CASE REPORT

NATIONAL GALLERY DC

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

GROUP 1

- **Selena Cobb-Flowers**
- **Pooja Bhagat**
- **Abid Sheikh**
- **Deborah Wale Ibinayo**
- **Alajuwon Thomas**
- **Emmanuel Odeh**

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

On January 21, 2016, DigiTech Inc. was called in to assist with the National Gallery, Washington DC (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museum of art at the NGDC.

- Tracy is a suspect in the above-mentioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- DigiTech Inc. was tasked with investigating evidence relevant to the above-mentioned conspiracy.
- To do analysis DigiTech used following tools:
    - Autopsy
    - DB Browser for SQLite
    - Kali Linux
    - Google map

2. DETAILS OF TRACY'S IPHONE

Traces phone details could be found three ways.

2.1 Physical Device information

a. Mac or serial number below is details

TableInfo TableName SoftwareVersion SerialNumber

CompassCalibration 370.3 86004482Y7H

2.2 Network information

a. Wi-Fi information

WifiLocation 370.3 86004482Y7H

Location 370.3 86004482Y7H

Wifi 370.3 86004482Y7H

WifiLocationHarvest 370.3 86004482Y7H

LocationHarvest 370.3 86004482Y7H

2.3 Data information

a. Information about voice data

Cell 370.3 86004482Y7H

CellLocation 370.3 86004482Y7H

CellLocationBoxes 370.3 86004482Y7H

CellLocationLocal 370.3 86004482Y7H

CellLocationLocalBoxes 370.3 86004482Y7H

CellLocationHarvest 370.3 86004482Y7H

b. Information about SMS

Cell 370.3 86004482Y7H

CellLocation 370.3 86004482Y7H

CellLocationBoxes 370.3 86004482Y7H

CellLocationLocal 370.3 86004482Y7H

CellLocationLocalBoxes 370.3 86004482Y7H

CellLocationHarvest 370.3 86004482Y7H

3. 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
Email:	tracysumtwelve@gmail.com
Work email:	tracy.sumtwelve@nationalgallerydc.org
Relationship:	Accused

Pat:

Phone Number: +15713083236

Email: perrypatsum@yahoo.com, patsumtwelve@gmail.com

Relationship: Brother

Terry:

Phone Number: 7038296071
Email: NA
Relationship: Daughter

Joe:

Phone Number: Not evidence found for phone number

Email: joe.sum.twelve@gmail.co

Relationship: Divorced Spouse

Carry:

Phone Number: +12027252124

Email: carrysum2012@yahoo.com

Relationship: Acquaintance

4. EVIDENCE RELATING TO THEFT OF VALUABLE STAMPS

Below table shows Summary of the evidence found as it relates to the theft of valuable stamps. This evidence shows that Stamp of Kazakstan2 listed twice for insurance purposes of $29,000 each.

Armed Forces Reserve	$43,000
Stamp of Kazakstan2	$29,000
BradyCo	$12,000
Woman's Profile	$31,000
1929 Napal	$27,000
Stamp of Kazakstan2	$29,000
Douglas MacArther	$35,000
Nederland	$30,000
Mongolia	$24,000

5. EVIDENCE RELATING TO DEFACEMENT OF MUSEUM ART

Above evidence are for Insurance for Stamp of Kazakstan2 $29,000. This impacts **4322-Stamp insurance** and **4322-Stamp insurance** policies that is resulting these two stamps defaced or damaged.

