Case Report

National Gallery DC

### Tracy’s iPhone 2012-07-15-National-Gallery

Created by:

Cameo Reindl

Mary Yang

Phillip Snell

Abdisalan Firin

Georges Avenie

# Table of Contents

[Case Report](#_8mjg1w2w81ai)

[National Gallery DC](#_lrib8gqk2z7b)

[Tracy’s iPhone [2012-07-15-National-Gallery]](#_219o4hryceis)

[Table of Contents](#_786gzvga2e8h)

[Executive Summary](#_ccs3x82xm1tu)

[Equipment and Tools](#_hw4rzs3hh4tn)

[Details of Tracy’s iPhone](#_ebsdggfieq5h)

[Evidence to Establish Personas](#_qixiazcd0tiw)

[Evidence relating to theft of valuable stamps](#_5ri2s3hfb3bw)

[Evidence relating to defacement of museum art](#_kt32233q8aao)

[Plot Timeline](#_nz1crxu2ypd4)

[Conclusion](#_m5r3zcqmj9ou)

Appendix A: [Correspondence Evidence](#_w4pkinqwxqi8)

Appendix B: [WiFi and GPS Location Information](#_f8fx30pgaw29)

Appendix C: Iphone Photos

# 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. 1. Digitech Inc. found evidence that indicated Tracy was using the alias Coral and Pat was using the alias Perry. 2. Digitech Inc. found evidence that indicated Tracy was motivated by financial gain in planning the stamp heist. 3. Digitech Inc. found evidence of email correspondence to what is believed to be Tracy’s personal email and Pat containing the National Gallery DC stamp letters. 4. Digitech Inc. found evidence indicating Tracy was formulating a plan to steal stamps with her brother Pat. Additionally, Digitech Inc found evidence indicating Tracy knew that Pat was trying to force someone named King to help him with the heist. 5. Digitech Inc. found evidence indicating Tracy helped an individual named Carry for financial gain. The evidence included leaking sensitive security rotation information about the National Gallery to Carry. Furthermore, there is evidence indicating that Tracy helped Carry smuggle a tablet into the Gallery. However, there is evidence indicating that Tracy was unaware of the bigger plan that Carr

### Equipment and Tools

The following tools were used for forensic analysis:

1. Autopsy 4.10.0 2.

2. Google Maps

3. Google Spreadsheets

4. Kali linux

5. Sqlitebrowser

6. Azurelab

# Details of Tracy’s iPhone

# Case Name: 2012-07-15-National-Gallery Case #: 1EZ215-P

Details of Tracy’s iPhone

| **Name** | **Findings** | **Location in iPhone image file** |
| --- | --- | --- |
| Model | iPhone1,2 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelve’s iPhone | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log.1 |
| OS Version | OS-version: iPhone OS 4.2.1 (8c148) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Install Time | 6/6/2012 12:03:28 -0700 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| User Email | [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org)  [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail |
| Phone Number | 1 (703) 340-9661 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log.1 |
| Serial Number | 86004482Y7H | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log.1 |
| IMEI | “InternationalMobileEquipmentIdentity” = “012021003735398” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5//root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095DC3241330462923F6fea5 | root@kali/corpus/trace-phone-md5-original |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | root@kali/corpus/trace-phone-md5-original |

# 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) 340-9661

Personal Email: tracysumtwelve@gmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused

Pat:

Phone Number: 571-308-3236

Email: patsumtwelve@gmail.com

Relationship: trace’s brother

Terry:

Phone Number: 703-829-6071

Email: N/A

Relationship: tracy’s daughter

Joe:

Phone Number: N/A

Email:Joe.sum.twelve@gmail.com

Relationship:Tracy’s soon to be ex-husband

Carry:

Phone Number: 202-725-2124

Email:carrysum2012@yahoo.com

Relationship: Tracy’s acquaintance

King:

Email:throne1966@hotmail.com

Relationship: Pat’s friend who gets blackmailed to the heist.

# Evidence relating to theft of valuable stamps

Tracy plans to steal stamps from the national gallery. Joe, who is Tracy’s soon to be ex-husband, installs a keylogger into Tracy's phone. He discovers the conspiracy and reports it to the police. The phone belongs to Tracy and the email is [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com), and also was found configured for the native mail application on the iphone. The mailbox for her work email which is, [tracey.sumtwelve@nationalgallerydc.org](mailto:tracey.sumtwelve@nationalgallerydc.org) was also configured on the phone.

