Cybersecurity

21.3 The Final Report

Case Report
National Gallery DC

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.

Based on the evidence known and shown below, A Krasnovian supporter named Alex who lives outside the United States wishes to embarrass the United States by defacing an art exhibit at the National Gallery in DC. Alex has contacted Carry who he (Alex) knows through extended family connections, he (Alex) has asked Carry to help him orchestrate the aforementioned task.

Carry is also a Krasnovian supporter and is an acquaintance of Tracy who works as a supervisor at the National Gallery, Carry contacts Tracy and offers her money to help her with the task that she is conspiring to complete. Tracy is happy to accept the offer as she is struggling to pay school fees for her daughter Terry due to the fact that she is going through a divorce with her soon to be ex-husband Joe.

Joe is financially well off and is still bitter with the issues with their marriage, so he has decided to stop paying their daughter's school fees as well as installing a keylogger on Tracy's iPhone in an attempt to spy on both Tracy and Terry.

Pat is a police officer in the D.C. Enforcers Bureau and also Tracy's brother, he has been helping Tracy to complete a different task of stealing the valuable stamps by putting her in contact with a known robber who goes by the name King Throne.

Equipment and Tools

To preserve the integrity of Tracy's iPhone, it was initially imaged using Encase - an industry standard in digital forensics imaging software. This image was then analysed using Autopsy - an open-source digital forensics tool that allowed the extraction of relevant files from the iPhone image, as well as the collection of screenshots to document evidence. SQLitebrowser (https://sqlitebrowser.org/) and Google Maps (https://maps.google.com/) were also used to analyse SQL databases and GPS coordinates extracted from the iPhone image.

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 1 or 2	vol_vol5/logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	vol_vol5/logs/lockdownd.log
OS Version	iPhone OS 4.2.1	vol_vol5/logs/AppleSupport/general.log
Install Time	6/6/2012 05:03:28	vol_vol5/logs/AppleSupport/general.log
User Email	tracy.sumtwelve@nationalgallerydc.org tracysumtwelve@gmail.com coralbluetwo@hotmail.com	vol_vol5/mobile/Library/Mail
Phone Number	(703) 340-9661	vol_vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	vol_vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	vol_vol5/logs/lockdownd.log
IMEI	012021003735398	vol_vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	

Evidence to Establish Personas

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

Tracy Sumtwelve (aka “Coral”):

Phone Number:	+1 703-340-9961
Personal Email:	tracysumtwelve@gmail.com
	coralbluetwo@hotmail.com
Work Email:	tracy.sumtwelve@nationalgallerydc.org
Relationship:	Accused

Pat Sumtwelve (aka “Perry”):

Phone Number:	+1 571-308-3236
Email:	patsumtwelve@gmail.com
	perrypatsum@yahoo.com
Relationship:	Brother of Accused

Terry:

Phone Number:	+1 703-829-6071
Email:	Not found
Relationship:	Daughter of Accused

Joe:

Phone Number:	Not found
Email:	joe.sum.twelve@gmail.com
Relationship:	Ex-husband of Accused

Carry (aka “Carrie” and “Cat”):

Phone Number:	+1 202-725-2124
Email:	carrysum2012@yahoo.com
Relationship:	Acquaintance of Accused

