



Cybersecurity

21.3 The Final Report

Case Report

National Gallery DC

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

Team Members-Aakhil Kassim, Timin Thaver and Brenda Schecher

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.

- Tracy used the alias "Coral" to have email communication with Pat (alias: Perry) who is Tracy's brother. Perry provided instructions on how to set up virtual machines to isolate their suspicious activities.
 - The instructions were masked behind a seemingly innocuous MP3 file which lends to the idea that they have something to hide.
- Tracy is directly connected to the "Coral" alias because her text messages with Pat about email attachments match the activity on the coralbluetwo@hotmail.com email address.
 - Tracy emails herself to the Coral mail account to save some files related to stamp insurance. This activity is suspicious because attempts have been made to encrypt the files and the files provide evidence related to the theft of the valuable stamps.
 - Pictures of the stamps in Tracy's photos indicate the coordinates of the National Gallery.
 - Group email to King giving details about the theft at the National Gallery is evidence of the theft of valuable stamps.
- Tracy and Carry arranged a meeting at a restaurant. This interaction later transpired into Carry meeting Tracy at the National Gallery where Carry would give Tracy a tablet computer to help with the "flash mob."
 - There is no other evidence obtained to indicate Tracy was a part of the flash mob.
- The conversations found between Tracy and her daughter Terry are not part of the suspicious activity. However, the text messages with Terry reveal a weak relationship. This stressful situation also likely contributed to Tracy's overall willingness to involve herself in criminal activity.

Equipment and Tools

- Kali Linux
- Sqlite Browser (DB Browser for SQLite)
- Google Maps/Google Earth
- Nano (text edit)
- Note Pad
- GNU Coreutils (grep, awk, date, etc)
- Autopsy 4.10 (Based on The Sleuth Kit 4.6.5)
- Vim Editor (to separate base64 blobs from eml files)
- fcrackzip
- <https://www.gaijin.at/en/tools/time-converter> (to convert GPS CFAbsoluteTime)

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 3G	vol_vol5/logs/AppleSupport/general.log
Host Name	Tracysumtwelves iphone	vol_vol5/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	vol_vol5/logs/AppleSupport/general.log
Install Time	06/06/2012 12: 03:28	vol_vol5/logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	vol_vol5/mobile/Library/Mail/IMAP-*
Phone Number	703-340-9961	vol_vol5/logs/lockdownd.log
Serial Number	86004482Y7H	vol_vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/wireless/Library/logs/lockdown.log
IMEI	012021003735398	vol_vol5/root/Library/Lockdown/activation_records/wild card_record.plist
MD5 Hash	34c4888f095dc3241330462923f6 fea5	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f 52d6577ccb534ca0d1e83ffd2768 3e621607	

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
Alias Email	coralbluetwo@hotmail.com
Relationship:	Accused (alias Coral)

Pat:

Phone Number:	571-308-3236
Email:	patsumtwelve@gmail.com
Alias Email:	perrypatsum@yahoo.com
Relationship:	Tracy's brother (alias Perry)

Terry:

Phone Number:	703-829-6071
Email:	Unknown
Relationship:	Daughter of Tracy

Joe:

Phone Number:	Unknown
Email:	Unknown
Relationship:	Ex Husband

Carry:

Phone Number: 202-725-2124
Email: Unknown
Relationship: Ties with Alex and Tracy

King:

Phone Number: N/A
Email: throne1966@hotmail.com
Relationship: He is the burglar that is set to do the heist.

Conclusions:

- Pat and Tracy conspired over Email. Both made attempts to mask their activity when using Email technology.
- Tracy's weakening familial relations with Terry and Joe appear to have motivated her to criminal activity for financial gain to provide for her daughter and improve their relationship.
- Tracy and Carry likely discussed their criminal plans against the National Gallery at the restaurant.
- King is enlisted to help them with stealing stamps at the National Gallery. Tracy works at the National Gallery.

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 from Appendix A:

→ Artifact: EMAIL-03

- ◆ Tracy sends an email to herself from her personal gmail account to the coralbluetwo hotmail account. Two files are attached, documents.zip and docs.zip. The documents.zip file is encrypted which suggests Tracy wants to hide this resource. Nonetheless both zip files contain PDF files related to stamp insurance. **This is suspicious activity that suggests she is involved in planning illicit activities related to stamps.**

→ Artifact: EMAIL-04

- ◆ This email shows the communication between Pat, King, and Tracy discussing the heist, and the tools required to carry it out (contained in the needs.txt PDF file).

