Case Report

National Gallery DC

### **Tracy’s iPhone [2012-07-15-National-Gallery] by Julie Haynes**

# Table of Contents

[Case Report](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.8mjg1w2w81ai)

[National Gallery DC](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.lrib8gqk2z7b)

[Tracy’s iPhone [2012-07-15-National-Gallery]](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.219o4hryceis)

[Table of Contents](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.786gzvga2e8h)

[Executive Summary](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.ccs3x82xm1tu)

[Equipment and Tools](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.hw4rzs3hh4tn)

[Details of Tracy’s iPhone](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.ebsdggfieq5h)

[Evidence to Establish Personas](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.qixiazcd0tiw)

[Evidence relating to theft of valuable stamps](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.5ri2s3hfb3bw)

[Evidence relating to defacement of museum art](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.kt32233q8aao)

[Plot Timeline](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.nz1crxu2ypd4)

[Conclusion](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.m5r3zcqmj9ou)

Appendix A: [Correspondence Evidence](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.w4pkinqwxqi8)

Appendix B: [WiFi and GPS Location Information](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.f8fx30pgaw29)

Appendix C: [Files](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.f8fx30pgaw29) in EMail

Appendix D: [Emails](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.f8fx30pgaw29) from Tracy’s MacBook

# Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

* Tracy is a suspect in the aforementioned conspiracy.
* As part of the investigation, Tracy’s iPhone was taken into custody.
* Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

* **Tracy** is divorced woman who works at National Gallery. She unknowingly is used by Carry (Cat) to allow a group to enter the National Museum under the guise of a flash mob but their real goal is defacement of foreign artwork. She needs money to pay for her daughter’s private school and engages in researching the value of stamps that can be stolen from the National Gallery. Tracy also uses the alias of Coral Blue.
* **Joe** is the ex-husband of Terry. He is financially well-off and bitter about the divorce. Joe installed a keylogger on Tracy’s MacBook laptop before the divorce – some of the files are included in appendix D, although they may not be admissible.
* **Terry** is the 15 year old daughter of Tracy and Joe. Terry currently attends an expensive private school that Tracy can no longer afford to pay for since her divorce. Terry would rather live with her Dad instead of her Mom if necessary to stay at her private school.
* **Carry** is an acquaintance of Tracy. She is tech-savvy and knows how to use social media. She is also a Krasnovian supporter in the US and appears to use Tracy as a connection to get into the National Gallery under the guise of hosting a flashmob when she is actually defacing foreign artwork in order to cause embarrassment to the U.S. Carry also uses the alias of Cat.
* **Perry** is Tracy's brother. He is corrupt police detective with D.C. Enforcers Bureau and is willing to help his sister even if it requires illegal activity. He enlists a parolee to break into the National Gallery. Perry also uses the alias of Pat
* **King** is a parolee who is used by Perry to break in to the National Gallery. King also uses the alias ofKart.

### **Equipment and Tools**

* Autopsy
* SQLite
* Kali Linux CLI

# Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone 1,2 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/AppleSupport/general.log  /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Media/DCIM/100APPLE/IMG\_0042.JPG |
| Host Name | Tracy Sumtwelve’s iphone | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log.1 |
| OS Version | iPhone OS 4.2.1(8C148) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/AppleSupport/general.log |
| Install Time | 2012-06-06 12:03:28 -0700 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/AddressBook.sqlitedb  /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| User Email | [tracysumtwelve@gmail.com@imap.gmail.com](mailto:tracysumtwelve@gmail.com@imap.gmail.com)  [tracysumtwelve@nationalgallerydc.org@ppod51018.outlook.com](mailto:tracysumtwelve@nationalgallerydc.org@ppod51018.outlook.com)  [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/AddressBook.sqlitedb  /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail/Envelope Index |
| Phone Number | 1-703-340-9661 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/AddressBook.sqlitedb |
| Serial Number | 86004482Y7H | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/AppleSupport/general.log |
| ICCID | 8901410355195342366 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log |
| IMEI | 012021003735398 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Media/DCIM/100APPLE/IMG\_0042.JPG |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 |  |

# Evidence to Establish Personas

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

Tracy, alias CoralBlue:

Phone Number: (703) 340-9961

Personal Email: tracysumtwelve@gmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused

Perry, alias Pat:

Phone Number:  571-308-3286

Email: patsumtwelve@gmail.com

Relationship: Brother of accused

Terry:

Phone Number:  703-829-6071

Email:

Relationship: Daughter of accused

Joe:

Phone Number:

Email:

Relationship: Ex-husband of accused

Carry, alias Kat:

Phone Number:  202-725-2124

Email: [carrysum2012@yahoo.com](mailto:carrysum2012@yahoo.com),

Relationship: Acquaintance of accused

Awen

Phone Number:

Email: [Awen.Throsam@m57.biz](mailto:Awen.Throsam@m57.biz)

Relationship: TBD

# 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.

* Artifact ID 9223372036854766317: Email on 6/9/2012 from Tracy’s work email to her personal email containing PDF attachments with information about stamp insurance.
* Artifact ID 9223372036854766317: Emails on 6/10/2012 from Perry enlisting King to perform a break-in, a copy of the same email from Perry to Tracy, and a reply from King agreeing to break in along with a request for supplies listed in a needs.txt file.
* Artifact ID 9223372036854774734: Text messages between Tracy and Perry discussing the stamp insurance PDF documents.

# 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.

* Artifact ID 9223372036854774734: Text messages between Tracy and Carry discussing a tablet that Carry gives to Tracy and discussing the flash mob.

# Plot Timeline

Note: Converted date timestamps to dates at: <https://www.timestampconvert.com/>

|  |  |
| --- | --- |
| **TIMESTAMP** | **EVENT** |
| 6/9/2012 10:44 EST | Email Tracy sent email containing 3 PDF stamp insurance documents to her coralbluetwo email address. |
| 6/10/2012 10:49 AM EST | Perry sent King an email telling him that he had a job for him. |
| 6/10/2012 12:24:57 EST | Perry forwarded the email he had just sent to King to his sister, Tracy. |
| 6/10/2012 11:19 AM EST | King replied to Perry and said he would do the job. He also included a “needs.txt” file containing a list of items needed to do the job. |
| 6/12/2012 4:04 PM EST | Call to 650-887-0260 |
| 6/12/2012 4:52 PM EST | Call to daughter, Terry, at 703-829-6191 |
| 6/13/2012 12:29 PM EST | Call to brother, Perry, at 571-308-3236 |
| 6/22/2012 1:34 PM EST | Call to 571-245-8517 |
| 7/3/2012 9:41 AM EST | Text from Tracy to daughter “Hey honey. I’m not sure if we can afford Prufrock anymore… What do you think about maybe switching to someplace else?” |
| 7/3/2012 10:04 AM EST | Text from daughter “moving schools at this point would be the worst! I would rather live with dad and stay at Prufrock than change schools ☹” |
| 7/6/2012 11:18 AM EST | Call to brother, Perry, at 571-308-3236 |
| 7/10/2012 11:26 AM EST | Text from Perry (Pat) to Tracy “hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know.” |
| 7/10/2012 11:58 AM EST | Text from Tracy to Perry (Pat) “sure thing I’ll let her know.” |
| 7/11/2012 8:41 AM EST | Text from Carry at 202-725-2124 “I’m almost there where should I meet you?” |
| 7/11/2012 8:49 AM EST | Text to Carry at 02-725-2124 “just meet me out front, I’ll take the tablet in.” |
| 7/12/2012 1:06 PM EST | Text to or from Carry 202-725-2124 “How’s the flashmob going” |
|  |  |

# Conclusion

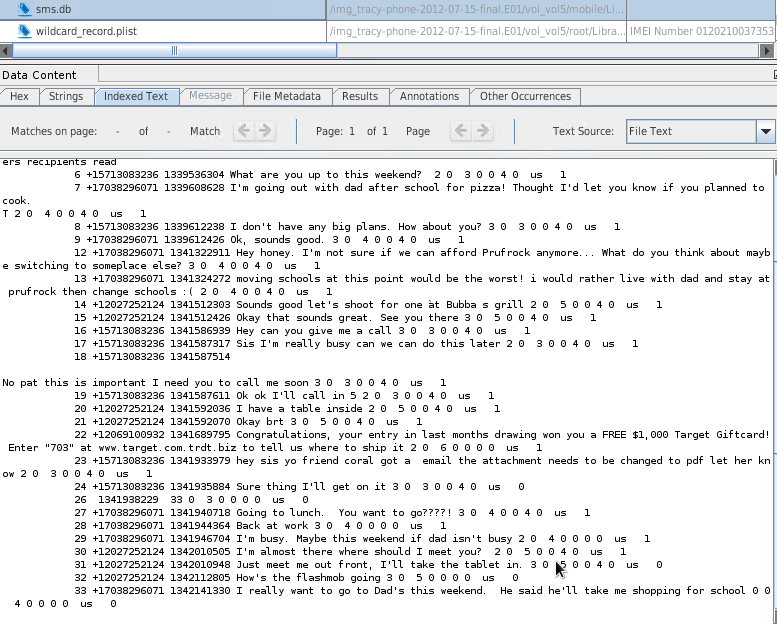
Evidence found on Tracy’s iPhone indicated the following:

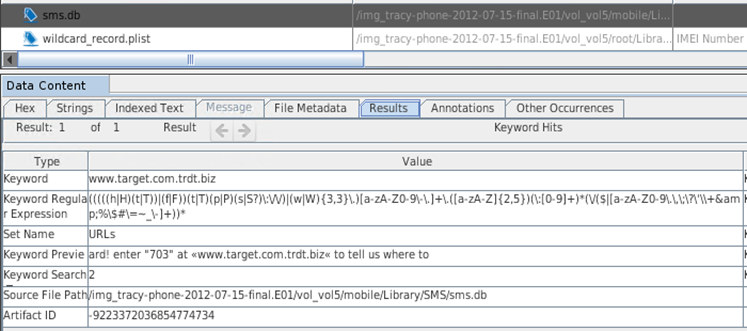
* Tracy used the alias Coral Blue to send copies of the stamp insurance PDF documents to herself.
* Perry used the alias Pat to send text messages to Tracy’s alias to discuss the PDF documents.
* Perry used the alias Pat to send a copy of the email enlisting King for the break-in to Tracy’s alias Coral Blue.
* mail on 6/9/2012 from Tracy’s work email to her personal email containing PDF attachments with information about stamp insurance.
* Tracy agreed to take a tablet in to the National Gallery for Carry and possibly agreed to help her gain entrance for a flash mob.

# Appendix A: Correspondence Evidence

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Master Timeline of NGDC | | | | |
| Artifact # | Timestamp | Header Information | Key Information | Evidence Location |
|  | 6/5/2012 3:58 PM EST | From: [Woina.Honril@m57.biz](mailto:Woina.Honril@m57.biz) sender IP is 208.97.132.83  To: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com)  Subject: Busy | Contains the 000002.doc attachment that contained information on euthanizing four animals with BSE | 43149-INBOX.mbox/Attachments/63/3/000002.doc  Ls |
| 9223372036854766317 | 6/9/2012 10:44 EST | Email from [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  Subject: things  To: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | Contained the documents.zip file which contains the 3 PDF files about the Stamp insurance. | 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx |
|  | 6/10/2012 10:49 AM EST | Email from [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  To [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  Cc [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | Content:  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 paroles, the feds won’t need a search warrant. Well hit me up. You know where to find me. | 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx |
|  | 6/10/2012 12:24:57 EST | Email from PatTeeSumTwelve ([patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com))  Subject Fwd: can’t pass up  To: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | (Forwarded previous email message to Tracy) | 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx |
|  | 6/10/2012 11:19 AM EST | Email from King kthings [throne1966@hotmail.com](mailto:throne1966@hotmail.com)  To [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  Subject: RE: can’t pass up | Content:  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  Needs.txt:  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) |  |
|  | 6/12/2012 4:04 PM EST | Call to 650-887-0260 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/wireless/Library?CallHistory/call\_history.db |
|  | 6/12/2012 4:52 PM EST | Call to 703-829-6191 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/wireless/Library?CallHistory/call\_history.db |
|  | 6/13/2012 12:29 PM EST | Call to 1-571-308-3236 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/wireless/Library?CallHistory/call\_history.db |
|  | 6/22/2012 1:34 PM EST | Call to 571-245-8517 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/wireless/Library?CallHistory/call\_history.db |
| 9223372036854774734 | 7/3/2012 9:41 AM EST | Text to 703-829-6071 | Text from Tracy to daughter “Hey honey. I’m not sure if we can afford Prufrock anymore… What do you think about maybe switching to someplace else?” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |
| 9223372036854774734 | 7/3/2012 10:04 AM EST | Text from 703-829-6071 | Text from daughter “moving schools at this point would be the worst! I would rather live with dad and stay at Prufrock than change schools ☹” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |
|  | 7/6/2012 11:18 AM EST | Call to 571-308-3236 |  | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/wireless/Library?CallHistory/call\_history.db |
| 9223372036854774734 | 7/10/2012 11:26 AM EST | Text from 571-308-3286 | Text from Pat to Tracy “hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know.” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |
| 9223372036854774734 | 7/10/2012 11:58 AM EST | Text to 571-308-3286 | Text from Tracy to Pat “sure thing I’ll let her know.” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |
| 9223372036854774734 | 7/11/2012 8:41 AM EST | Text from 202-725-2124 | Text from Carry: “I’m almost there where should I meet you?” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |
| 9223372036854774734 | 7/11/2012 8:49 AM EST | Text to 202-725-2124 | Text from Tracy to Carry “just meet me out front, I’ll take the tablet in.” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |
| 9223372036854774734 | 7/12/2012 1:06 PM EST | Text to/from? 202-725-2124” | Text between Tracy and Carry: “How’s the flashmob going” | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/SMS/sms.db |

