

# Case Report

## National Gallery DC

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

Presented by:  
Jason Scherer

# 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.

Tamps from the NGDC. Tracy provided the NGDC information to assist Carry with a flash mob, which Tracy's phone was used as evidence to show collusion between Tracy, Pat, and King to steal stamps a cover to damage foreign art at the NGDC in a bid to embarrass the United States internationally.

## Equipment and Tools

Windows VM including Kali linux machine.  
Autopsy used to look through files of cloned iPhone

## Details of Tracy's iPhone

Case Name: 2012-07-15-National-Gallery Case #: 1EZ215-P

### Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 1,2 3G	vol5/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	vol5/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	vol5/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	vol5/mobile/Library/Logs/AppleSupport/general.log
User Email	<a href="mailto:Tracy.sumtwelve@nationalgallerydc.org">Tracy.sumtwelve@nationalgallerydc.org</a> <a href="mailto:tracy.sumtwelve@gmail.com">tracy.sumtwelve@gmail.com</a> <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a>	vol5/mobile/Library/Mail
Phone Number	1(703)340-9661	vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	vol5/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log.1
IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577cc d534ca0d1e83ffd27683e621607	

# 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](mailto:tracysumtwelve@gmail.com)  
Work email: [tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org)  
Relationship: ex husband: Joe  
daughter: Terry

Pat: Alias - Perry

Phone Number: (571)308-3236  
Email: [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com)  
Relationship: Brother

Terry:

Phone Number: (703)829-6071  
Email: N/A  
Relationship: Daughter of Joe and Tracy

Joe:

Phone Number: N/A  
Email: [joe.sum.twelve@gmail.com](mailto:joe.sum.twelve@gmail.com)  
Relationship: ex-husband of tracey/father of Terry

Carry: Alias - Cat

Phone Number: (202)725-2124  
Email: carrysum2021@yahoo.com  
Relationship: Acquaintance of Tracy

Data collected from Tracy's phone gives us a number of names and aliases, with additional contact info, including emails and phone numbers. Tracy is a supervisor at the NGDC and colluded with her brother Pat (alias Perry) and an individual named King (alias Kart), to steal stamps from the NGDC. In addition Tracy is receiving assistance from Carry (alias Cat), at the NGDC, to get pictures from a tablet.

Joe is the ex-husband of Tracy and installed a keylogging device on Tracy's laptop to monitor their daughter, Tracy's, internet usage. The keylogger led Joe to discover Tracy's intention to steal stamps from the NGDC, resulting in him reporting her to the police. Tracy's brother Pat is a police detective and is very devoted to Tracy's daughter Terry. Pat has protected King (alias Kart) by not arresting him in exchange for future favors.

Carry (alias Cat) is a Krasnovian sympathizer who is contacted by Alex, a Krasnovian, to orchestrate the plot to embarrass the United States by defacing foreign artwork at the NGDC. Alex is a Krasnovian with aims to humiliate the United States by defacing foreign artwork. He knows Carry via familial connections and initiated contact with her to orchestrate their plan.

## 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.

Evidence collected from Tracy's phone clearly demonstrate Tracy, Pat, and King were colluding together to steal stamps held at the NGDC. Tracy's phone even contains image files of the stamps they want to steal. An email sent from Pat to King provides instructions about the planned theft, while asking for assistance, instead of blackmailing him. An email sent from king provides a list of needed tools to perform the theft.

## 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.

Evidence gathered from Tracy's phone shows communication with Carry to set up a flash mob to create a distraction as cover. Carry's plan to create a flash mob is a cover for their own Krasnovian plot. There are a number of SMS messages in regard to setting up the flash mob.

## Plot Timeline

- Tuesday, June 19, 2012 – Pat sends Tracy information about a Virtual Machine.
- Thursday, July 5, 2012 – SMS messages between Tracy and Carry ask for a meeting at Bubba's Grill.
- Friday, July 6, 2012 – Tracy meets Carry at Bubba's Grill.
- Friday, July 6, 2012 - SMS between Tracy, Pat, and King discuss tools needed for stamp theft.
- Tuesday, July 10, 2012
- Sunday, July 08, 2012 - Tracy takes photographs of desired stamps for theft.
- Monday, July 9, 2012 - Tracy sends a message to herself consisting of copies of memos about insurance for specific stamps
- Wednesday, July 11, 2012 – Tracy meets Carry to take Carry's tablet with her.
- Thursday, July 12, 2012 – Tracy asks Carry about the flash mob status.