# Plot Timeline

# Correspondence Evidence Worksheet

### 

| Master Timeline of NGDC | | | | |
| --- | --- | --- | --- | --- |
| Artifact # | Timestamp | Header Information | Key Information | Evidence Location |
| 1 | 6/12/2012 21:25:04 | From: Pat  To: Tracy | What are you up to this weekend? | SMS-Message Data |
| 2 | 6/12/2012  10:04:50 | From: (650) 887-0260  To: Tracy | This call lasted only 20 seconds from data received. | Call-Data |
| 2 | 6/12/2012  20:52:14 | From: (703) 829-6191  To: Tracy | This call lasted 56 seconds as shown on the chart. | Call-Data |
| 2 | 6/13/2012  16:29:13 | From: Tracy  To: Pat | Tracy called Pat but there was no answer. | Call-Data |
| 2 | 6/13/2012 17:30:28 | From: Terry  To: Tracy | I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. | SMS-Message Data |
| 3 | 6/13/2012 18:30:38 | From: Tracy  To: Pat | I don't have any big plans. How about you? | SMS-Message Data |
| 4 | 6/13/2012 18:33:46 | From: Tracy  To: Terry | Ok, sounds good. | SMS-Message Data |
| 5 | 6/19/2012 14:38:59 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Crazydave by the VMs | Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file. | EMAIL-MailBox Data |
| 6 | 6/22/2012  17:34:26 | From: (571) 245-8517  To: Tracy | As you can see on the chart Tracy missed a call from (517)245-8517 | Call-Data  \*failed\* |
| 6 | 7/3/2012 13:41:51 | From: Tracy  To: Terry | Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else? | SMS-Message Data |
| 7 | 7/3/2012 14:04:32 | From: Terry  To: Tracy | moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools :( | SMS-Message Data |
| 8 | 7/5/2012 18:18:23 | From: Carry  To: Tracy | Sounds good let's shoot for one àt Bubba s grill | SMS-Message Data |
| 9 | 7/5/2012 18:20:26 | From: Tracy  To: Carry | Okay that sounds great. See you there | SMS-Message Data |
| 10 | 7/6/2012 11:49:31 | F: patsumtwelve@gmail.com  T: throne1966@hotmail.com  Cc:coralbluetwo@hotmail.com  Subject: can't pass up | Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at national gallery. He also threatens King to comply or else he would put King’s parole in jeopardy. | EMAIL-MailBox Data |
| 11 | 7/6/2012 15:02:19 | From: Tracy  To: Pat | Hey can you give me a call | SMS-Message Data |
| 12 | 7/6/2012 15:08:37 | From: Pat  To: Tracy | Sis I'm really busy can we can do this later | SMS-Message Data |
| 13 | 7/6/2012 15:11:54 | From: Tracy  To: Pat | No pat this is important I need you to call me soon | SMS-Message Data |
| 14 | 7/6/2012 15:13:31 | From: Pat  To: Tracy | Ok ok I'll call in 5 | SMS-Message Data |
|  | 7/6/2012  15:18:50 | From: Pat  To: Tracy | Pat calls Tracy and as you can see from the data they spoke for approximately 4 minutes and 4 seconds. | Call-Data |
| 15 | 7/6/2012 16:27:16 | From: Carry  To: Tracy | I have a table inside | SMS-Message Data |
| 16 | 7/6/2012 16:27:50 | From: Tracy  To: Carry | Okay brt | SMS-Message Data |
| 17 | 7/7/2012 19:36:35 |  | Congratulations, your entry in last months drawing won you a FREE $1,000 Target Giftcard! Enter "703" at www.target.com.trdt.biz to tell us where to ship it | SMS-Message Data |
| 18 | 7/9/2012 10:44:11 | F: tracysumtwelve@gmail.com  T: 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. | EMAIL-MailBox Data |
| 19 | 7/10/2012 11:19:00 | F: patsumtwelve@gmail.com  T: 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. | EMAIL-MailBox Data |
| 20 | 7/10/2012 15:26:19 | From: Pat  To:Tracy | hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know | SMS-Message Data |
| 21 | 7/10/2012 15:58:04 | From: Tracy  To: Pat | Sure thing I'll get on it | SMS-Message Data |
| 22 | 7/10/2012 16:37:09 | From:Tracy  To: Pat  \*Message failed\* | <?xml version="1.0" encoding="UTF-8"?>  <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">  <plist version="1.0">  <array>  <string>+15713083236</string>  </array>  </plist> | SMS-MMS-Message Data |
| 23 | 7/10/2012 17:18:38 | From: Tracy  To: Terry | Going to lunch. You want to go????! | SMS-Message Data |
| 24 | 7/10/2012 18:19:24 | From: Tracy  To: Terry | Back at work | SMS-Message Data |
| 25 | 7/10/2012 18:58:24 | From: Terry  To: Tracy | I'm busy. Maybe this weekend if dad isn't busy | SMS-Message Data |
| 26 | 7/11/2012 12:41:45 | From: Carry  To: Tracy | I'm almost there where should I meet you? | SMS-Message Data |
| 27 | 7/11/2012 12:49:08 | From: Tracy  To: Carry | Just meet me out front, I'll take the tablet in. | SMS-Message Data |
| 28 | 7/12/2012 17:06:45 | From: Tracy  To: Carry | How's the flashmob going | SMS-Message Data |
| 29 | 7/13/2012 1:02:10 | From: Terry  To: Tracy | I really want to go to Dad's this weekend. He said he'll take me shopping for school | SMS-Message Data |