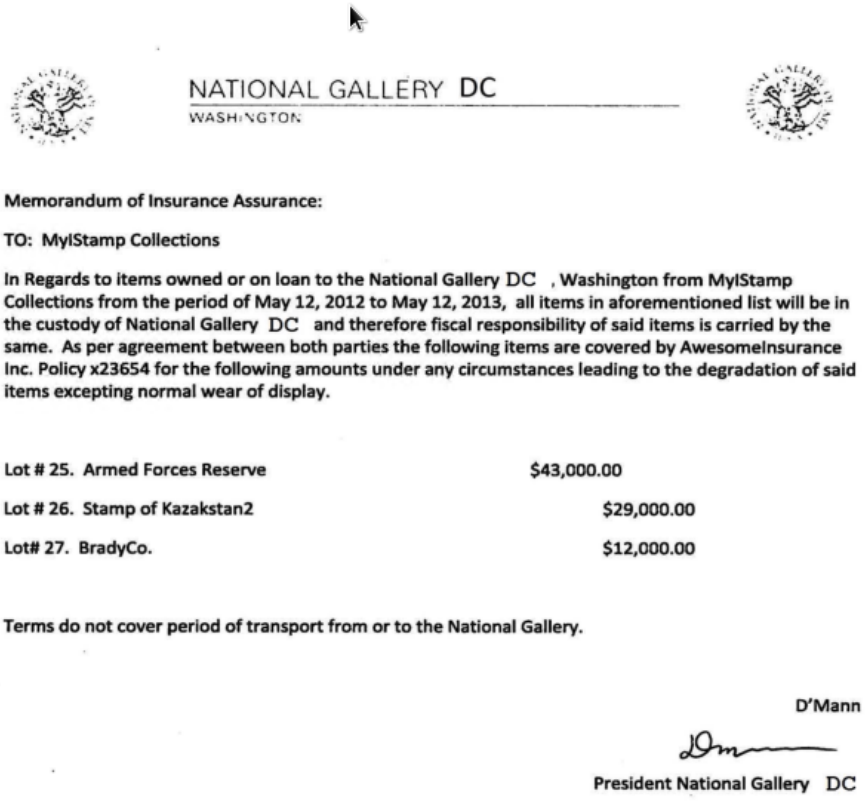
King Throne (aka “Kart”):

Phone Number:	Not found
Email:	throne1966@hotmail.com
Relationship:	Acquaintance of Accused’s Brother (Pat)

Evidence relating to the theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

There was an attachment folder in the emails which had three .pdf files that showed the amount of money the stamps are insured for, all of which were valued in the tens of thousands of US dollars. There were also photo images in Tracy's phone, documenting each of the stamps listed in the insurance documents.



NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 25. Armed Forces Reserve	**$43,000.00**
Lot # 26. Stamp of Kazakstan2	**$29,000.00**
Lot# 27. BradyCo.	**$12,000.00**

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

Figure 1 - Stamp_insurance1.pdf email attachment.

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0051.jpg
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0056.jpg
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0057.jpg

Figures 2, 3 & 4 - The three stamps mentioned in Figure 1.

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 11. Woman's Profile	**$31,000.00**
Lot # 12. Stamp of Kazakstan	**$29,000.00**
Lot# 13. 1929 Napal	**$27,000.00**

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

Figure 5 - Stamp_insurance2.pdf email attachment.

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0067.jpg
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0055.jpg
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0050.jpg


Figures 6, 7 & 8 - The three stamps mentioned in Figure 5.

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 1. Douglas MacArther	**$35,000.00**
Lot # 2. Nederland	**$30,000.00**
Lot# 3. Mongolia	**$24,000.00**

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

Figure 9 - Stamp_insurance3.pdf email attachment.

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0054.jpg
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0065.jpg
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0071.jpg

Figures 10, 11 & 12 - The three stamps mentioned in Figure 9.

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 image of Tracy's iPhone contains no direct evidence implicating Tracy actively conspired in the defacement of the museum art. SMS and email messages between Tracy and Carrie show that Tracy knew she was breaching museum security by providing information on guard movement and by helping Carrie get her tablet into the gallery. However all collected evidence suggests Tracy was ignorant of Carrie's true motivations to use the innocent-sounding "flash mob" to deface the museum's art.

```
30 +12027252124 1342010505 I'm almost there where should I meet you?  2 0  5 0 0 4 0  us   1
31 +12027252124 1342010948 Just meet me out front, I'll take the tablet in. 3 0  5 0 0 4 0  us   0
32 +12027252124 1342112805 How's the flashmob going 3 0  5 0 0 0 0  us   0
```