## Conclusion

Evidence found on Tracy's iPhone indicated the following:

Based on Email correspondence, text messages, photo evidence, and additional information, Terry colluded with Pat and King to steal expensive stamps from the NGDC. During this investigation it was discovered that Tracy was unwittingly willing to give sensitive information crucial to Carry's plan to conduct a flash mob as cover for her own scheme to damage artwork of foreign nations, in a bid to embarrass the United States. Email correspondence revealed that Tracy and Pat used aliases to hide their identity. Tracy's alias was Coral and Pat's alias was Perry.

Tracy is undergoing financial stress with her daughter, Terry's, tuition to Prufrock, based upon her SMS messages and a note to herself left on her phone. The evidence of the attached file describing the necessary tools to carry out the theft, the stamp insurance memos, and photos of the stamps reveal the breadth of the scheme. The discovery of the plot to deface artwork by foreign actors was a consequence of the initial investigation.

## Appendix A: Correspondence Evidence

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

# Correspondence Evidence Worksheet

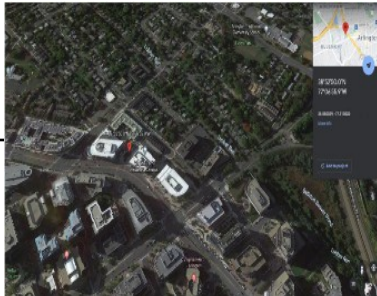
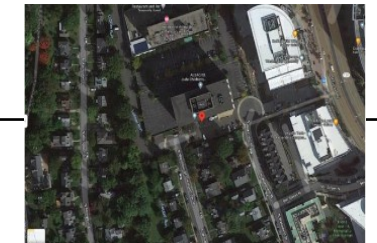
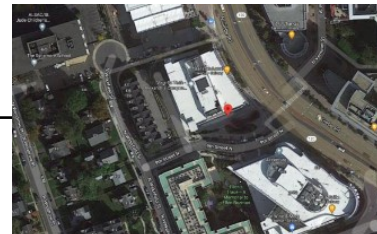
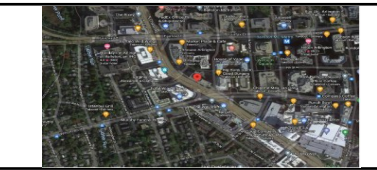

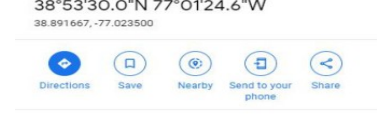

Master Timeline of NGDC			
Artifact #	Timestamp	Header Information	Key Information
1	6/19/2012 20:06:33	F: <a href="mailto:patsumtwelve@gmail.com">patsumtwelve@gmail.com</a> T: <a href="mailto:tracysumtwelve@gmail.com">tracysumtwelve@gmail.com</a> Subject: Paris Speak and answer	Pat sends an email to Tracy letting her know that she agrees with her plan and asks that she use aliases for further communication
2	6/19/2012 20:26:47	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:tracysumtwelve@gmail.com">tracysumtwelve@gmail.com</a> Subject: Look me up sometime	Pat (alias Perry) emails Tracy to use aliases for communication
3	6/19/2012 21:38:59	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Pay (alias Perry) emails Tracy (alias Coral) with instructions to install a VM hidden within an audio file
4	6/19/2012 17:43:15	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject RE: Crazydave by the VMs	Pat (alias Perry) replies to Tracy (alias Coral) on an existing email thread about a VM installation saying she should listen to other songs. Tracy (alias Coral) confirms that the instructions sent earlier in the audio file
5	6/28/2012 19:31:33	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject: Whats going on	Pat (alias Perry) asks Tracy (alias Coral) to communicate using aliases and the VM to keep their activities secret. Pat also suggests they may need to perform more illegal activities as they are facing financial hardship. Pat also tells her that few of his coworkers were adept at these sorts of things and will inform her if anything happens.
6	6/29/2012 14:21:56	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:coraltwoblu@hotmail.com">coraltwoblu@hotmail.com</a> Subject Re: Whats going on	Pat suggests they use a VM and aliases to communicate while looking for ways to make money. Tracy responds that she will keep her eyes open and insists Pat try find work soon. Tracy also says she is monitoring insurance papers for something that could be useful.
7	6/29/2012	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:tracysumtwelve@gmail.com">tracysumtwelve@gmail.com</a> Subject: Hey sis	Pat (alias Perry) emails Tracy, referring to her as "sister" and asks about Terry. Pat asks her to check with Coral with whom he has been planning things. He also suggests they get dinner as friends, implying them and

