Case Report
National Gallery DC

Tracy’s iPhone [2012-07-15-National-Gallery]

Table of Contents

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.

Alex is seeking to embarrass the United States and damage public relations by defacing foreign art belonging to Majavia that is on display at the National Gallery during the month of July. Tracy plans to steal stamps from the National Gallery. Joe, Tracy's soon to be ex-husband, installs a keylogger, discovers the conspiracy, and reports it to the police.

Equipment and Tools

- Autopsy
- SQLite Browser
- Kali Linux

Details of Tracy's iPhone

Host Name: Tracy Sumtwelve's iPhone
Model: iPhone 3G
OS Version: iPhone OS 4.2.1 (8C148)
Install Time: 6/6/2012 19:03:28
Phone #: (703) 340-9961
Serial #: 86004482Y7H
ICCID: 89014103255195342366
IMEI: 012021003735398

Evidence to Establish Personas

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

Tracy aka Coral Blue:
Phone Number: 703.340.9961
Personal Email: tracysumtwelve@gmail.com
Personal Email: coralbluetwo@hotmail.com
Work Email: tracy.sumtwelve@nationalgallerydc.org
Relationship: Accused/ Employee at the National Gallery DC

Pat aka Perry:
Phone Number: 571.308.3236
Email: patsumtwelve@gmail.com
Email: perrypatsum@yahoo.com
Relationship: Tracy's Brother

Terry:
Phone Number: 703.829.6071
Email: N/A
Relationship: Tracy and Joe's Daughter

Joe:
Phone Number:
Email: joe.sum.twelve@gmail.com
Relationship: Terry's Father / Currently going through a Divorce with Tracy

Carry:
Phone Number: 202.725.2124
Email: carrysum2012@yahoo.com
Relationship: Terry's Friend IT and Alex's Subordinate

Alex:
Phone: Unknown
Email: Unknown
Relationship:
Alex is a Krasnovian supporter who wishes to embarrass the United States. He lives outside the United States, presumably in a region called Krasnovia.

Tracy and Pat are strapped for cash. Tracy has full custody of her daughter, Terry, but is struggling to pay Terry's tuition for school. Joe refuses to help pay for Terry's tuition unless he has full custody of his daughter. Tracy and Pat decide to sell stamps stolen from the National

Gallery DC for extra cash. Carry influences Terry into a museum art heist at the National Gallery in DC. Carry is a representative of Alex, a Krasnovian supporter, who is intent on embarrassing the US. Joe, Tracy's husband, prevents extensive damage because of the spyware/keylogger that he inserted on Tracy's phone.

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. Tracy mentions keeping tabs on items of value going through the gallery to her brother Pat through email on Friday, June 29, 2012 (Artifact 07). The stamp insurance documents extracted from Tracy's mail attachments (Artifact 21, Artifact 22, and Artifact 23) indicate that the stamps are valuable and items of interest for Tracy. An album of stamp images extracted from Tracy's phone indicate her possession of the stamps, and can be found in Appendix D below.

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. Pat, Tracy's brother, emails King to help with the defacement of the museum art (Artifact 13). Carry emails Tracy about getting his tablet through security. Carry intends to take pictures of the flashmob (Artifact 15). Carry offers to pay Tracy in order to help with the flash mob. A suspicious mail attachment is found indicating the necessary items that Carry will need to initiate the flashmob (Artifact 24). Tracy sends a text message to Carry asking how the flash mob is going (Artifact 19).

Plot Timeline

- June 19, 2012- Pat and Tracy establish aliases. Pat's alias is Perry and Tracy's alias is Coral Blue (Artifact 01).
- June 28, 2012- Pat mentions that money is rough for both of them (Artifact 05).
- June 29, 2012- "Perry" and "Coral" mention that the gallery will be hosting special events soon (Artifact
- July 2, 2012- Tracy asks Joe for help to pay for Terry's school tuition (Artifact 09).
- July 5, 2012- Carry notices that Tracy has been having a hard time and offers to take her to lunch (Artifact 11).
- July 6, 2012- Pat proposes heist at the National Gallery to King (Artifact 13).