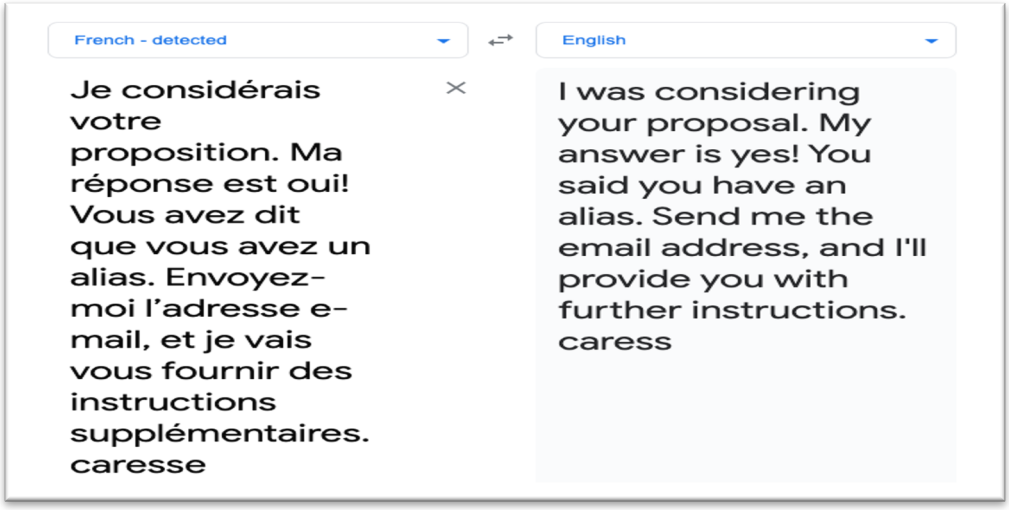
6. PLOT TIMELINE

July 7th Payment of $1000 was made via a suspicious Giftcard
July 10th An email was received with an attachment including all items needed for the heist.
July 11th Tracy allowed Carry to bring in her tablet to obtain information regarding the gallery
July 12th A question was asked “How was the flashmob going?”

