### 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.

* SMS correspondence corroborating the communication between the involved subjects.
* Emails corroborated through the needs.txt explained the Modus Operandi on how they are going to break in, what they will be wearing, how to walk silently, detecting lasers, use as a means of escape if caught.
* The email established the timeline for when the group was going to commit the heist at the National Galley on July, 20th 2012.

### **Equipment and Tools:**

The tools used to gather and collect the evidence from Tray’s phone was Autopsy 4.10.0, the kali terminal window and nano was used to view text content.

# 

# **Details of Tracy’s iPhone:**

# iPhone Forensic Image: Important Databases and Files

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iphone 1, 2 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelves iPhone | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/preferences/SystemConfiiguration/preferences.plist |
| OS Version | Version 3, 4.2.1 (8C148) | img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/AppleSupport |
| Install Time | 06/06/12012 12:03 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| User Email | [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  [tracysumtwelve@](mailto:tracysumtwelve@gmail.com)nationalgallerydc.org@pod51018.outlook.com  [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | img\_tracy-phone-2012-07-15-final.E01/vol\_vol5//$CarvedFiles  img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile.Library/Mail |
| Phone Number | (703) 340-9661 | img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log |
| Serial Number | 86004482Y7H | img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/AppleSupport |
| ICCID | 89014103255195342366 | img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log |
| IMEI | 01021003735398 | mg\_tracy-phone-2012-07-15-final.E01/vol\_vol4/usr/libexec/lockdownd |
| MD5 Hash | cde7ae3ac48c0345e9a1988b |  |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 |  |

Some of the following information is from *iPhone Forensics* by Jonathan Zdziarski. Published by O'Reilly Media, Inc., 2008.

The following contains a description of the major files and how to access them in Autopsy.

# **Evidence to Establish Person’s:**

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

**Tracy:**

Phone Number: (703) 340-9961

Personal Email: tracysumtwelve@gmail.com

Work Email: [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org)

coralbluetwo@hotmail.com

Relationship: Suspect

**Pat:**

Phone Number: 15713083236

Email: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)

[perrypatsum@yahoo.com](mailto:perrypatsum@yahoo.com)

Relationship: Brother

**Terry:**

Phone Number: 17038296071

Email:

Relationship: Daughter

**Joe:**

Phone Number:

Email: joe.sum.twelve@gmail.com

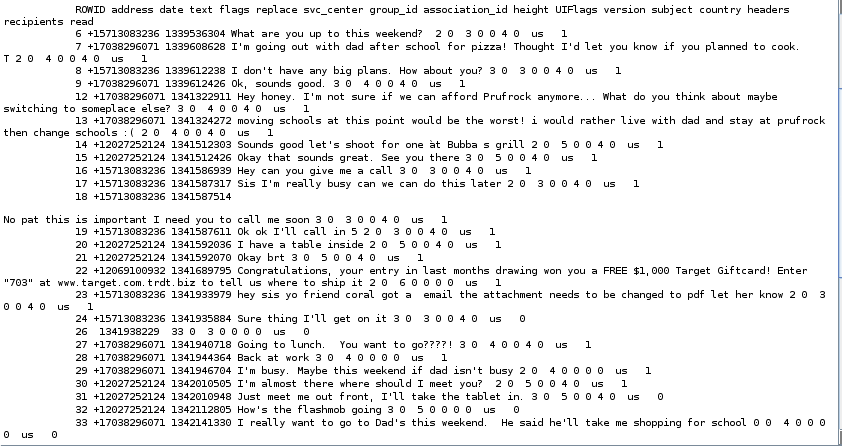
Relationship: Ex Husband

**Carry:**

Phone Number: 12027252124

Email: carrysum2012@yahoo.com

Relationship: Alex’s contact used to contact Tracy

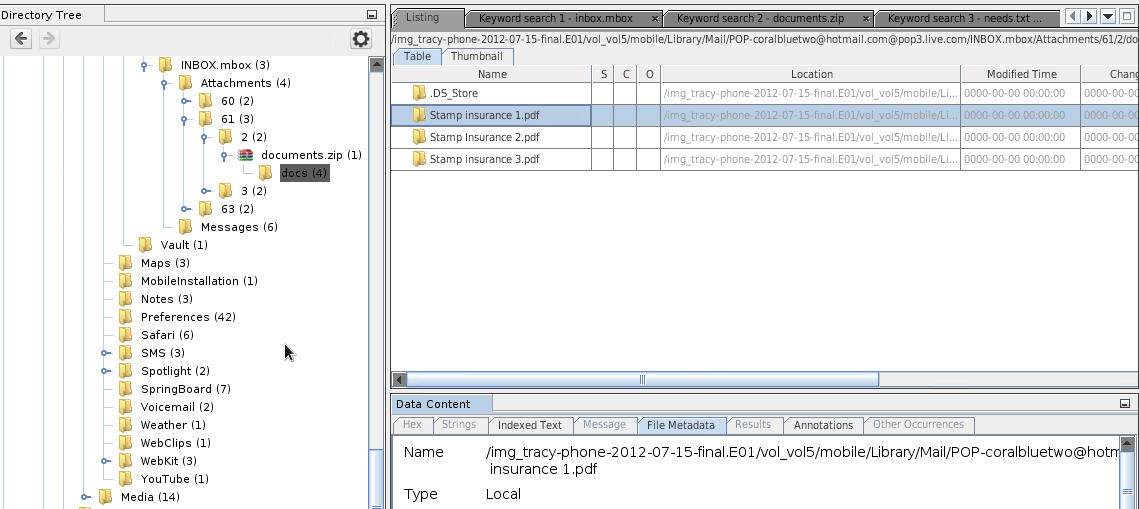
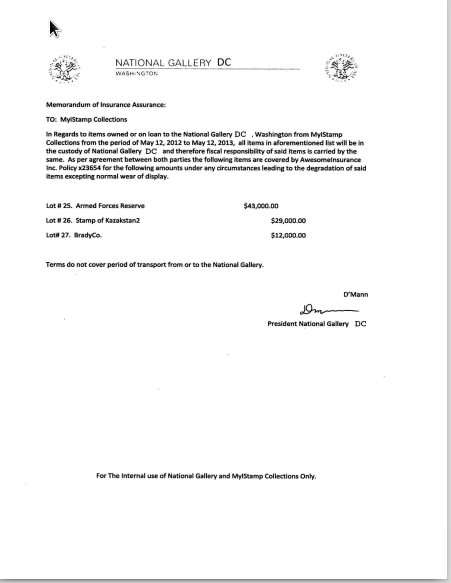
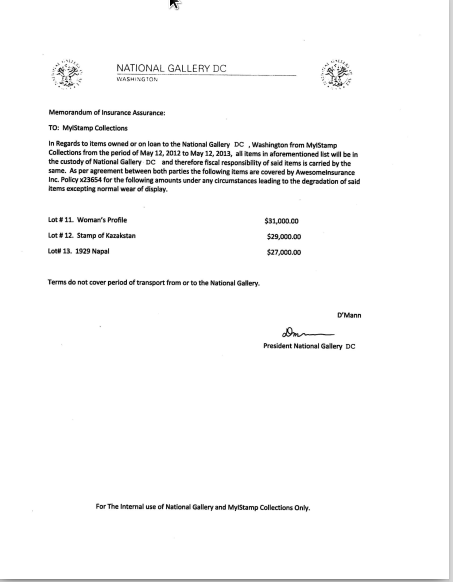


In these text messages we can see Tracy admitting to terry that she can’t afford to pay for her tuition at prufrock. Also we can see Alex’s contact Carry messaging to ask Tracy about the flashmob that was organized at the National Gallery. We can also see Pat requesting tracy to change some email attachments to pdf format most likely the stamp insurance documents.