### 

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

● Tracy was using the alias Coral and Pat was using the alias Perry

● Tracy’s prime motive was financial gain for planning the stamp heist.

● Tracy emailed National Gallery DC stamp letters to her personal email account and to Pat

● Tracy formulated a plan with Pat to steal stamps

● Tracy knew that Pat was trying to blackmail someone named King to help with the heist.

● Tracy helped Carry also, for financial gain.

● Tracy leaked sensitive security rotation information about the National gallery to Carry.

● Tracy helped Carry smuggle a tablet into the Gallery.

● Tracy did not know about the bigger plan that Carry had in mind

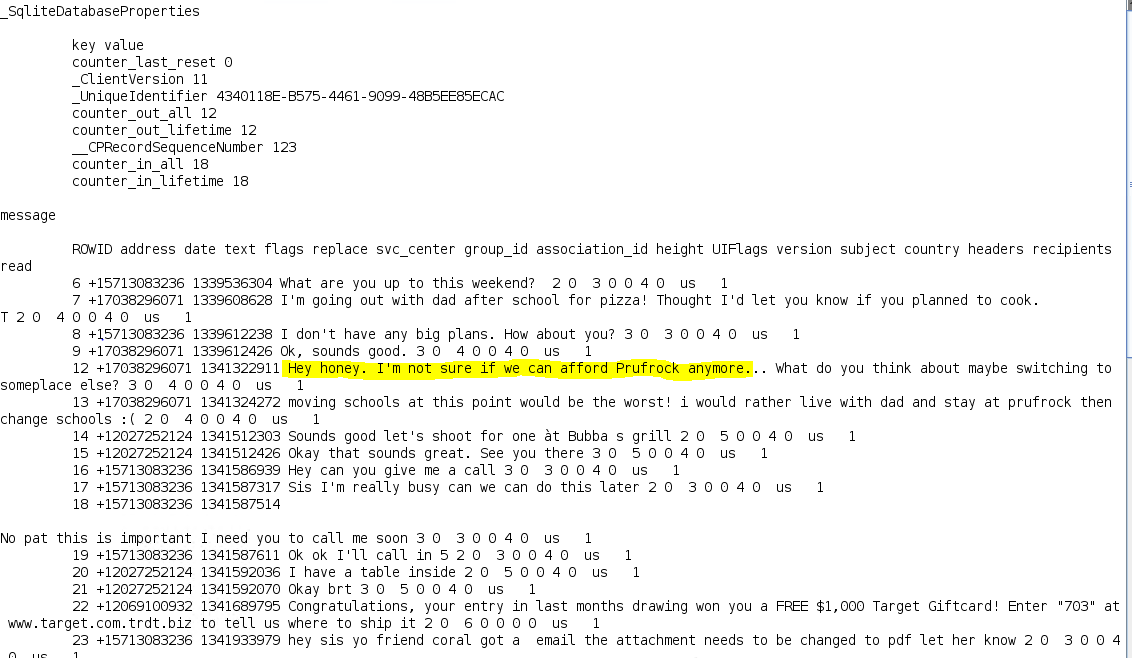
# Appendix A: Correspondence Evidence

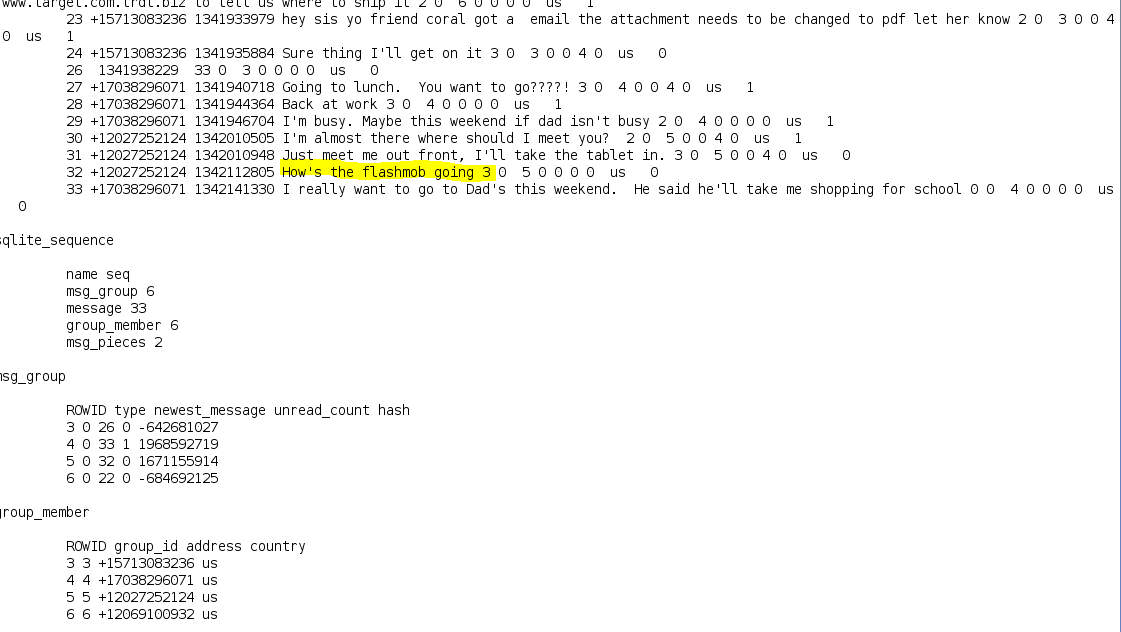
This subsection will provide an amalgamation of the email and SMS corresponce evidence. SMS: Information on SMS conversations recorded on the phone was found at

“/mobile/Library/SMS/sms.db”

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

Screenshots here for the sms.db





# 

# Location Information Worksheet

### 

| Location Information (cell location) | | |
| --- | --- | --- |
| Timestamp | Relative Path | Map Screenshot |
| 2012-6-13 19:01:21 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-02 16:19:23 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-05 16:32:46 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-10 16:31:10 | root/Library/Caches/locationd/consolidated.db |  |

### 

| Location Information (Wifi location) | | |
| --- | --- | --- |
| Timestamp | Relative path | Map Screenshot |
| 2012-06-13 19:01:22 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-02 16:19:24 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-03 13:42:42 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-03 13:42:42 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-05 16:32:47 | root/Library/Caches/locationd/consolidated.db |  |
| 2012-07-10 16:31:12 | root/Library/Caches/locationd/consolidated.db |  |