Figure 13 - SMS messages sent from Tracy's Phone to Carrie

Plot Timeline

- 19 June 2012 - Pat replies to an email from Tracy in French, agreeing to her proposal and asking for Tracy to email him using her alias (“Coral”) so he can send instructions.
- 5 July 2012 - Carry makes initial email contact with Terry, requesting a lunch meet
- 6 July 2012 - Tracy emails Stamp Insurance PDFs to her own alias “Coral”
- 6 July 2012 - Carry and Tracy meet for lunch, discuss “flash mob event”
- 6 July 2012 - Tracy emails Carry thanking her for lunch
- 6 July 2012 - Pat makes initial email contact with King, requesting support for a heist and threatening to contact King’s parole officer if he refuses.
- 8 July 2012 - Tracy takes photos of rare stamps at the gallery
- 9 July 2012 - Carry emails Tracy, requesting Tracy get Carry’s tablet into the gallery for the flash mob and to pay Tracy for her help.
- 10 July 2012 - Tracy replies to Carry saying she can get the tablet into the gallery, and asks when Carry would like to access the gallery.
- 10 July 2012 - King replies to Pat by email, providing a list of equipment required to undertake the heist
- 10 July 2012 - Pat forwards the email from King to Tracy
- 11 July 2012 - Carry emails Tracy, requesting Museum guard schedules and offering money for the information
- 12 July 2012 - Tracy emails Carry, saying she’ll provide guard schedules

Conclusion

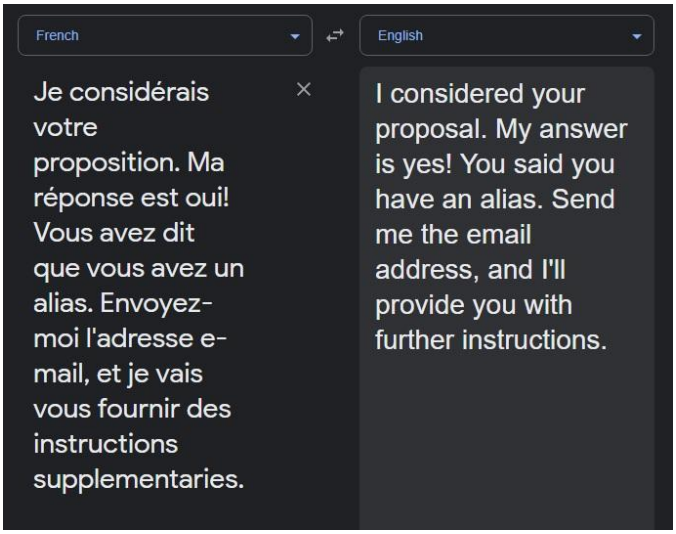
Evidence found on Tracy’s iPhone indicated the following:

- Pat and Tracy began conspiring to steal high-value items from the museum no later than 19 June 2012
- Pat and Tracy established aliases as “Perry” and “Coral” respectively, and created new email addresses with these aliases no later than 5 July 2012.
- Tracy collected insurance documents for high-value stamps displayed at the museum, and photographed the corresponding stamps on 8 July 2012
- Pat blackmailed parolee King into providing support to the heist on 6 July 2012
- King provided Pat a list of equipment required for a museum heist, and Pat forwarded this information on to Tracy with a request she would procure it.
- Tracy met with Carrie in person on 5 July 2012 and discussed Tracy providing support for an unsanctioned “flashmob” event at the museum organised by Carrie.
- Tracy agreed to smuggle Carrie’s tablet into the museum, and also provided museum guard schedules to Carrie.
- All recorded WiFi activity occurred in an area <290m East-West and <260m North-South, centered on the intersection of N Glebe Rd and 9 St N in West Arlington.