# **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.

We were able to find email evidence of Tracy emailing herself insurance information on 3 different stamps compressed into a zipped document called documents.zip



# 

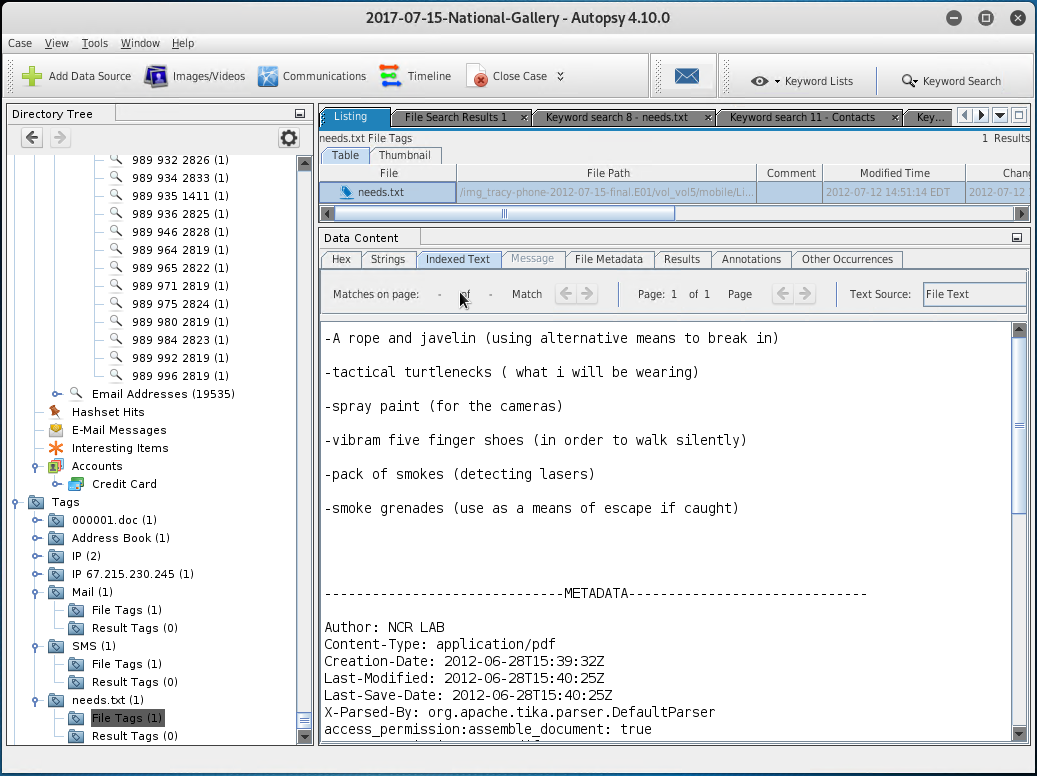
# 



# 

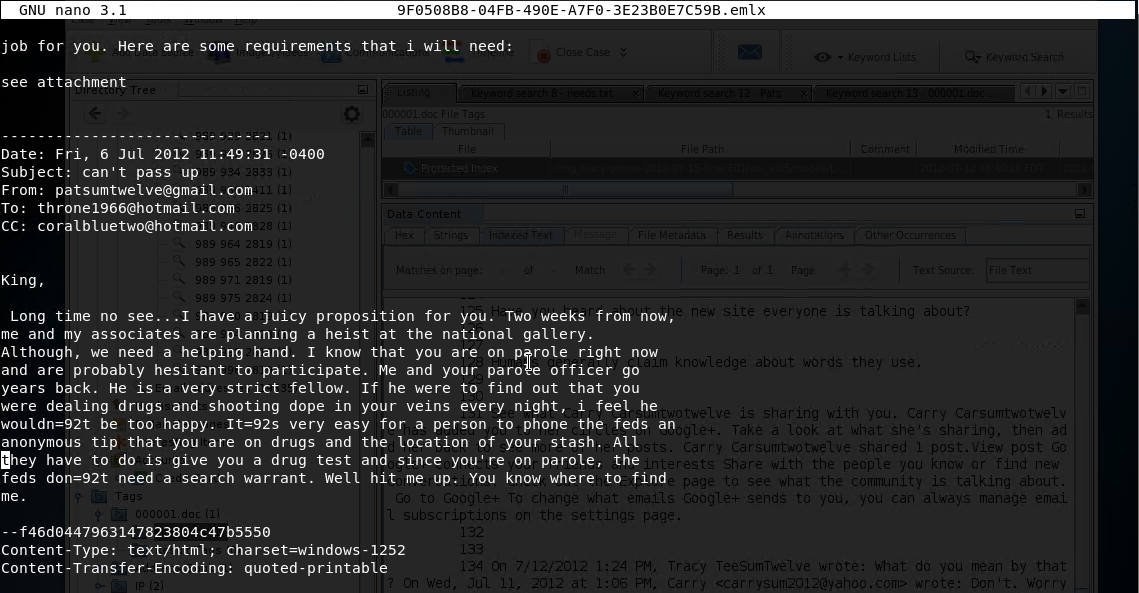
# **Evidence relating to defacement of museum art:**