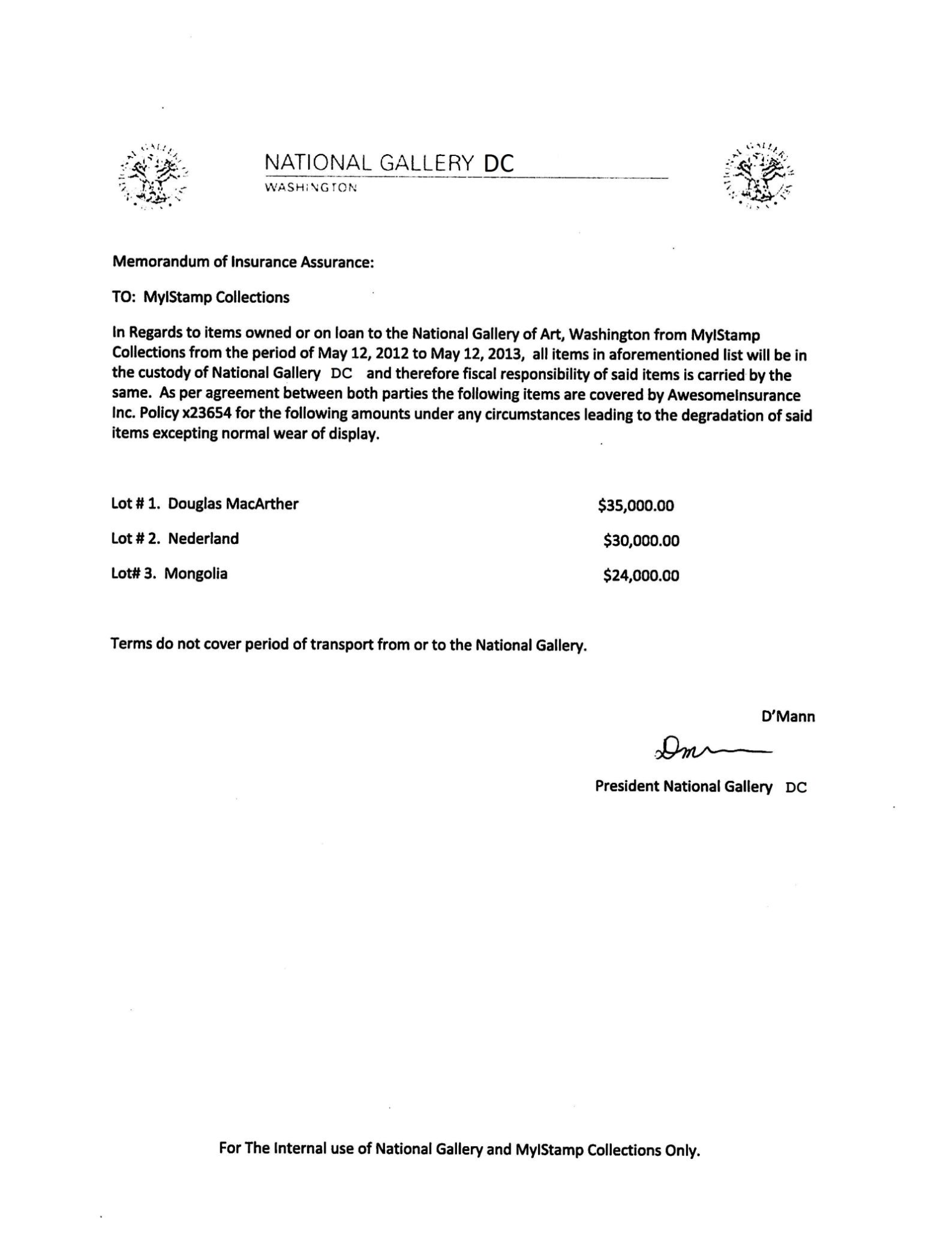
### 

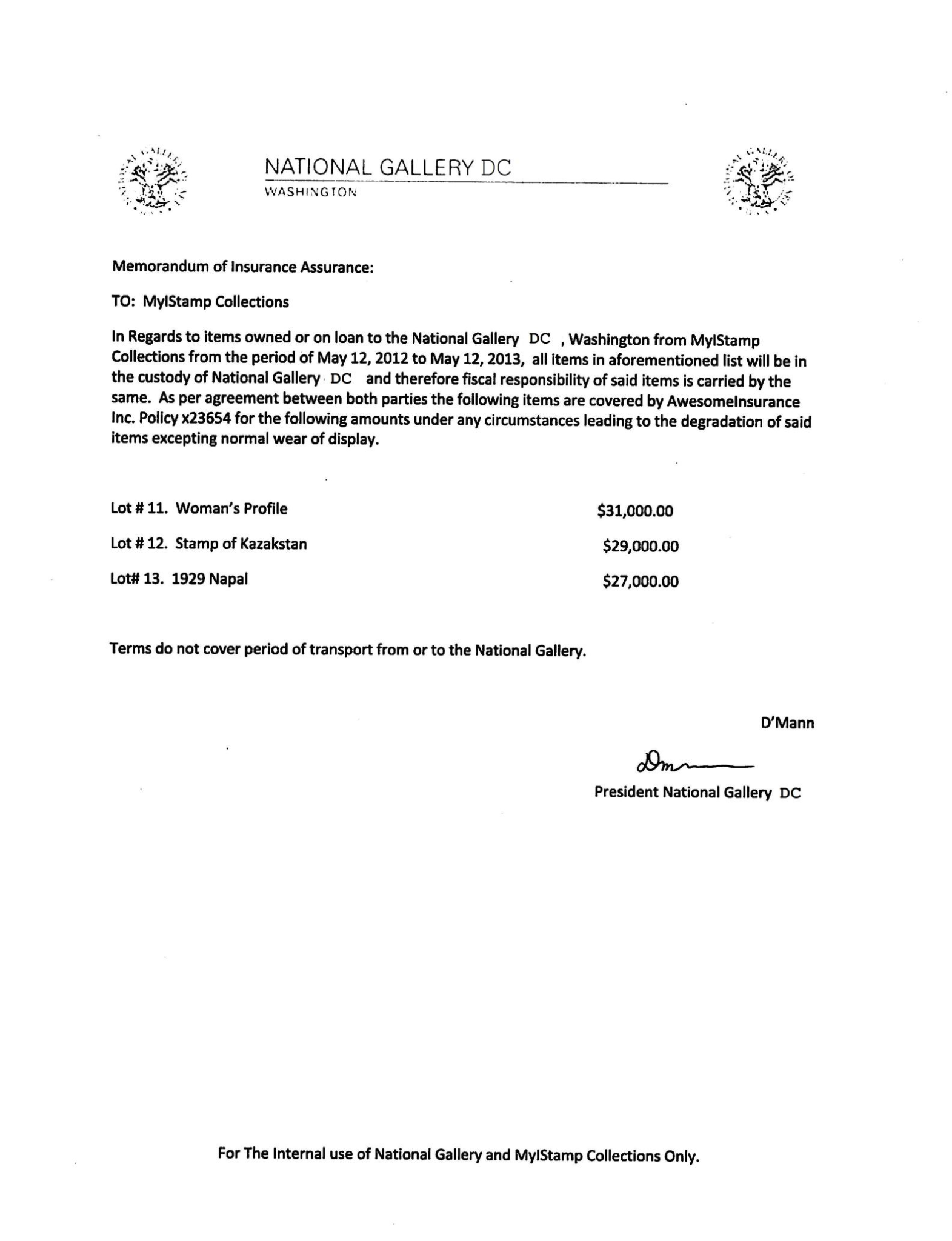
# Appendix B: Stamp Insurance Documents

We see the value of the stamps in the email attachment of Tracy and the pictures of the stamps on Tracy’s Iphone.

# 

# 





# Appendix C: Iphone Photos

# Case Name: 2012-07-15-National-Gallery Case #: 1EZ215-P

## 33 photos taken by Tracy's phone around the National Gallery.

On dates 2012-07-08 and 2012-07-11, evidence shows random pictures and pictures of some of the stamps they were attempting to steal.

## Details of Tracy’s iPhone

| **Name** | **Findings** | **Location in iPhone image file** |
| --- | --- | --- |
| IMG\_0042.JPG  2012-07-08  12:33:37 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0043.JPG  2012-07-08  12:34:31 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0044.JPG  2012-07-08  12:34:50 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0045.JPG  2012-07-08  12:35:50 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0046.JPG  2012-07-08  12:36:30 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0047.JPG  2012-07-08  12:37:16 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0049.JPG  2012-07-08  12:37:37 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0048.JPG  2012-07-08  12:41:41 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0050.JPG  2012-07-08  12:41:53 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0051.JPG  2012-07-08  12:42:03 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0052.JPG  2012-07-08  12:42:48 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0053.JPG  2012-07-08  12:44:13 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0054.JPG  2012-07-08  12:49:25 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0056.JPG  2012-07-08  12:49:37 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| ING\_0055.JPG  2012-07-08  12:49:49 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0057.JPG  2012-07-08  12:50:07 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0058.JPG  2012-07-08  12:50:20 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0059.JPG  2012-07-08  12:50:34 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0060.JPG  2012-07-08  12:50:50 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0061.JPG  2012-07-08  12:50:53 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0062.JPG  2012-07-08  12:51:03 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0063.JPG  2012-07-08  12:51:14 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0064.JPG  2012-07-08  12:51:44 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0065.JPG  2012-07-08  12:59:55 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0066.JPG  2012-07-08  01:00:01 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0067.JPG  2012-07-08  01:00:08 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0068.JPG  2012-07-08  01:00:12 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0069.JPG  2012-07-08  01:00:23 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0070.JPG  2012-07-08  01:02:23 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |
| IMG\_0071.JPG  2012-07-11  12:18:48 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/MOBILE/MEDIA/DCIM/100APPLE/ |