- July 9, 2012- Carry asks Tracy to help her get her tablet through the National Gallery's security (Artifact 15).
- July 10, 2012-Tracy agrees to help Carry get her tablet through the National Gallery's security (Artifact 16).
- July 10, 2012- Carry informs Tracy that she would like to come to the National Gallery tomorrow [July 11th] at 9 (Artifact 17).
- July 12, 2012- The flash mob at the National Gallery (Artifact 19).

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy used the alias Coral and Pat used the alias Perry.
- Pat and Tracy conspired to steal valuable stamps from the National Gallery.
- Motivation for the stamp theft most likely began with Tracy's inability to afford Terry's tuition.
- Carry, a Krasnovian supporter, and Alex's subordinate orchestrated a flash mob to deface the National Gallery's art and embarrass the US.
- Joe, Tracy's ex-husband, installed the keylogger on Tracy's phone, and reported these illegal activities to the authorities.

Appendix A: Correspondence Evidence

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
01	Date: Tue, 19 Jun 2012 13:26:47 -0700 (PDT)	From: Perry Patsum <perrypatsum@yahoo.com> To: Tracy Sumtwelve <tracysumtwelve@gmail.com Subject: Look me up sometime	Perry talked to Tracy's brother about an email, and said to have her friend "Alias" send him an email.	Email
02	Date: Tue, 19 Jun 2012 14:39:34 -0700 (PDT)	From: Perry Patsum <perrypatsum@yahoo.com> To: Coral BlueTwo	Perry replies to Coral BlueTwo that he is just now receiving the emails.	Email

		<coralbluetwo@hotmail.com> Subject: Re: ???		
03	Date: Tue, 19 Jun 2012 16:06:33 -0400	From: Pat TeeSumTwelve <patsumtwelve@gmail.com> To: Tracy TeeSumTwelve <TracySumtwelve@gmail.com> Subject: Paris Speak and answer	Translation from French: Pat asks Tracy to send the email address of her Alias and he will send her additional instructions.	Email
04	Tuesday, June 19, 2012 5:02 PM	From: Coral BlueTwo <coralbluetwo@hotmail.com> To: Perry Patsum <perrypatsum@yahoo.com> Subject: ???	Coral asks if Perry is getting the two emails that they sent already.	Email
05	Date: Thu, 28 Jun 2012 12:31:33 -0700 (PDT)	From: Perry Patsum <perrypatsum@yahoo.com> Reply-To: Perry Patsum <perrypatsum@yahoo.com> To: Coral Bluetwo coralbluetwo@hotmail.com Subject: Whats going on	Perry says they should communicate through this channel now that “everything is set up.” He mentions money is rough for both of them, and that he knows people who are good at these types of “things.”	Email
06	Date: June 29, 2012 @ 07:31:36	From: Perry Patsum <perrypatsum@yahoo.com> To: Tracy TeeSumTwelve tracysumtwelve@gmail.com	petty/pat checking in with sis (tracy). Asking if Terry sorted out the problems in her literature class. Discusses about having to sort things out with Coral. Wants to have dinner.	Email
07	Fri, 29 Jun 2012 08:21:36 -0700	From: Perry Patsum <perrypatsum@yahoo.com> Reply-To: Perry Patsum <perrypatsum@yahoo.com> To: Coral coralbluetwo@hotmail.com Subject: Re: Whats going on	Mention of “insurance type” documents that place values on certain objects. Mention of the gallery hosting interesting events this time of year. Mention of “kiddo” getting bent out of shape at the prospect of having to change schools.	Email
08	Date: Fri, 29 Jun 2012 07:31:36 -0700 (PDT)	From: Perry Patsum <perrypatsum@yahoo.com> To: Tracy SumTwelve		