→ Artifact: TXT-PAT-07

- ◆ In this text message, Pat tells Tracy to tell Coral to change the attachment extension to PDF. This message refers to the attachment (needs.txt) sent by King in EMAIL-04, which contains a list of tools needed for the heist. **This confirms Tracy's involvement.**

Evidence from Appendix B:

- GPS and Wifi/Cellular information for the months of June and July place Tracy in and around the National Gallery for meetings and heist.
- Artifact 10 Shows Tracy's Cellular Location was at the National Gallery on the weekend before the heist.

Evidence from Appendix C:

- Pictures of the National Gallery stamps and associated insurance docs were found in Tracy's possession.

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 from Appendix A:

- Artifact: TXT-CARRY-05
 - ◆ Carry informs Tracy that she is "almost there," likely referring to the National Gallery. Carry then asks where she should meet Tracy.
 - ◆ This message suggests that Tracy and Carry have planned to meet at the National Gallery for some reason, which must be related to the defacement of museum art.
- Artifact: TXT-CARRY-06
 - ◆ In response to Carry's previous message, Tracy instructs Carry to meet her at the front of the Gallery. Tracy also mentions that she will take Carry's tablet inside the Gallery.
 - ◆ This confirms Tracy's involvement with Carry.
- Artifact: TXT-CARRY-07
 - ◆ In this text message, Tracy asks Carry about how the flash mob is going.
 - ◆ The flash mob at the Gallery was planned as a diversion to cover for the defacement of museum art.

Evidence from Appendix B:

- Artifact 10: Primary evidence that Tracy visited the National Gallery on the weekend before the flash mob.
- GPS and Wifi/Cellular information for the months of June and July place Tracy in and around the National Gallery for meetings and heist.

Plot Timeline

- Tue 19 Jun 2012 - EMAIL-01:
 - ◆ Perry tells Coral to listen to an mp3 file called Crazydave1.mp3, which contains hidden instructions on setting up VirtualBox for a "big lived project."
- Thu 05 Jul 2012 - TXT-CARRY-01:
 - ◆ Carry wants to meet Tracy at 1 pm at Bubba's Grill.
- Thu 05 Jul 2012 - TXT-CARRY-02:
 - ◆ Tracy agrees to meet Carry. (They eventually get a table and meet)
- Fri 06 Jul 2012 - TXT-PAT-03:
 - ◆ Tracy asks Pat to call her.
- Fri 06 Jul 2012 - TXT-PAT-06:
 - ◆ Pat will call Tracy in 5 minutes.
- Mon 09 Jul 2012 - EMAIL-03:
 - ◆ Tracy sends herself encrypted documents about stamp insurance.
- Tue 10 Jul 2012 - EMAIL-04:
 - ◆ Pat contacts King who forwards the needed tools list for the heist at the National Gallery to Tracy (Coral).
- Tue 10 Jul 2012 - TXT-PAT-07:
 - ◆ Pat tells Tracy to tell Coral to change the attachment extension to PDF
- Tue 10 Jul 2012 - TXT-PAT-08:
 - ◆ Tracy says she will get on it (the email attachment). - confirms involvement.
- Wed 11 Jul 2012 - TXT-CARRY-05:
 - ◆ Carry is "almost there" (likely the National Gallery) and asks where to meet Tracy.
- Wed 11 Jul 2012 - TXT-CARRY-06:
 - ◆ Tracy tells Carry to meet her at the front of the Gallery and will take Carry's tablet in.
- Thu 12 Jul 2012 - TXT-CARRY-07:
 - ◆ Tracy asks how the flash mob is going.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

Tracy is involved in suspicious activities with Pat and Carry.