			their aliases as if they were additional persons. This appears to be an attempt at misdirection.
8	6/29/2012 15:21:35	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject Re: Whats going on	Pat replies to the email to assure Tracy about her concerns about the IA watching them. Pat mentions that they can get the job done.
9	7/2/2012 16:13:18	F: <a href="mailto:perrypatsum@yahoo.com">perrypatsum@yahoo.com</a> T: <a href="mailto:coralbluetwo@hotmail.com">coralbluetwo@hotmail.com</a> Subject Re: Some good news	Tracy emails Pat about an interesting foreign exhibit and that from assessing paperwork regarding it she feels it would be a big deal. Pay responds feeling hopeful this might be what they were looking for.

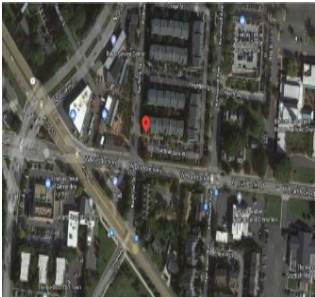

## Appendix B: WiFi and GPS Location Information



# Location Information Worksheet

Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	Wednesday, June 13, 2012 7:01:21 PM	Cell Location: 38 52'39.6"N 77 06'55.7"W	Location: Virginia Tech Research Center – Arlington (900 N Glebe Rd, Arlington, VA 2203, USA)	
2	Sunday June 13, 1915 7:01:22 Pm	Wifi Location: 38 52'50.0"N 77 06'55.9"W	Location: Virginia Tech Research Center – Arlington (900 N Glebe Rd, Arlington, VA 2203, USA)	
3	Monday. July 2, 2012, 4:19:23 PM	Cell Location: 38 52'51.3"N 77 07'01.6"W	Location: 4600 Fairfax Dr, Arlington, VA 22203, USA	
4	Monday. July 2, 2012, 4:19:24 PM	Wifi Location: 38 52'51.3"N 77 07'01.6"W	Location: 800 N Glebe Rd, Arlington, VA 22203, USA	
5	Tuesday, July 3, 2012 1:42:42 PM	Wifi Location: 38 52'50.3"N 77 06'56.1"W	Location: 900 N Glebe Rd, Arlington, VA 22203, USA	
6	Thursday, July 5, 2012 4:32:46 PM	Cell Location: 38 52'46.2"N 77 06'52.6"W	Arlington, VA 22203, USA	
7	Thursday, July 5, 2012 4:32:47 PM	Wifi location: 38 52'46.2"N 77 06'52.6"W	Location: 801 N Glebe Rd Arlington, VA 22203, USA	
8	Sunday, July 8, 2012 12:33:36 PM	Cell Location: 38 52'46.2"N 77 06'52.6"W	National Gallery of Art, Washington, DC 20408, USA	

9	Sunday, July 8, 2012 12:41:41 PM	Cell Location: 38 53'27.0"N 77 01'19.9W	Northwest Washington, Washington, DC 20408, USA	
10	Tuesday, July 10, 2012 4:31:10 PM	Cell Location: 38 51'05.1"N 77 04'41.7"W	Location 1700 Army navy Dr, Arlington, VA 22202, USA	
11	Tuesday, July 10, 2012 4:31:12 PM	Wifi Location: 38 50'54.0"N 77 04'55.9"W	Location 2693 24 <sup>th</sup> Rd S, Arlington, VA 22206, USA	

12	Tuesday, July 10, 2012 4:45:00 PM	Cell Location: 38 49'37.4"N 77 05'10.0"W	Location 1737 W Braddock PI, Alexandria, VA 22302, USA	
13	Tuesday, July 10, 2012 4:45:01 PM	Wifi Location: 38 49'39.5"N 77 05'17.0"W	Location 4104 36 <sup>th</sup> St S, Arlington, VA 22206 USA	
14	Tuesday, July 10, 2012 4:46:29 PM	Wifi Location: 38 49'44.7"N 77 05'05.1"W	Location 1701 Centre Plaza, Alexandria, VA 22302, United States	