		<tracysumtwelve@gmail.com> Subject: hey sis		
09	Mon, Jul 2, 2012 at 4:06 PM	From: Tracy Sumtwelve <tracysumtwelve@gmail.com> To: Joe Sumtwelve <joe.sum.twelve@gmail.com> Subject: Regarding Terry	Tracy asks Joe for help with Terry's tuition.	Email
10	Date: Tue, 3 Jul 2012 09:29:37 -0400	From: Joe Sumtwelve joe.sum.twelve@gmail.com To: Tracy Sumtwelve tracysumtwelve@gmail.com Subject: Re: Regarding Terry	Joe informs Tracy that he won't be paying for Terry's school if Terry isn't living with him	Email
11	Thu, 5 Jul 2012 08:51:31 (PDT)	From: Carry Sumttwentytwelve carrysum2012@yahoo.com To: tracysumtwelve@gmail.com Subject: Long time no see...	Carry notices on Facebook that Tracy has been having a hard time recently. She wants to make plans to meet up on Friday	Email
12	Fri, Jul 6, 2012 10:55 AM PDT	From:Tracy SumTwelve tracysumtwelve@gmail.com Carry Sumttwentytwelve carrysum2012@yahoo.com	Tracy thanks Carry for lunch.	Email
13	Fri, 6 Jul 2012 08:49:31 (PDT) Date: Fri, 6 Jul 2012 11:49:31	From: Pat TeeSumTwelve patsumtwelve@gmail.com To: throne1966@hotmail.com Cc: coralbluetwo@hotmail.com Subject: can't pass up	Pat proposes a heist at the national gallery to King and CCs Tracy's personal email. He uses an intimidation tactic by mentioning that he is familiar with King's parole officer, and he threatens to provide an anonymous tip to the feds about King's drug dealing, if King refuses to help with the heist. Two weeks from Fri. July 6th indicates that the attack will occur on Fri. July 20th.	Email

14	Date: Fri, 6 Jul 2012 11:27:51 -0400	From: Pat TeeSumTwelve patsumtwelve@gmail.com To: Tracy Sumtwelve tracysumtwelve@gmail.com Subject: Re: Good News	Pat informs Tracy about King.	Email
15	Date: Jul 9, 2012 Time: 2:18 PM	From: Carry Sumttwentytwelve To: Tracy Sumtwelve tracysumtwelve@gmail.com	Carry asks Tracy for help to get her tablet through security so she can take pictures for her flash mob event. Carry mentions security doesn't like computers in the gallery.	Email
16	Tue, Jul 10, 2012 6:29 AM PDT	From: Tracy Sumtwelve tracysumtwelve@gmail.com To: Carry Sumtwentytwelve	Tracy agrees to help Carry get her tablet through security.	Email
17	Date: Tue, 10 Jul 2012 06:48:40 -0700 (PDT)	From: Carry Sumttwentytwelve carrysum2012@yahoo.com To: tracysumtwelve@gmail.com Subject: Re: Long time no see...	Carry asks to come to the gallery "tommorrow" at 9.	Email
18	7/10/2012 15:26:19	From: Pat To: Tracy	hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know. *(note: this is the needs.pdf file)*	SMS
19	7/12/2012	From: Tracy To: Carry	How's the flashmob going?	SMS