- Tracy used the alias Coral, Pat used the alias Perry
- Tracy and Pat conspired to steal stamps
- Tracy sent herself encrypted documents about stamp insurance
- King agreed to help with the heist and provided a list of needed tools.
- Tracy communicated with Carry about the National Gallery
- Discussions with Carry included meeting locations and the flash mob event

The evidence above points to Tracy's involvement in criminal activities under investigation

Using email account aliases, Tracy and Pat plotted together. Pat used the email address 'patsumtwelve@gmail.com' instead of his usual email address 'perryatsum@yahoo.com', while Tracy used 'coralbluetwo@hotmail.com' instead of her 'tracysumtwelve@gmail.com'. Their scheme involved stealing valuable stamps with the help of a known criminal named King who has an email address of 'throne1966@hotmail.com'. Pat, who has connections with King's parole officer, was able to influence him.

Meanwhile, Tracy collaborated with Carry to deliver a notebook containing data relevant to a flash mob Carry wants to orchestrate. This would distract the museum's security guards while King carries out the theft. Tracy sent herself documents related to the stamps, including their insurance value. Additionally, Tracy received a notification about a \$1000 'Gift Card' from a website that appears to be from Target but is actually located on the trdt.biz domain. The source of this payment is unclear at this time, but it is likely from either Carry via Alex or directly from Alex.

Appendix A: Correspondence Evidence

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

Group members: Aakhil Kassim, Brenda Schecher, and Timin Thaver

Email Messages

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
01	06/19/2012 14:39:00 PTD	From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: received email.	Perry emails Coral (Tracy) saying he got her email. asking her to check out a song by the VMs. He loves the base. The Crazydave1.mp3 file was used to mask secret instructions on how to install virtual machines with virtualbox to share a project called "biglived".	INBOX.mbox /Messages EMLX File: 3896FC6F-A083-4D39-B0A2-CE68368D44CA.eml x
02	07/06/2012 11:49:31	From: patsumtwelve@gmail.com To: throne1966@hotmail.com cc: coralbluetwo@hotmail.com Subject: Cant pass up	Pat (Perry) indicates he will be doing a heist in two weeks and needs King's (Kart) help. original email to King asking for help to do the heist attachment: needs.txt	INBOX.mbox /Messages EMLX File: 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.eml x
03	07/09/2012 07:47:58 PTD	From: tracysumtwelve@gmail.com To: Coralbluetwo@hotmail.com Subject:somethings	Tracy sends email to herself documents labeled in a documents.zip file. Attachment documents.zip	INBOX.mbox /Messages EMLX File: 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.eml lx
04	07/10/2012	From:	Pat (Perry)forward an email to Coral	INBOX.mbox

	2 8:24:57 PTD original email- 07/10/201 2 11: 19 AM	patsumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: Re: Cant Pass Up Attachments- needs.txt forwarded email from patsumtwelve@gmail addressed to throne1966@hotmail.com	(Tracy) showing the attachment of what is needed to provide King (Kart) so he can do the heist. Attachment needs.txt	/Messages EMLX File: 9F0508B8-0 4FB-490E-A 7F0-3E23B0 E7C59B.eml x
05	07/10/201 2 :11:19 AM	From: throne1966@hotmail.com To: patsumtwelve@gmail.com Re: Cant pass up attachment needs.txt	King (Kart) kthings responds to Pat indicating he needs some tools and attaches	INBOX.mbox /Messages EMLX File: 9F0508B8-0 4FB-490E-A 7F0-3E23B0 E7C59B.eml x

Text Messages

Text Message Timeline of NGDC				
Artifact ID	Timestamp	Header Information	Key Information	Evidence Location
TXT PAT-01	Tue 12 Jun 2012 05:25:04 PM EDT	From: Pat To: Tracy	Pat asks about Tracy's weekend plans	sms.db
TXT PAT-02	Wed 13 Jun 2012 02:30:38 PM EDT	From: Tracy To: Pat	Tracy has no big plans.	sms.db
TXT PAT-03	Fri 06 Jul 2012 11:02:19 AM EDT	From: Tracy To: Pat	Tracy asks Pat to call her.	sms.db
TXT PAT-04	Fri 06 Jul 2012 11:08:37 AM EDT	From: Pat To: Tracy	Pat is busy and cannot call Tracy until later.	sms.db

TXT PAT-05	Fri 06 Jul 2012 11:11:54 AM EDT	From: Tracy To: Pat	Tracy demands that they call soon to discuss something important.	sms.db
TXT PAT-06	Fri 06 Jul 2012 11:13:31 AM EDT	From: Pat To: Tracy	Pat will call Tracy in 5 minutes.	sms.db