Appendix A: Correspondence Evidence

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

Table 1.2: Contents of Email

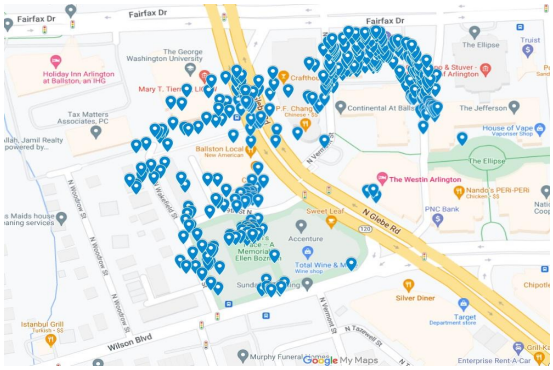
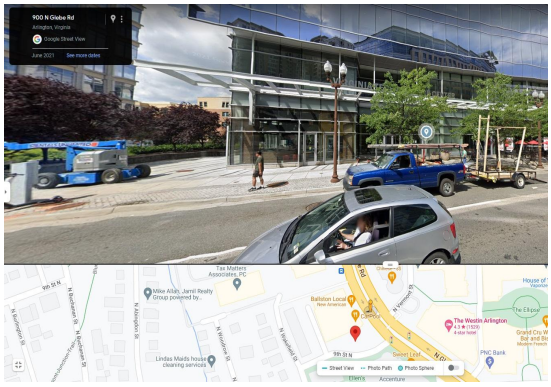
Timestamps	Header Information	Body
19JUN2012 16:06	“Paris Speak and answer” patsumtwelve@gmail.com to TracySumtwelve@gmail.com	Received: by 10.60.58.74 with HTTP; Tue, 19 Jun 2012 13:06:33 -0700 (PDT) Date: Tue, 19 Jun 2012 16:06:33 -0400 Message-ID: <CAA0mepmcN=zlRcEfU9v+CmJcNQViq5PFtOE761M2r=GYCjUyqA@mail.gmail.com> Subject: Paris Speak and answer From: Pat TeeSumTwelve <patsumtwelve@gmail.com> To: Tracy TeeSumTwelve <TracySumtwelve@gmail.com> Content-Type: multipart/alternative; boundary=f46d04478937ae6d9604c2d8d1a4 --f46d04478937ae6d9604c2d8d1a4 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: quoted-printable Tracy, Je consid=E9rais votre proposition. Ma r=E9ponse est oui! Vous avez dit que vous avez un alias. Envoyez-moi l'adresse e-mail, et je vais vous fournir des instructions suppl=E9mentaires. caresse --f46d04478937ae6d9604c2d8d1a4
19JUN2012 16:06	Translation of “Paris Speak and answer” patsumtwelve@gmail.com to TracySumtwelve@gmail.com	

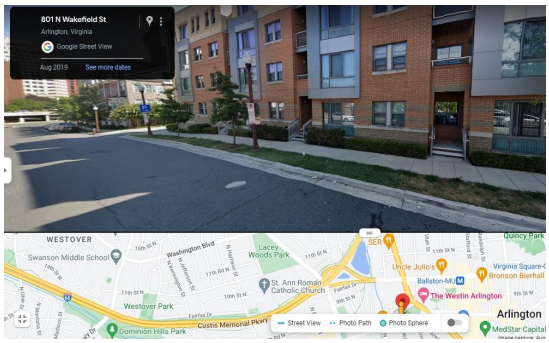
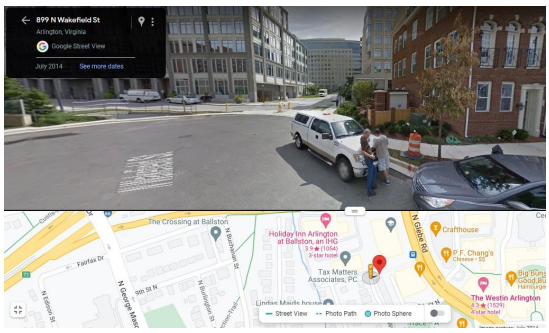
5JUL2012	carrysum2012@yahoo.com to TracySumtwelve@gmail.com	>> On Jul 5, 2012, at 11:51 AM, Carry Sumttventytwelve wrote:
		>>>
		>>> Hi,
		>>>
		>>> I saw on facebook that you were having a hard time lately, and i realized that we haven't spoken face to face in quite a while. I was really hoping that we could get together and have lunch. Does this Friday sound good? Let me know.
		>>>
		>>> -Carry