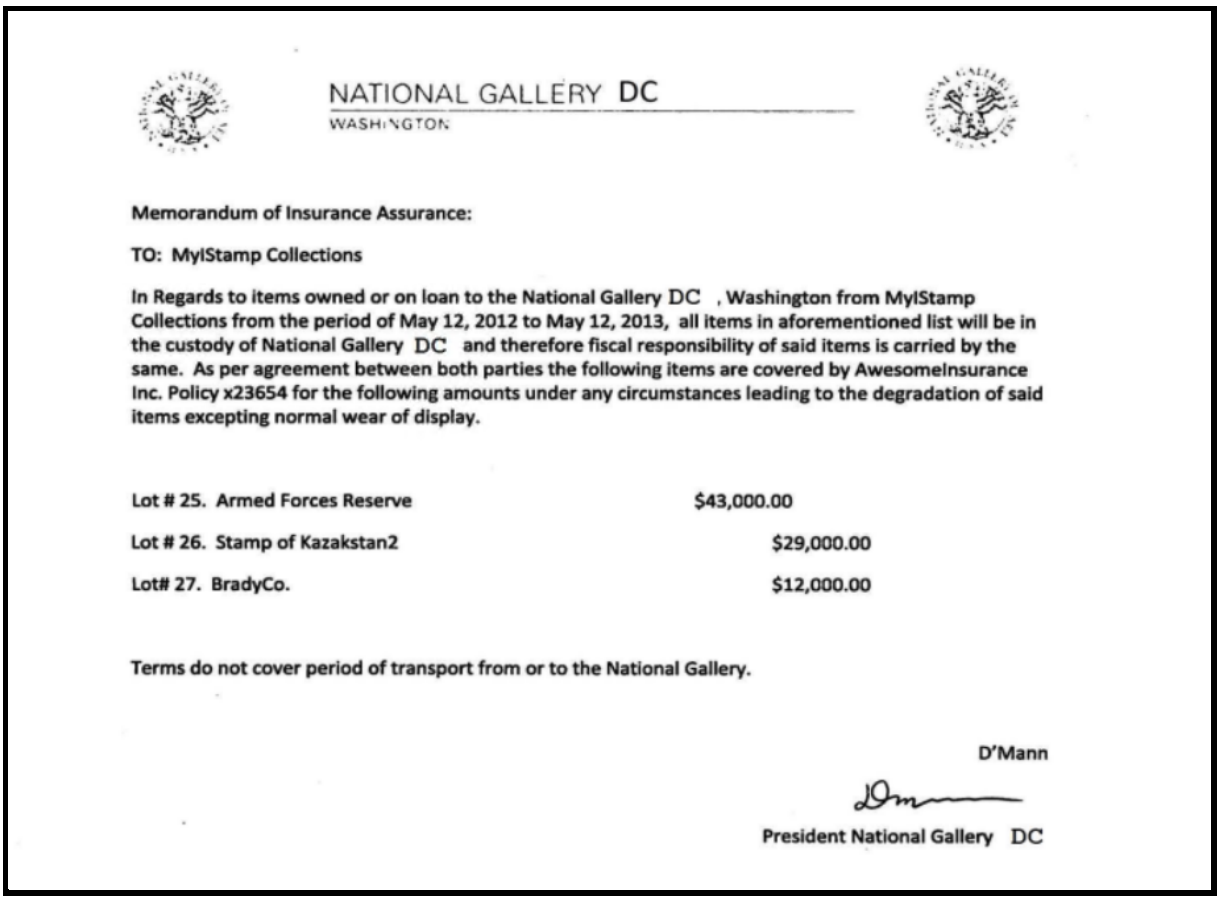
Appendix B: WiFi and GPS Location Information

Location Information			
Artifact #	Timestamp	Header Information	Body
1.1	3.61	GPS Coordinates	900 N Glebe Rd Arlington, Virginia 38.88055896 -77.11553561
1.2	3.61	GPS Coordinates	N Glebe Rd, Arlington, VA 22203 38.88106083 -77.11533838
1.3	3.61	GPS Coordinates	801 N Wakefield St, Arlington, VA 22203 38.88005346 -77.11595332
1.4	3.61	GPS Coordinates	Bluemont, Arlington, VA 22203 38.88093715 -77.11640596
1.5	3.61	GPS Coordinates	851-977 N Glebe Rd, Arlington, VA 22203 38.88138395 -77.11556851
1.6	3.61	GPS Coordinates	4501-4507 Wilson Blvd, Arlington, VA 22203 38.87970983 -77.11530274
1.7	3.61	GPS Coordinates	4420 Fairfax Dr, Arlington, VA 22203 38.8815732 -77.11455619


Fairfax Dr
N Glebe Rd
237
120
Two Six Technologie
The Hard Yards
14. 38.8815732
-77.11455619
15. 38.88144159
-77.1140722
Buffalo Wild Wings
Takeout • Delivery
Crafthouse-Arlington
6. 38.88138395
-77.11556851
13. 38.88143724
-77.11478394
7. 38.88139647
-77.11564362
P.F. Chang's
Takeout • Delivery
2. 38.88106083
-77.11533838
4. 38.88093715,
-77.11640596
Virginia Tech -
Alexandria Campus...
N Vermont St
The Westin
Arlington Gateway
4.3 ★ (1331)
4-star hotel
N Wakefield St
1. 38.88055896,
-77.11553561
Nando's Peri-Pe
Takeout • Delive
Willis Towers Watson
Ace
3. 38.88005346
-77.11595332
Mussel Bar & Grille
Takeout • Delivery
Wilson Blv
5. 38.87996816,
-77.11601394
801 N Wakefield St,
Arlington, VA 22203
The Jordan
8. 38.87974703
-77.11598318
12. 38.87969988
-77.11591041
10. 38.87970983
-77.11530274
CVS Pharn
The Waycroft
9. 38.87969022
-77.1154859
Target