TXT PAT-07	Tue 10 Jul 2012 11:26:19 AM EDT	From: Pat To: Tracy	Pat tells Tracy to tell Coral to change the attachment extension to PDF.	sms.db
TXT PAT-08	Tue 10 Jul 2012 11:58:04 AM EDT	From: Tracy To: Pat	Tracy says she will get on it (the email attachment)	sms.db
TXT TERRY-0 1	Wed 13 Jun 2012 01:30:28 PM EDT	From: Terry To: Tracy	Terry informs Tracy that she is going out for pizza and not to cook for her.	sms.db
TXT TERRY-0 2	Wed 13 Jun 2012 02:33:46 PM EDT	From: Tracy To: Terry	Tracy acknowledges.	sms.db
TXT TERRY-0 3	Tue 03 Jul 2012 09:41:51 AM EDT	From Tracy To: Terry	Tracy asks Terry about switching schools due to financial troubles.	sms.db
TXT TERRY-0 4	Tue 03 Jul 2012 10:04:32 AM EDT	From: Terry To: Tracy	Terry does not want to change schools and would rather stay with her Dad (Joe) to continue the same school.	sms.db
TXT TERRY-0 4	Tue 10 Jul 2012 01:18:38 PM EDT	From: Tracy To: Terry	Tracy asks Terry to join her for lunch.	sms.db
TXT TERRY-0 5	Tue 10 Jul 2012 02:19:24 PM EDT	From: Tracy To: Terry	Tracy is back at work after lunch alone.	sms.db
TXT TERRY-0 6	Tue 10 Jul 2012 02:58:24 PM EDT	From: Terry To: Tracy	Terry was busy and can only meet the upcoming weekend if her dad (Joe) isn't busy.	sms.db
TXT TERRY-0 7	Thu 12 Jul 2012 09:02:10 PM EDT	From: Terry To: Tracy	Terry really wants to go to her Dad's place so she can go shopping for school.	sms.db

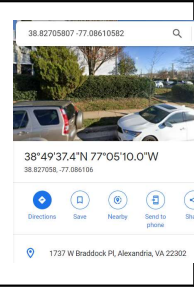
TXT CARRY-0 1	Thu 05 Jul 2012 02:18:23 PM EDT	From: Carry To: Tracy	Carry wants to meet Tracy at 1pm at Bubba's Grill.	sms.db
TXT CARRY-0 2	Thu 05 Jul 2012 02:20:26 PM EDT	From: Tracy To: Carry	Tracy agrees to meet Carry.	sms.db
TXT CARRY-0 3	Fri 06 Jul 2012 12:27:16 PM EDT	From: Carry To: Tracy	It's the next day. Carry tells Tracy she has a table at the restaurant.	sms.db
TXT CARRY-0 4	Fri 06 Jul 2012 12:27:50 PM EDT	From: Tracy To: Carry	Tracy says she will be right there.	sms.db
TXT CARRY-0 5	Wed 11 Jul 2012 08:41:45 AM EDT	From: Carry To: Tracy	Carry is "almost there", likely the National Gallery. Carry asks where she should meet Tracy.	sms.db
TXT CARRY-0 6	Wed 11 Jul 2012 08:49:08 AM EDT	From: Tracy To: Carry	Tracy tells Carry to meet her out at the front of the Gallery. Tracy will take Carry's tablet in.	sms.db
TXT CARRY-0 7	Thu 12 Jul 2012 01:06:45 PM EDT	From: Tracy To: Carry	Tracy asks how the flash mob is going.	sms.db
TXT CARRY-0 8	Fri 13 Jul 2012	From: Terry To: Carry	Terry wants to go to her dad's for the weekend to do school shopping	sms.db

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1	Wed, 2012-06-13 15:01:22 EDT	Wifi Location	Coordinates are 38.88055896, -77.11553561 Near Virginia Tech Research Center 900 N Grebe Road Arlington, VA 22203	
2	Wed, 2012-06-13 15:01:22 EDT	Wifi Location	Coordinates are 38.88106083, -77.11533838 Near Virginia Tech Research Center 901 N. Grebe Road Arlington, VA 22203	
3	Wed, 2012-06-13 15:01:22 EDT	Wifi Location	Coordinates are 38.8805346, -77.11595332 Near Virginia Tech Research Center 900 N Grebe Road Arlington, VA 22203	