6JUL2012 11:49	“can’t pass up” patsumtwelve@gmail.com to throne1966@hotmail.com	
9JUL2012 14:18	“RE: Long time no see…” carrysum2012@yahoo.com to TracySumtwelve@gmail.com	>On Jul 9, 2012, at 2:18 PM, Carry Sumttwentytwelve wrote: >> Hey I was wondering >> if there was any way you could help me get my tablet into the gallery. I know security isn't to keen on computers and the like in the gallery, but maybe you could pull some strings and get it in for me? I can make it worth your while :) But really I would happy to get lunch again or something else for your help. I want to get some pictures for my flash mob event I told you about. Let me know. >> ------------------------------
10JUL2012 06:29	“RE: Long time no see…” TracySumtwelve@gmail.com to carrysum2012@yahoo.com	------------------------------ On Tue, Jul 10, 2012 6:29 AM PDT Tracy Sumtwelve wrote: >Hey, >I can definitely help get your tablet in. Our security guards can be pretty ridiculous sometimes! When would you want to get in and take a look around? >Tracy
10JUL2012 06:48	“RE: Long time no see…” carrysum2012@yahoo.com to TracySumtwelve@gmail.com	Date: Tue, 10 Jul 2012 06:48:40 -0700 (PDT) From: Carry Sumttwentytwelve <carrysum2012@yahoo.com> Subject: Re: Long time no see... To: tracysumtwelve@gmail.com MIME-Version: 1.0 Content-Type: text/plain; charset=us-ascii Awesome this will be a big help. Can i come in tommorrow, around 9? ------------------------------
10JUL2012 11:19	“RE: can’t pass up” throne1966@hotmail.com to patsumtwelve@gmail.com	

10JUL2012 11:19	“Fwd: can’t pass up” Attachment - Needs.txt patsumtwelve@gmail.com to coralbluetwo@hotmail.com	-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)
10JUL2012 11:24:57	“Fwd: can’t pass up” patsumtwelve@gmail.com to coralbluetwo@hotmail.com	Date: Tue, 10 Jul 2012 11:24:57 -0400 Message-ID: <CAA0mepmJ5+K6puFdL7GYC75pFyJ5HWDtJ3ANRW3d2dWP4Lo3dA@mail.gmail.com> Subject: Fwd: can't pass up From: Pat TeeSumTwelve <patsumtwelve@gmail.com> To: coralbluetwo@hotmail.com Content-Type: multipart/mixed; boundary=f46d0447963147823c04c47b5552 Return-Path: patsumtwelve@gmail.com X-OriginalArrivalTime: 10 Jul 2012 15:24:58.0245 (UTC) FILETIME=[2A69E350:01CD5E B0] --f46d0447963147823c04c47b5552 Content-Type: multipart/alternative; boundary=f46d0447963147823804c47b5550 --f46d0447963147823804c47b5550 Content-Type: text/plain; charset=windows-1252 Content-Transfer-Encoding: quoted-printable this is what we need to get for the guy thats going to make our job happen
11JUL2012 14:53	“RE: Long time no see…” carrysum2012@yahoo.com to TracySumtwelve@gmail.com	>On Wed, Jul 11, 2012 at 2:53 PM, Carry Sumttwentytwelve < >carrysum2012@yahoo.com> wrote: > >> >> >> Hey so i'm putting together this event we talked about and i want to make >> it as painless as possible. I know that your security folk sometimes get >> a little out of sorts. Is there a good time or maybe you could just let >> know the shift changes so you dont have to know when i am going to do this. >> I have a pretty good budget for the event if you would like a little >> something for the info. >>
12JUL2012 13:24	“RE: Long time no see…” TracySumtwelve@gmail.com to carrysum2012@yahoo.com	<tracysumtwelve@gmail.com> wrote: Okay carrie I'm going to send this but you need to make sure no one else sees it okay I could get in a bunch of trouble. I want to help you and I could really use some ex tra cash too but please please be careful.

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact	**Timestamp**	**Header**	**Body**	**Map Screenshot**
1	All Time	WiFi - Overview	All WiFi GeoLocations	Arlington, Washington D.C. 
2	3.61306882473715E8	WiFi	38.88055896, -77.11553561	900 N Glebe Rd 
3	3.61306882473715E8	WiFi	38.88106083, -77.11533838	P.F Chang's Restuarant 

4	3.61306882473715E8	WiFi	38.88005346, -77.11595332	801 N Wakefield St 
5	3.61306882473715E8	WiFi	38.88093715, -77.11640596	899 N Wakefield St 
6	3.61306882473715E8	WiFi	38.88139647, -77.11564362	950 N Glebe Rd