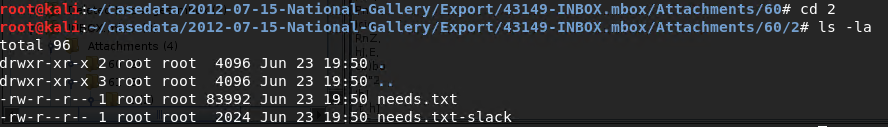


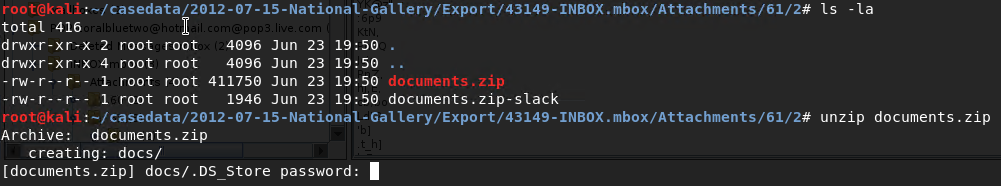


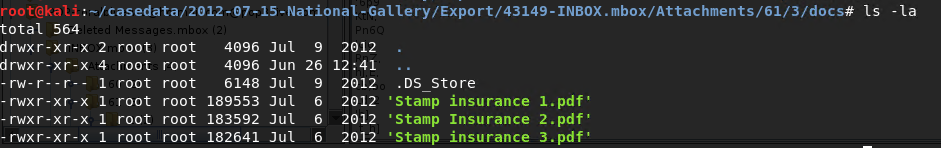
# Appendix B: WiFi and GPS Location Information

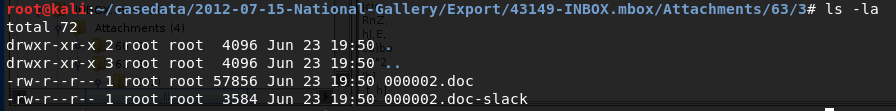
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location Information | | | | |
| Artifact # | Timestamp | Header Information | Body | Map Screenshot |
|  |  | 44:1e:a1:f4:d:7f |  |  |
|  |  | 0:18:39:fb:4f:bd | 38.88063263,-77.11677783 |  |
|  |  | B8:9b:c9:22:a:6b | 38.82789164,-77.08565932 |  |
|  |  |  |  |  |