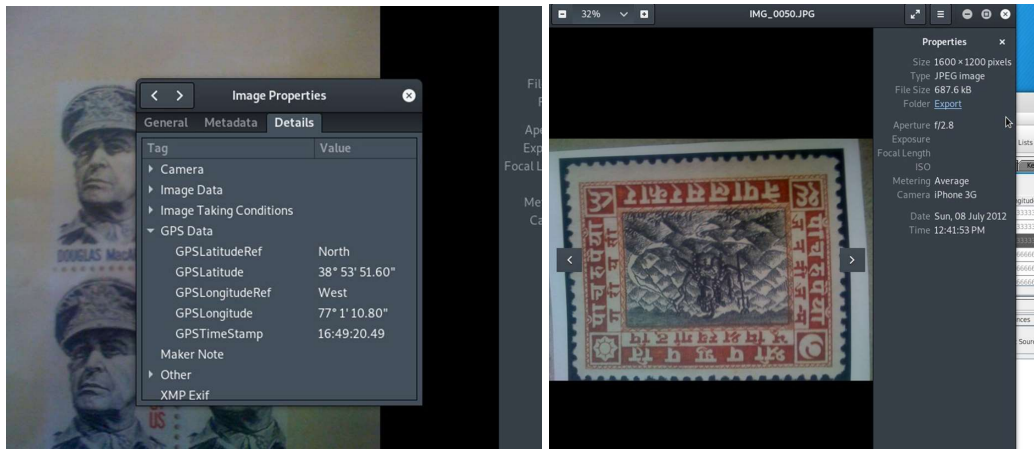
4	Wed, 2012-06-13 15:01:22 EDT	Wifi Location	Coordinates are 38.87974703 -77.11598318 Near The Jordan Apartments 801 N Wakefield Street Arlington, VA 22203	
5	Wed, 2012-06-13 15:04:03 EDT	Wifi Location	Coordinates are 38.88143724, -77.11478394 Close to P.F. Chang's 901 N Vermont Street Arlington, VA 22201	
6	Wed, 2012-06-13 15:01 EDT	Cell Location	Coordinates are 38.87767624 -77.11546951 621 N Wakefield St, Arlington, VA 22203	
7	Sat, 2012-06-23 13:12:16 EDT	Cell Location (Local)	Coordinates are 38.9048634166667 -77.0483737833333 2150 M St NW, Washington, DC 20037	
8	Mon, 2012-07-02 12:19:23 EDT	Cell Location	Coordinates are 38.88092339 -77.11709934 4600 Fairfax Drive Arlington, VA 22203	

9	Thu, 2012-07-05 12:32:46 EDT	Cell Location	Coordinates are 38.87948584 -77.11460208 Arlington, VA	 A screenshot of a Google Maps interface showing a location in Arlington, VA. The map displays a street view of a construction site with orange safety barriers. The coordinates 38°52'46.2"N 77°06'52.6"W are shown, along with the address Arlington, VA 22203. Navigation and sharing options are visible at the bottom.
10	Sun, 2012-07-08 12:34:40 EDT	Cell Location (Local)	Coordinates are 38.8917478666667 -77.0234627166667 National Gallery of Art, Washington, DC 20004	 A screenshot of a Google Maps interface showing the National Gallery of Art in Washington, DC. The map shows a large, modern building with a glass facade. The coordinates 38°53'30.3"N 77°01'24.5"W are displayed, along with the address National Gallery of Art, Washington, DC 20004. Navigation and sharing options are visible at the bottom.
11	Sun, 2012-07-08 12:39:10 EDT	Cell Location (Local)	Coordinates are 38.8908919333333 -77.02163135 Northwest Washington, Washington, DC	 A screenshot of a Google Maps interface showing a location in Northwest Washington, DC. The map displays a large, modern building with a glass facade. The coordinates 38°53'27.2"N 77°01'17.9"W are shown, along with the address Northwest Washington, Washington, DC. Navigation and sharing options are visible at the bottom.
12	Tue, 2012-07-10 12:47:12 EDT	Cell Location (Local)	Coordinates are 38.8287627666667 -77.0859360666667 Alexandria City Public Schools, Alexandria, VA	 A screenshot of a Google Maps interface showing a location in Alexandria, VA. The map displays a large, modern building with a glass facade. The coordinates 38°49'43.6"N 77°05'09.4"W are shown, along with the address Alexandria City Public Schools, Alexandria, VA. Navigation and sharing options are visible at the bottom.
13	Tue, 2012-07-10 12:31 EDT	Cell Location	Coordinates are 38.85141718 -77.07823592 1700 Army Navy Dr, Arlington, VA 22202	 A screenshot of a Google Maps interface showing a location in Arlington, VA. The map displays a large, modern building with a glass facade. The coordinates 38°51'05.1"N 77°04'41.7"W are shown, along with the address 1700 Army Navy Dr, Arlington, VA 22202. Navigation and sharing options are visible at the bottom.

