



Cybersecurity

## 21.3 The Final Report

# Case Report National Gallery DC

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

# Table of Contents

---

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

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

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

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

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

## 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.

[Provide a brief summary of your findings here.]

## Equipment and Tools

Digittech uses Autopsy, an open source forensics tool frequently used in the industry. Websites, including google maps, were referenced and used as well.

## Details of Tracy's iPhone

Phone Number: (703) 340-9961

Model: iPhone 1,2

Serial Number: 86004482Y7H

iPhone Name: Tracy Sumtwelves iPhone

IMEI: 012021003735398

## 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: [perryatsum@yahoo.com](mailto:perryatsum@yahoo.com)  
patsumtwelve@gmail.com  
Relationship: Tracy's brother

Terry:

Phone Number: (703) 829-6071  
Email: NA  
Relationship: Tracy and Joe's daughter

Joe:

Phone Number: NA  
Email: NA  
Relationship: Tracy's ex husband

Carry:

Phone Number: (202) 725-2124  
Email: NA  
Relationship: Accomplice

King:

Phone Number: NA  
Email: throne1966@hotmail.com  
Relationship: Pat's acquaintance

Tracy, supervisor at NGDC, her brother Pat, and accomplice King, conspired to steal stamps from NGDC. Joe, Tracy's ex husband, turned them into the police.

## 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.

The evidence provided suggests Tracy, Pat and King conspired to steal stamps from NGDC.

Correspondence between Pat and King suggests that Pat blackmailed King into assisting with the heist. King replies with a list of supplies needed to complete the heist. Kings reply is forwarded to Tracy to acquire this list of supplies.

Tracy emails herself a ZIP file containing PDF files about stamp insurance, listing stamps and their specific insurances.

Stamp Insurance1.pdf

- Armed Forces Reserve
- Stamp of Kazakstan
- Brady & Co

Stamp Insurance2.pdf

- Profile
- Stamp of Kazakstan
- 1929 Nepal

Stamp Insurance3.pdf

- Douglas MacArthur
- Netherland
- Mongolia

Finally, Tracy's cellphone location suggests she was near or in NGDC.

## 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.

A Flashmob was conducted in order to deface museum art, messages between Carry and Tracy suggest they were both involved.

Tracy and Carry meeting at Bubbas Grill

Tracy and Carry meetup with Carry's tablet

Tracy asks Carry how the flashmob is going

## Plot Timeline

06/19/12 - Pat give virtual machine info to tracy

07/05/12 - Messages between Tracy and Carry to meet at Bubbas Grill

07/06/12 - Tracy and Carry meet at Bubbas Grill

07/06/12-07/10/12 - Emails between Pat, King and Tracy regarding necessary supplies

07/08/12 - Tracy photographs stamps

07/09/12 - Tracy sends stamp insurance pdf's to herself

07/11/12 - Tracy and Carry meet with Carry's tablet

07/12/12 - Tracy inquires to Carry about flashmob

## Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Evidence gathered from Tracy's phone indicates Tracy, Pat and King intended to steal valuable stamps from NGDC. Both Tracy and Pat used aliases Coral and Perry respectively. Tracy and Carry were also involved in a flashmob intended to destroy museum art. Emails, messages, and photos suggest the four individuals involved committed various crimes, for various reasons, of varying severity, but they were all involved.

## Appendix A: Correspondence Evidence

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

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1	Jul 6 2012 15:49:31	Subject: cant pass up From: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> To: <a href="mailto:throne1966@hotmail.com">throne1966@hotmail.com</a> CC: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a>	Pat blackmails king into helping with the heist	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/9F0E-A7F0-3E23B0E7C59B.elmx
2	Jul 7 2012 14:47:58	From: Tracy Sumtwelve ( <a href="mailto:tracysumtwelve@gmail.com">tracysumtwelve@gmail.com</a> ) To: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a>  Subject: Things	Contains zip file referencing stamp insurances	/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/IN