Mail Attachment Evidence

Artifact 21: Stamp Insurance 1



NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 25. Armed Forces Reserve	$43,000.00
Lot # 26. Stamp of Kazakstan2	$29,000.00
Lot# 27. BradyCo.	$12,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

Artifact 22: Stamp Insurance 2

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyiStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyiStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

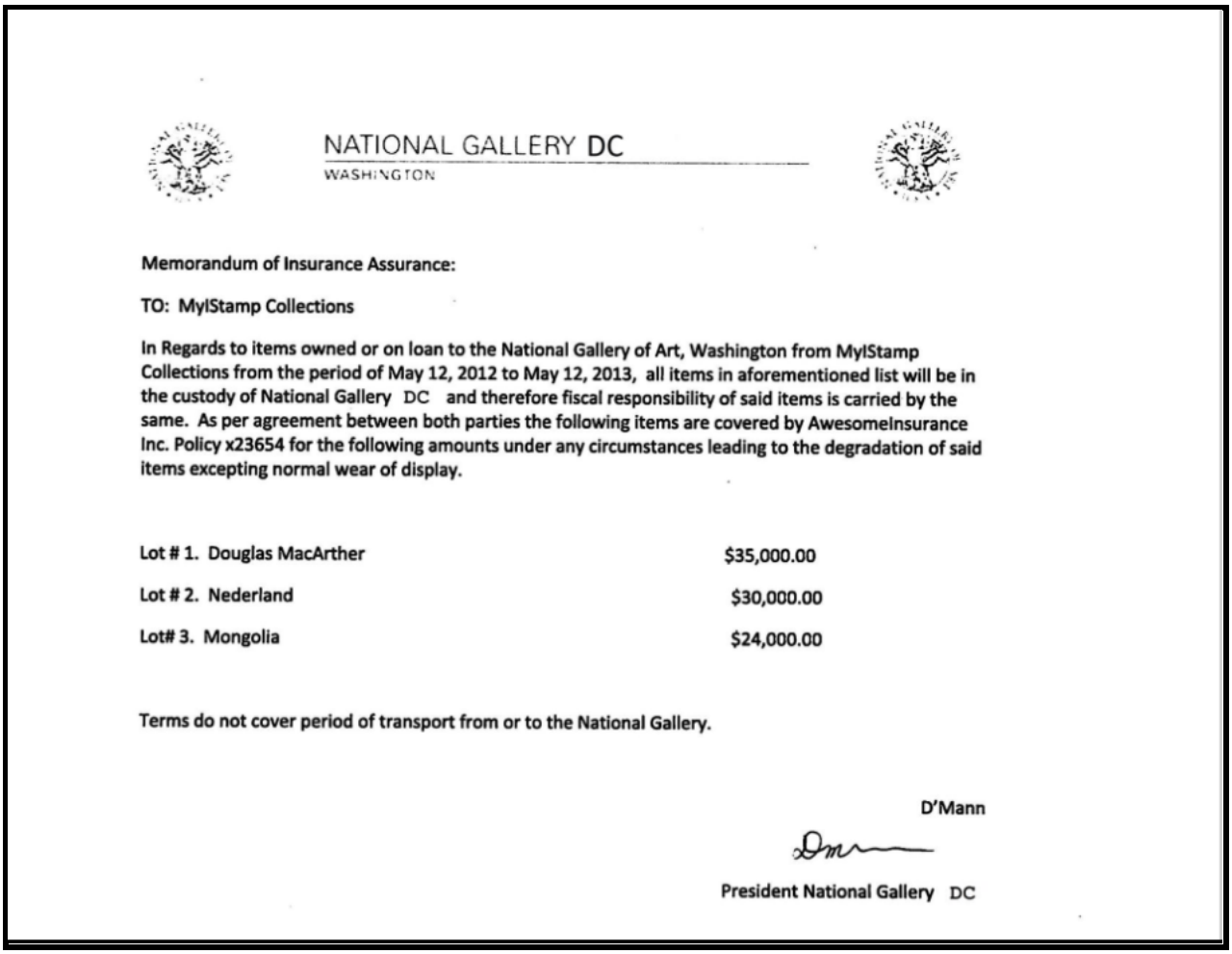
Lot # 11. Woman's Profile	$31,000.00
Lot # 12. Stamp of Kazakstan	$29,000.00
Lot# 13. 1929 Napal	$27,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