# Appendix C – Files in Email

**Needs.txt**

**Stamp Insurance Documents**



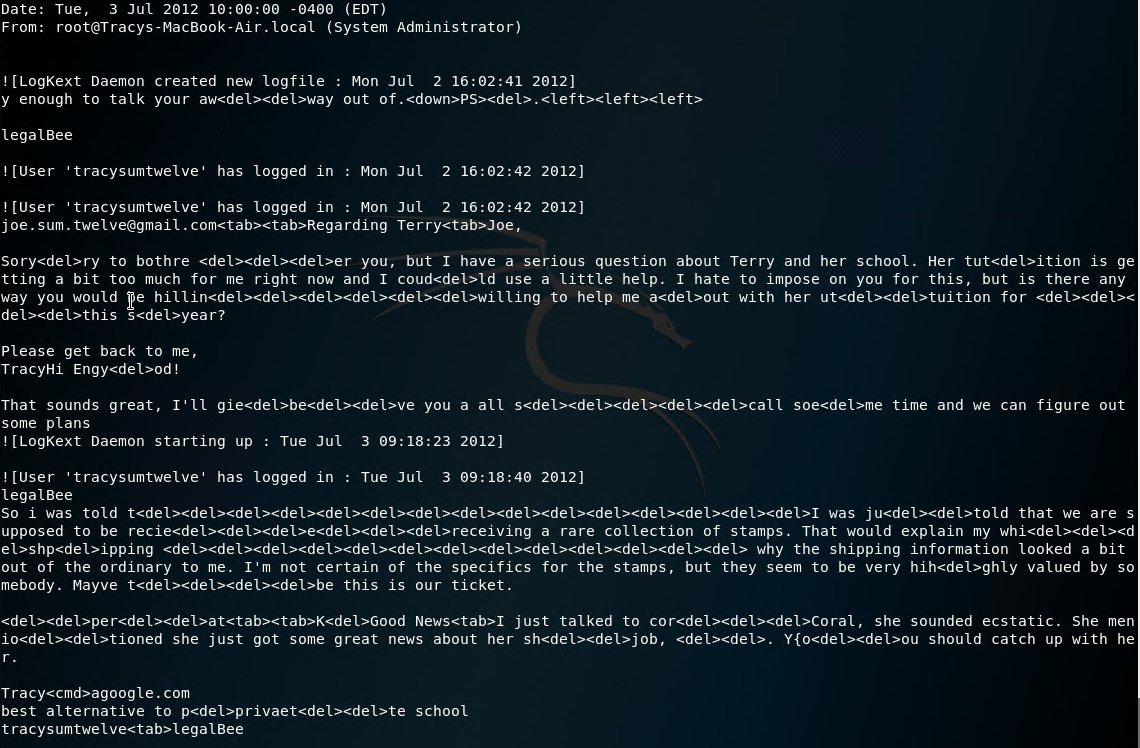
**Unidentified Docume**nt

# Appendix D – Emails from Tracy’s MacBook – Admissibility not Determined

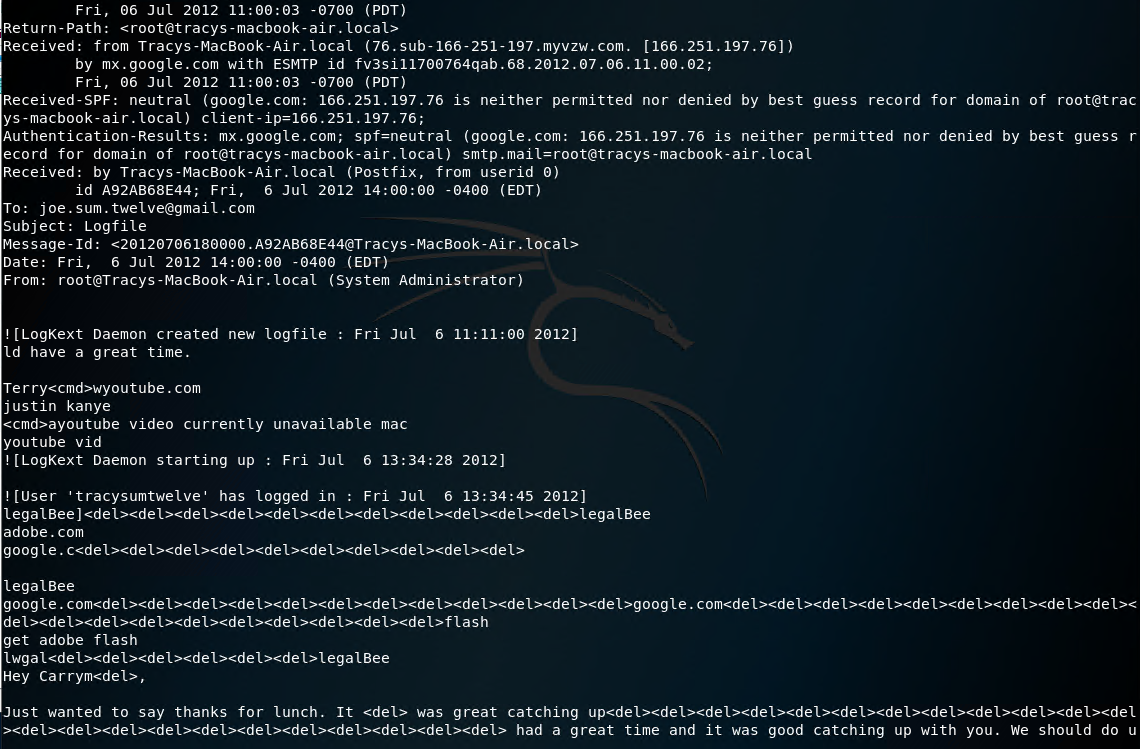
**EMAILS from Tracy’s MacBook**

6/29/2012 11:00 AM EST from Tracy (coralbluetwo@hotmail.com) to joe.sum.twelve.gmail.com discussing insurance documents that place value on certain objects.

7/3/2012 09:18 AM EST from Tracy discussing receipt of a rare collection of stamps and stating “this is our ticket”



7/6/2012 6:13 AM/PM? from Tracy to Carry saying “thanks for lunch”.



7/9/2012 09:14 AM/PM? from Tracy to Perry stating that “Here are those documents I talked to you about. The password is your old dog’s name.”

07/10/2012 09:15 AM/PM? From Tracy stating that she can “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?”.