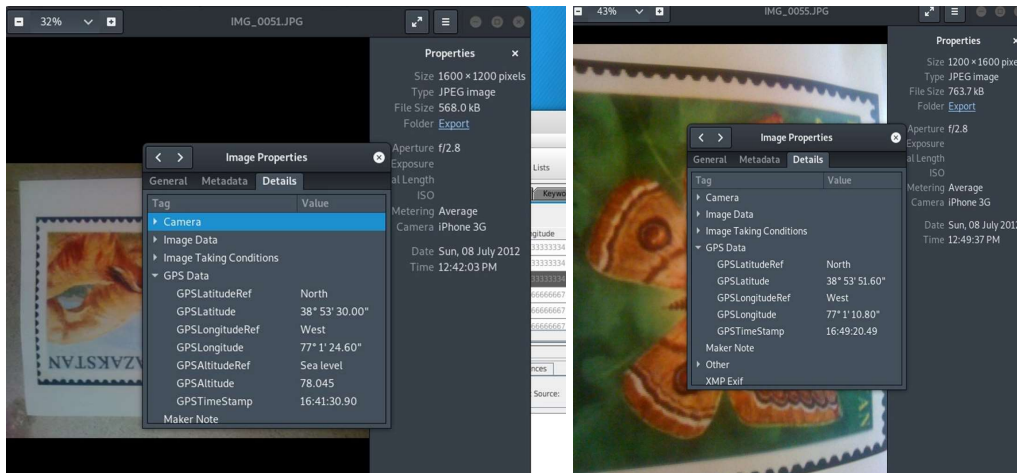
14	Tue, 2012-07-10 12:44 EDT	Cell Location	Coordinates are 38.82705807 -77.08610582	
----	---------------------------------	---------------	--	---

Appendix C: Picture Evidence–Stamps & Stamp Insurance Papers

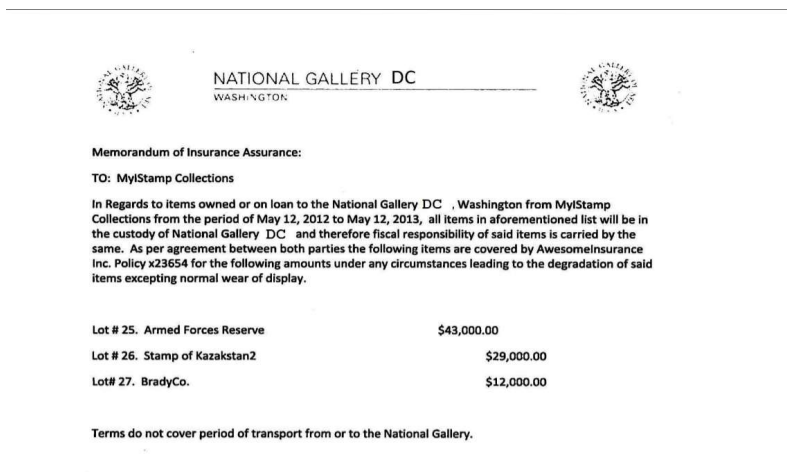
Picture of stamps, coordinates and times
Coordinates embedded in pictures is address for National Gallery



Coordinates for National Gallery



Pictures of Stamp Insurance Documents





NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MylStamp 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.

Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC, Washington from MylStamp 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