Artifact 23: Stamp Insurance 3



NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 1. Douglas MacArther	$35,000.00
Lot # 2. Nederland	$30,000.00
Lot# 3. Mongolia	$24,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

Artifact 24: Suspicious Needs.pdf extracted from Tracy's email attachments.

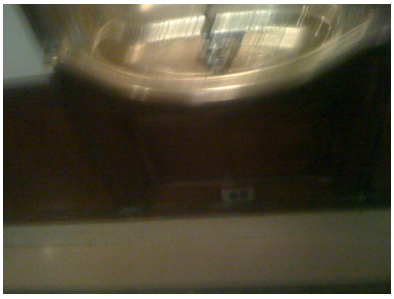
-A rope and javelin (using alternative means to break in)
-tactical turtlenecks (what i will be wearing)
-spray paint (for the cameras)
-vibram five finger shoes (in order to walk silently)
-pack of smokes (detecting lasers)
-smoke grenades (use as a means of escape if caught)

Collection of Photos Found in Tracy's Phone

Name	Path	Photo
IMG_0042.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0043.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0044.JPG	/Mobile/Media/DCIM/100Apple/	

IMG_0045.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0046.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0047.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0048.JPG	/Mobile/Media/DCIM/100Apple/	

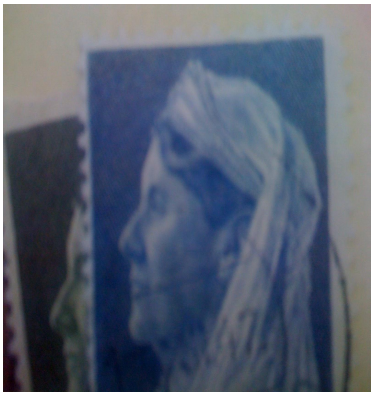
IMG_0049.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0050.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0051.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0052.JPG	/Mobile/Media/DCIM/100Apple/	

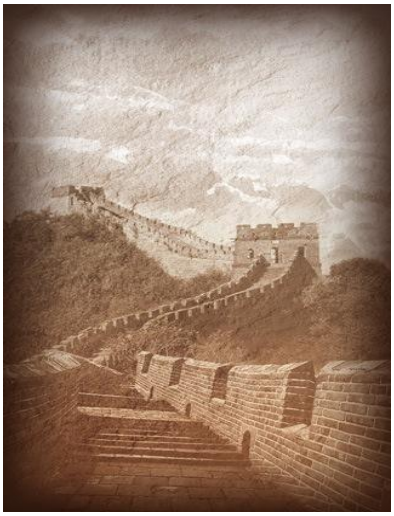
IMG_0053.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0054.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0055.JPG	/Mobile/Media/DCIM/100Apple/	

IMG_0056.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0057.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0058.JPG	/Mobile/Media/DCIM/100Apple/	

IMG_0059.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0060.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0061.JPG	/Mobile/Media/DCIM/100Apple/	

IMG_0062.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0063.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0064.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0065.JPG	/Mobile/Media/DCIM/100Apple/	

IMG_0066.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0067.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0068.JPG	/Mobile/Media/DCIM/100Apple/	
IMG_0069.JPG	/Mobile/Media/DCIM/100Apple/	

IMG_0071.JPG	/Mobile/Media/DCIM/100Apple/	

[Full GPS and SMS message data can be found here.]