		Attachment: documents.zip		BOX.mbox/ Messages/8 A3BD06F-C DB-4453-96 69-77E0682 3F2AE.emlx
3	Jul 10 2012 11:19:00	From: King kthings ( <a href="mailto:throne1966@hotmail.com">throne1966@hotmail.com</a> ) To:	King replies to Pat with needs.txt, his list of supplies	/vol5/mobile/ Library/Mail/ POP-coralbl uetwo@hotm ail.com@pop 3.live.com/IN BOX.mbox/ Messages/9 F0508B8-04 FB-490E-A7 F0-3E23B0E 7C59B.elmx/ Attachments/ 60/2/needs.t xt
4	Jul 10 2012 15:24:58	From: Pat Sum Twelve ( <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> ) To: <a href="mailto:coralblue@hotmail.com">coralblue@hotmail.com</a>  Subject: Fwd: can't pass up  Attachment: needs.txt	Pat forwards supplies list to Tracy	vol5/mobile/L ibrary/Mail/P OP-coralblue two@hotmail .com@pop3.l ive.com/INB OX.mbox/Me ssages/9F05 08B8-04FB- 490E-A7F0- 3E23B0E7C 59B.elmx/Att achments/60 /2/needs.txt
5	Jul 5 2012 18:18:23	From: Carry To: Tracy	Text from Carry about meeting Tracy at Bubbas Grill at 1pm	/vol5/mobile/ Library/SMS/ sms.db

6	Jul 5 2012 18:20:26	From: Tracy To: Carry	Tracys confirmation response to Carry	/vol5/mobile/ Library/SMS/ sms.db
7	Jul 11 2012 12:49:08	From: Tracy To: Carry	Tracy telling Carry she will bring the tablet, and to meet her up front	/vol5/mobile/ Library/SMS/ sms.db
8	Jul 12 2012 17:06:45	From: Tracy To: Carry	Tracy asking Carry how the Flash Mob is going.	/vol5/mobile/ Library/SMS/ sms.db

## Appendix B: WiFi and GPS Location Information

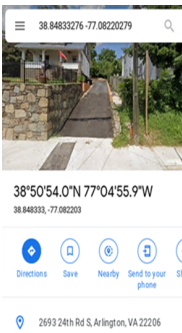
Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	Jul 2 2012 16:19:24	WiFi Location: 38.87990736 - 77.11460858 File: /vol5/root/Librar y/Caches/locati ond/consolidate d.dbd.db	800 N. Glebe Rd. Arlington, VA 22203	
2	Jul 5 2012 16:32:47	WiFi Location: 38.88054466 -77.11439651  File: /vol5/root/Librar y/Caches/locati ond/consolidate	801 N. Glebe Rd.  Arlington, VA 22203	



d.db

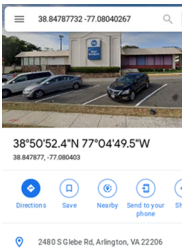
3      Jul 10      WiFi Location:      2693 24th Rd. S.  
2012      38.84833276      Arlington, VA 22206  
16:31:12      -77.08220279

File:  
/vol5/root/Librar  
y/Caches/locati  
ond/consolidate  
d.db



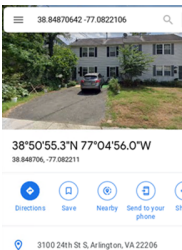
4      Jul 10      WiFi Location:      2480 S. Glebe Rd.  
2012      38.84787732      Arlington, va 22206  
16:31:12      -77.08040267

File:  
/vol5/root/Librar  
y/Caches/locati  
ond/consolidate  
d.db



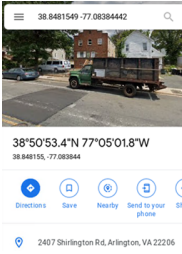
5      Jul 10      WiFi Location:      3100 24th St. S.  
2012      38.84870642      Arlington, VA 22206  
16:31:12      -77.0822106

