|  |
| --- |
| Cybersecurity |
| 21.3 The Final Report |

Case Report

National Gallery DC

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

# 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)

# 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. Pat and Tracy were planning to steal stamps from the National Gallery.

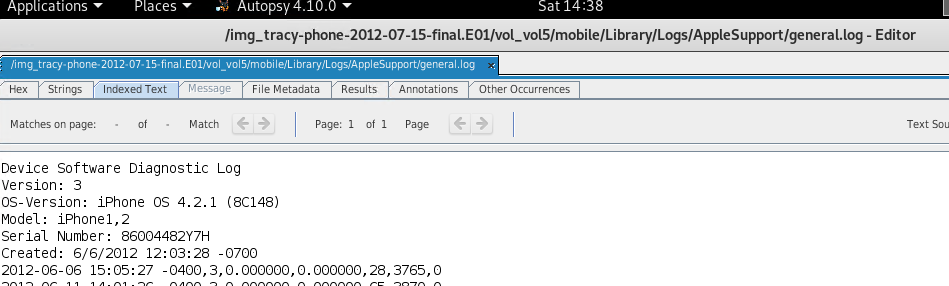
2. Tracy was going to help Carry violate gallery security protocol and bring in her tablet for a flash mob (actually, and attempt to deface art).

### Equipment and Tools

<Kali Linux terminal, Autopsy (digital forensics tool), SQLite.>

# Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone (1-2) | /mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelve’s iPhone | /mobile/Library/Logs/AppleSupport/general.log |
| OS Version | iPhone OS 4.2.1 (8C148) | /mobile/Library/Logs/AppleSupport/general.log |
| Install Time | 6/6/2012 19:03:28 | /mobile/Library/Logs/AppleSupport/general.log |
| User Email | [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com), [tracysumtwelve@nationalgallergydc.org](mailto:tracysumtwelve@nationalgallergydc.org) | vol5/mobile/Library/Mail |
| Phone Number | (703) 340-9661 | /mobile/Library/Logs/AppleSupport/general.log |
| Serial Number | 86004482Y7H | /mobile/Library/Logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | /logs/lockdownd.log.1 |
| IMEI | 012021003735398 | /root/Library/Lockdown/activation\_records/wildcard\_record.plis |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | /mobile/Library/Logs/AppleSupport/general.log |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | /mobile/Library/Logs/AppleSupport/general.log |



# 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

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused

Pat:

Phone Number: (571) 308-3236

Email: [pasumwelve@gmail.com](mailto:pasumwelve@gmail.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: accomplice/another accused

[Provide a summary of your conclusions here.]

# 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.

* [Pat unknowingly reveals that “Coral Blue” is Tracy (and her password)
* Pat (using the pseudonym “Perry”), Tracy (using the pseudonym “Coral”), and “King” discuss details regarding the heist, including materials needed
* The .pdf files in an attachment reveal the targets of the heist.]

# 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.

[ Carry and Tracy discuss details on the flash mob, including sneaking Carry’s tablet into the museum past the security guards. (Later to be confiscated for further museum art defacement evidence)

# Plot Timeline

[June 19, 2012 – Tracy and Pat set up aliases.

July 02, 2012 – Tracy asks Joe for help paying for daughter’s school. Joe refuses unless their daughter is allowed to live with him.

July 09, 2012 – Tracy emails herself the insurance claims for the stamps (with monetary value listed).

July 10, 2012, 6 am – Tracy and Carry discuss sneaking the tablet into the National Gallery.

July 10, 2012, 8 am – Pat sends an email to King trying to blackmail him into participating in their crime.

July 11, 2012 – Carry plans to come in around 9.

July 11, 2012 – Tracy circles around the National Gallery (waiting for someone?) ]

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* [In June 2012 Tracy and her brother Pat started planning to steal stamps and send each other secret messages via email. On July 09 Tracy emails herself insurance claims with the stamp monetary value, this indicates the plan to steal the stamps. Pat is trying to get King to become their accomplice. The reason for potential crime is Tracy’s financial difficulties: she is no longer able to afford the school tuition for her daughter, and her daughter would rather move in with her dad than transfer to a different school. Tracy’s financial difficulties make her vulnerable to participation in another crime. In her message of 2012-07-10 06:29 PDT Carry tells Tracy about a plan to stage a flash mob in the National Gallery Tracy agrees to help sneak Carry’s tablet into the gallery (violation of security rules). The tablet is being investigated as evidence in the case of potential artwork defacement. ]

# Appendix A: Correspondence Evidence

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

[

|  |  |  |
| --- | --- | --- |
| **Table 1.2: Contents of Email** | | |
| **Timestamps** | **Header Information** | **Body** |
| 6/19/2012 20:06:33 | : patsumtwelve@gmail.com  T: tracysumtwelve@gmail.com  Subject: Paris Speak and answer | Pat emails Tracy letting her know that he has accepted her proposal and asks her to email using her alias for further instructions. |
| 6/19/2012 21:38:59 | F: perrypatsum@yahoo.com  T: coralbluetwo@hotmail.com  Subject: Crazydave by the VMs Attachment: Crazydave1.mp3 | Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file. |
| 6/29/2012 14:31:36 | F: perrypatsum@yahoo.com  T: tracysumtwelve@gmail.com  Subject: hey sis | Pat (Perry) emails Tracy addressing her as ‘sister’ and enquires about Terry. Asks her to check in with Coral with whom he has been planning some things. He also suggests all of them going together for dinner as friends.  He asks Tracy to check in with Coral.  Possible misdirection attempted by referring to Coral as a third person in the narrative |
| 7/3/2012 14:53:04 | F: perrypatsum@yahoo.com  T :coralbluetwo@hotmail.com  Subject: Re: Some good news | Email Thread: Some good news  Tracy (Coral) emails Pat (Perry) saying that the exhibit is rare and highly valuable stamp collection and that may be this is their opportunity.  Pat (Perry) replies to Tracy (Coral) asking her to collect as much information as possible about the stamp exhibit and that in the meantime he would look into options for pulling off the heist. |
| 7/6/2012 15:49:31 | 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. |
| 7/9/2012 14:44:11 | 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. |
| 7/9/2012 18:18:47 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Re: Long time no see.. | Email Thread: Long time no see... Tracy thanked Carry for the lunch.  Carry emails Tracy asking for help sneaking in a tablet for a flash mob event they had spoken earlier about. Carry suggests that Tracy would be compensated in some way for the help. |
| 7/10/2012 13:48:40 | F: carrysum2012@yahoo.com  T: tracysumtwelve@gmail.com  Subject: Re: Long time no see... | Email Thread: Long time no see…  Tracy agrees to help Carry sneak in the tablet and asks when Carry would like to get in to take a look around the gallery.  Carry replies saying that this would be a big help and asks if she could come around 9 tomorrow. |
| 7/10/2012 15:24:57 | 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. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix B: WiFi and GPS Location Information

[

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Location Information** | | | | |
| **Artifact #** | **Timestamp** | **Header Information** | **Body Coordinates** | **Map Screenshot** |
|  | 3.61306882473715E8 |  | 38.88055896 -77.11553561 |  |
|  | 3.61307043743548E8 |  | 38.88155686 -77.11480695 |  |
|  | 3.63015762683134E8 |  | 38.88021904 -77.11561894 |  |
|  | 3.63198767554628E8 |  | 38.88055533 -77.11455225 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

your GPS Evidence Worksheet here.]