7. EMAIL CONTENT

Table 1.2: Contents of Email

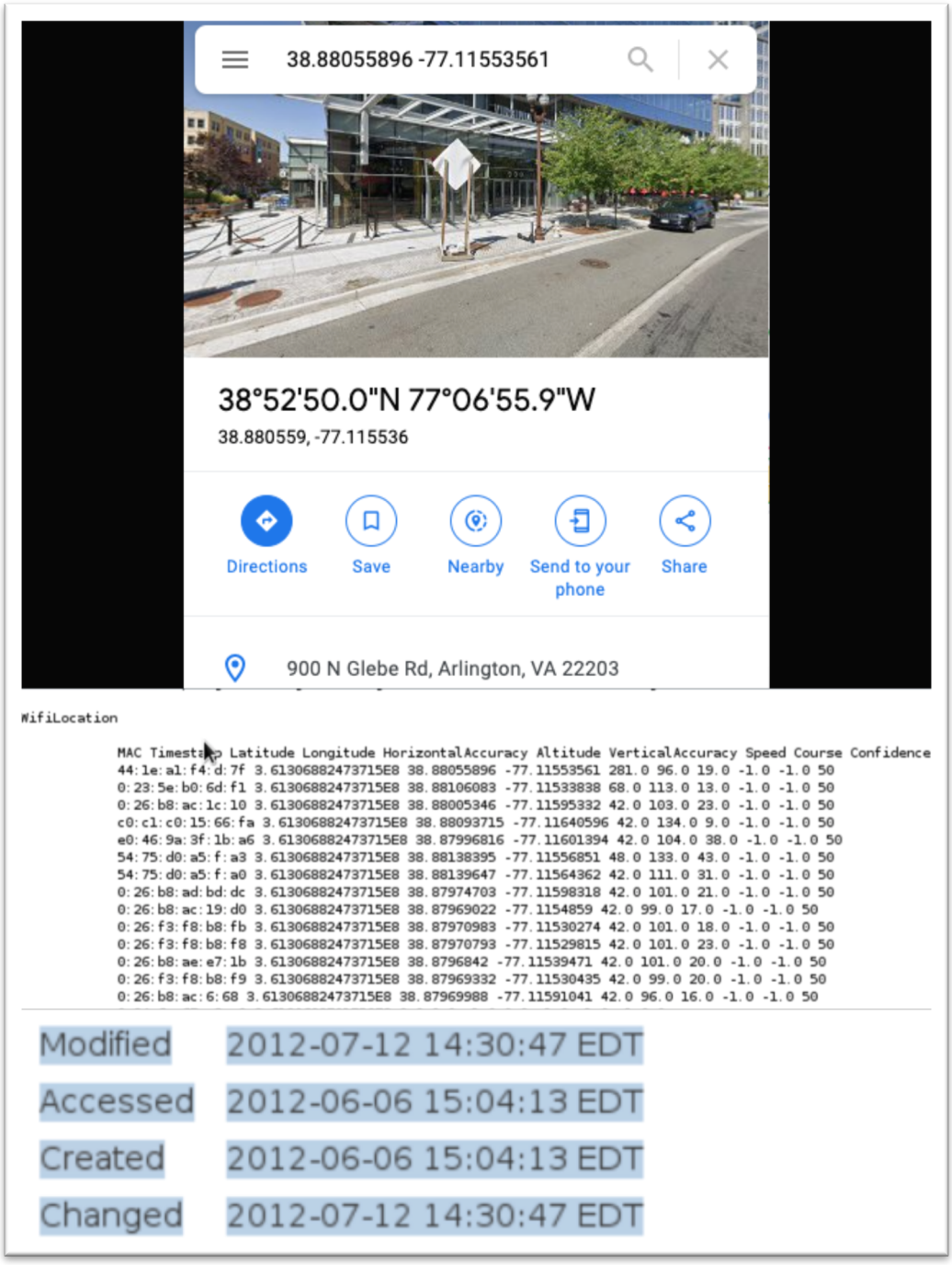
Timestamps	Header Information	Body
19 Jun 2021 14:39:04 -0700	From: Perry Patsum <perrypatsum@yahoo.com> Reply-To: Perry Patsum <perrypatsum@yahoo.com> Subject: Crazydave by the VMs To: Coral Bluetwo <coralbluetwo@hotmail.com>	Audio file included called Crazydave1.mp3 encoding is base64, which was mentioned in the email Hey Coral,=A0=0A=0AJust got your email. That took longer than expected! O= well! =0A=0A=0AYou've got to check out this new song by the VMs. I love the= base. Tell me what you think!=0A=0APerry=0A
Mon, 9 Jul 2012 10:44:11	From: Perry Patsum <perrypatsum@yahoo.com> Reply-To: Perry Patsum <perrypatsum@yahoo.com> Subject: Crazydave by the VMs To: Coral Bluetwo <coralbluetwo@hotmail.com>	documents.zip contains the three stamp insurance.pdf(.1 -3) files password unknown. Found additional files viewable without password requirement.
Date: Tue, 10 Jul 2012 11:24:57	Subject: Fwd: can't pass up From: Pat TeeSumTwelve <patsumtwelve@gmail.com> To: coralbluetwo@hotmail.com	this is what we need to get for the guy that's going to make our job happen 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)



8. SMS MESSAGE CONTENT

Phone	Date Timestamp	Text Discussion
12069100932	Saturday, July 7, 2012 3:36:35 PM	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
12027252124	Thursday, July 12, 2012 1:06:45 PM	How's the flashmob going
15713083236	Tuesday, July 10, 2012 3:26:19 PM	hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know
12027252124	Thursday, July 12, 2012 1:06:45 PM	How's the flashmob going
12027252124	Wednesday, July 11, 2012 8:49:08 AM	Just meet me out front, I'll take the tablet in.
12027252124	Wednesday, July 11, 2012 8:41:45 AM	I'm almost there where should I meet you?

9. WI-FI/GPS LOCATION INFORMATION



10. CONCLUSION

Evidence found on Tracy's iPhone indicated the following:

- Tracy used the alias Coral and Pat used the alias Perry.
- Planning of the Flashmob
- Able to retrieve Need.txt, which included items needed for the effort
- We could see from SMS a conversation occurred and financial payments were provided
- Time correlation of activities occurred within the specific timeframe for planning of the event
- Conversation between all parties appears suspicious regarding the art defacement
- And we noticed text messages from Tracy to her daughter; however, the mobile number was the same as Tracy's.
- We have Alias Email Addresses between Tracy and her brother