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.



The needs.txt explains the Modus Operandi on how they are going to break in, what they will be wearing, how to walk silently, detecting lasers, use of a means of escape if caught.

# **Plot Timeline:**



On Friday, July 6th 2012 [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com) wrote an email to [throne1966@hotmail.com](mailto:throne1966@hotmail.com) and [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) indicating “Two weeks from now, me and my associates are planning a heist at the national gallery.

The timeline for the national gallery heist would be conducted on Friday, July 20th 2012

# **Conclusion:**

Evidence found on Tracy’s iPhone indicated the following:

* We have come to the conclusion that we have enough evidence to connect Tracy, Pat, and Carry with the National Gallery Heist. We can tie Tracy to Carry using their text messaging history, where Carry asks Tracy how the flash mob that was used as a distraction was going. Also in the emails we can see Pat under the alias Perry emailing Tracy under the alias Coral, details to install and use a virtual machine hidden in a mp3 file. We also have email evidence of Pat contacting King at [throne1966@hotmail.com](mailto:throne1966@hotmail.com) to organize and do the groundwork of the heist, which Tracy ( Coral) was CC'd on
* We have found that Tracy was using the alias Coral and Pat was using the alias Perry to communicate with each other and Carry. More information can be found in the emails from King ([throne1966@hotmail.com](mailto:throne1966@hotmail.com)) requesting a list of items that he would need to pull off the heist under needs.txt

# **Appendix A: Correspondence Evidence:**

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

### 

|  |  |  |  |
| --- | --- | --- | --- |
| Master Timeline of NGDC | | | |
| Timestamp | Header Information | Key Information | Evidence Location |
| Fri, 6 Jul 2012 11:49:31 -0400 | Subject: can’t pass up  From: [pastsumtwelve@hotmail.com](mailto:pastsumtwelve@hotmail.com)  To:[throne1966@hoitmail.com](mailto:throne1966@hoitmail.com)  CC: [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com) | Emails speaking to how the subjects are going to conduct the National Gallery Heist  Needs.txt- (explains the MO on hos they are going to break in, what they will be wearing, how to walk silently, detecting lasers, use as a means of escape if caught) | 9F0508b8-04fb-490ea7f03e23b037c59b.emlx |
|  |  | No evidentiary value | F3F.emlx.slack |
| Fri, 5 Jul 2012 12:58:41 (-0700 PDT) | Subject: Busy  From: [Wiona.Honril@m57.biz](mailto:fromLWiona.Honril@m57.biz)  To: [coralblue@hotmail.com](mailto:coralblue@hotmail.com) | Encrypted file:  Filename=”000001.doc” | F3F.emxl |
| Mon, 9 Jul 2012, 10:44:11 -400 | Subject: things  Fom: [tracysumtwelve@gmai.com](mailto:tracysumtwelve@gmai.com)  To:  [coralblue@hotmail.com](mailto:coralblue@hotmail.com) | Encrypted file:  Filename=”documents.zp” | 83A.emlx |

### 

# **Appendix B: WiFi and GPS Location Information:**

