</p> <p>334 N Gordon St, Alexandria, VA 22304, USA RV8W+4P6 Alexandria, Virginia, USA</p>	
4.18	July 10, 2012 11:44:59	CellLocation	<p>Location:</p>  <p>38°54'15.5"N 77°00'20.0"W 98.904312, -77.005547</p> <p>Directions Save Nearby Send to phone Share</p> <p>100L N St NE, Washington, DC 20002, United States WX3V+PQ6 Washington, District of Columbia, USA</p>	
4.19	July 10, 2012 11:44:59	CellLocation	<p>Location:</p>  <p>38°54'15.7"N 77°00'15.6"W 98.904356, -77.004319</p> <p>Directions Save Nearby Send to phone Share</p> <p>Metropolitan Branch Trail, Washington, DC 20002, USA WX3W+P7V Washington, District of Columbia, USA</p>	



4.20	July 10, 2012 11:44:59	CellLocation	<div>Location:</div> <div>  <p>38°54'18.8"N 77°00'22.1"W 38.905224, -77.006149</p> <p> Directions Save Nearby Send to phone Share </p> <p>1150 First St NE, Washington, DC 20002, USA</p> <p>WX 4V+3G0 Washington, District of Columbia, USA</p> </div>	
------	---------------------------	--------------	--	--

The following are images found in Tracy’s iPhone that were reviewed in the investigation:



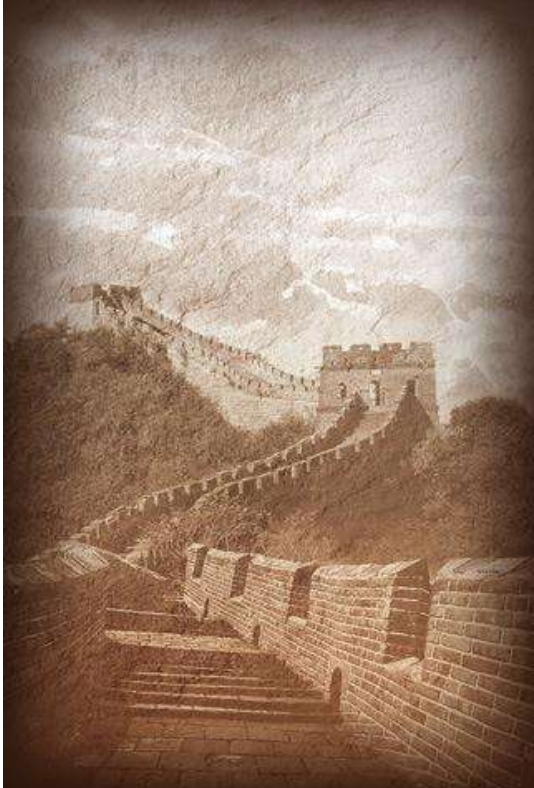
Images found in Tracy’s iPhone		
Artifact #	Header Information	Photo Evidence
5.1	<div>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0057.JPG</div> <div>Timestamp: Sunday July 8, 2012 at 12:50:07 EDT</div>	

<p>5.2</p>	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0056.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:49:49 EDT</p>	
<p>5.3</p>	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0055.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:49:37 EDT</p>	

5.4	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0054.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:49:25 EDT</p>	
5.5	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0064.JPG</p> <p>Timestamp: Sunday July 8, 2012 12:51:44 EDT</p>	



5.6	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0052.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:42:48 EDT</p>	
5.7	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0051.JPG</p> <p>Timestamp: Sunday July 8, 2012 12:42:03 EDT</p>	



5.8	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0050.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:41:53 EDT</p>	
5.9	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0049.JPG</p> <p>Timestamp: Sunday July 8 at 12:41:41 EDT</p>	
5.10	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0048.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:37:37 EDT</p>	



5.11	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0047.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:37:16 EDT</p>	
5.12	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0046.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:37:30 EDT</p>	
5.13	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0071</p> <p>Timestamp: Wednesday July 11, 2012 at 12:18:48 EDT</p>	



5.14	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0070.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 01:02:23 EDT</p>	
5.15	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0069.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 01:00:23 EDT</p>	
5.16	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0068.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 01:00:12 EDT</p>	

5.17	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0067.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 01:00:07 EDT</p>	
5.18	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0066.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 01:00:01 EDT</p>	

5.19	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0065.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:59:55 EDT</p>	
5.20	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0064.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:51:44 EDT</p>	

<p>5.21</p>	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0063.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:51:14 EDT</p>	
<p>5.22</p>	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0062.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:51:03 EDT</p>	

5.23	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0061.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:50:53 EDT</p>	
5.24	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0060.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:50:50 EDT</p>	

5.25	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0059.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:50:34 EDT</p>	
5.26	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0058.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:50:20 EDT</p>	

5.27	<p>File location:</p> <p>Timestamp: Sunday July 8, 2012 at 12:35:50 EDT</p>	
5.28	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0044.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:34:50 EDT</p>	

5.29	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0043.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:34:31 EDT</p>	 A photograph of a potted plant. The plant has large, heart-shaped green leaves with prominent veins. At the base of the leaves, there are numerous bright pink flowers. The plant is in a white pot, and the background is a bright, sunny outdoor area.
5.30	<p>File location: vol5/mobile/Media/DCIM/100APPLE/IMG_0042.JPG</p> <p>Timestamp: Sunday July 8, 2012 at 12:33:36 EDT</p>	 A photograph of a dense, green shrub or bush. The leaves are small and dark green, with some showing signs of aging or damage. The plant is growing in a garden or yard, with a concrete path visible in the foreground.