Fiile:  
/vol5/root/Librar  
y/Caches/locati  
ond/consolidate  
d.db



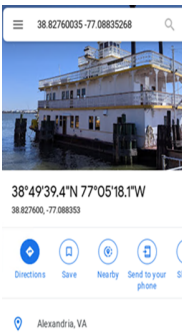
6 Jul 10 WiFi Location: 2407 Shirlington Rd.  
2012 38.8481549  
16:31:12 -77.08384442 Arlington, VA 22206

File:  
/vol5/root/Library/  
Caches/location/  
consolidated.db



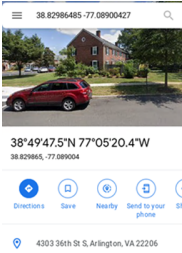
7 Jul 10 WiFi Location: Alexandria, VA  
2012 38.82760035  
16:45:01 -77.08835268

File:  
/vol5/root/Library/  
Caches/location/  
consolidated.db



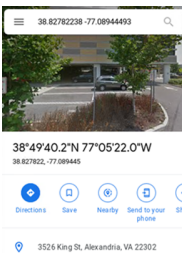
8 Jul 10 WiFi Location: 4303 36th St. S.  
2012 38.82986485  
16:45:01 -77.08900427 Arlington, VA 22206

File:  
/vol5/root/Library/  
Caches/location/  
consolidated.db



9 Jul 10 WiFi Location: 3526 King St.  
2012 38.82782238  
16:45:01 -77.08944493 Arlington, VA 22302

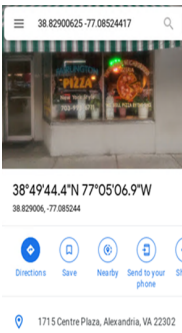
File:  
/vol5/root/Library/  
Caches/location/  
consolidated.db



d.db

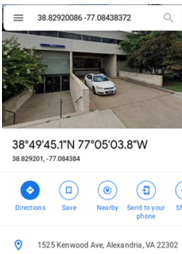
10 Jul 10 WiFi Location: 1715 Centre Plaza  
2012 38.82900625  
16:46:29 -77.08524417 Alexandria, VA 22302

File:  
/vol5/root/Librar  
y/Caches/locati  
ond/consolidate  
d.db



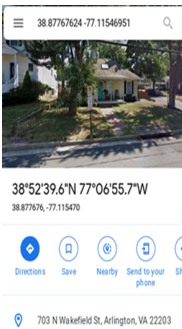
11 Jul 10 WiFi Location: 1525 Kenwood Ave.  
2012 38.82920086  
16:46:29 -77.08438372 Alexandria, VA 22302

File:  
/vol5/root/Librar  
y/Caches/locati  
ond/consolidate  
d.db



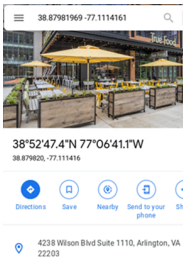
12 Jun 13 Cell Location: 703 N. Wakefield St.  
2012 38.87767624  
19:01:21 -77.11546951 Arlington, VA 22203

Fiile:  
/vol5/root/Librar  
y/Caches/locati  
ond/consolidate  
d.db

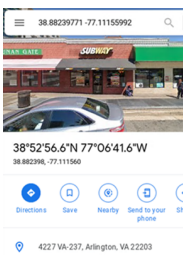


13 Jun 13 Cell Location: 4238 Wilson Blvd Suite 1110  
201219:01:21 38.87981969 Arlington, VA 22203  
-77.1114161

File:  
/vol5/root/Library/Caches/location/consolidated.db



14 Jul 2 2012 Cell Location: 4227 VA-237  
16:19:23 38.88239771 Arlington, VA 22203  
-77.11155992



15 Jul 10 Cell Location: 1700 Army Navy Dr.  
2012 38.85141718 Arlington, VA 22202  
16:31:10 -77.07823592

File:  
/vol5/root/Library/Caches/location/consolidated.db



16 Jul 8 2012 Cell Location Northwest Washington  
16:34:40 Local: Washington, DC 20408  
38.8917478666  
667  
-77.023462716

File:  
/vol5/root/Library/Caches/location/consolidated.db

