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.

During the investigation multiple incriminating correspondence were discovered between Tracy and what appears to be multiple other conspirators, via both email and text message. Tracy appears to be taking an active role in the organization of the alleged acts.

Equipment and Tools

Autopsy was used to view the contents of the devices WITHOUT writing to them as to preserve the data and it's integrity.
Sqlitebrowser is a terminal service used to easily rummage through sql code and view it in an easier to read fashion.

Details of Tracy's iPhone

Device Model: It believes its an Iphone 1 or 2 (Found in general.log in the Logs Folder)

OS version #: iphoneos4.2.1 (Found in general.log in the Logs Folder)

Device host name: Tracy Sumtwelves Iphone (Found in lockdownd.log.1 in logs)

Device Serial #: 86004482Y7H (Found in general.log in the Logs Folder)

Install Time: 6/6/2012 12:03:28 -0700 (Found in general.log in the Logs Folder)

ICCID: 89014103255195342366 (Found in lockdownd.log.1 in the logs folder under crash reporter)

IMEI: 01202100373598 (Found in root/library/lockdown/activation_records/wildcard_record.plist)

Phone number: 1 (703) 340-9661 (Found in lockdownd.log.1 in the logs folder under crash reporter)

Email Address: tracysumtwelve@gmail.com (found in com.apple.accountsetting.plist)

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: Patsumtwelve@gmail.com , Perrypatsum@yahoo.com
Relationship: Brother to Tracy

Terry:

Phone Number: (703) -829-6071
Email:
Relationship: Child of Tracy

Joe:

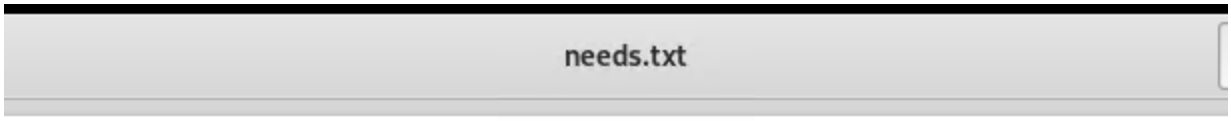
Phone Number: (703) 829-6191 (ASSUMPTION BASED ON KNOWN INFO)
Email:
Relationship: Husband of Tracy

Carry:

Phone Number: (202) 725-2124
Email: Carrysum2012@yahoo.com
Relationship:

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.
Tracy, Pat, and Carry conspired with an unknown entity known as “King” with the email address Throne1966@hotmail.com to rob the gallery. King replied with a list of items needed for a heist.



-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)

Further findings showed insurance documents on the phone as shown below.

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

Stamp Insurance 2.pdf 100%

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

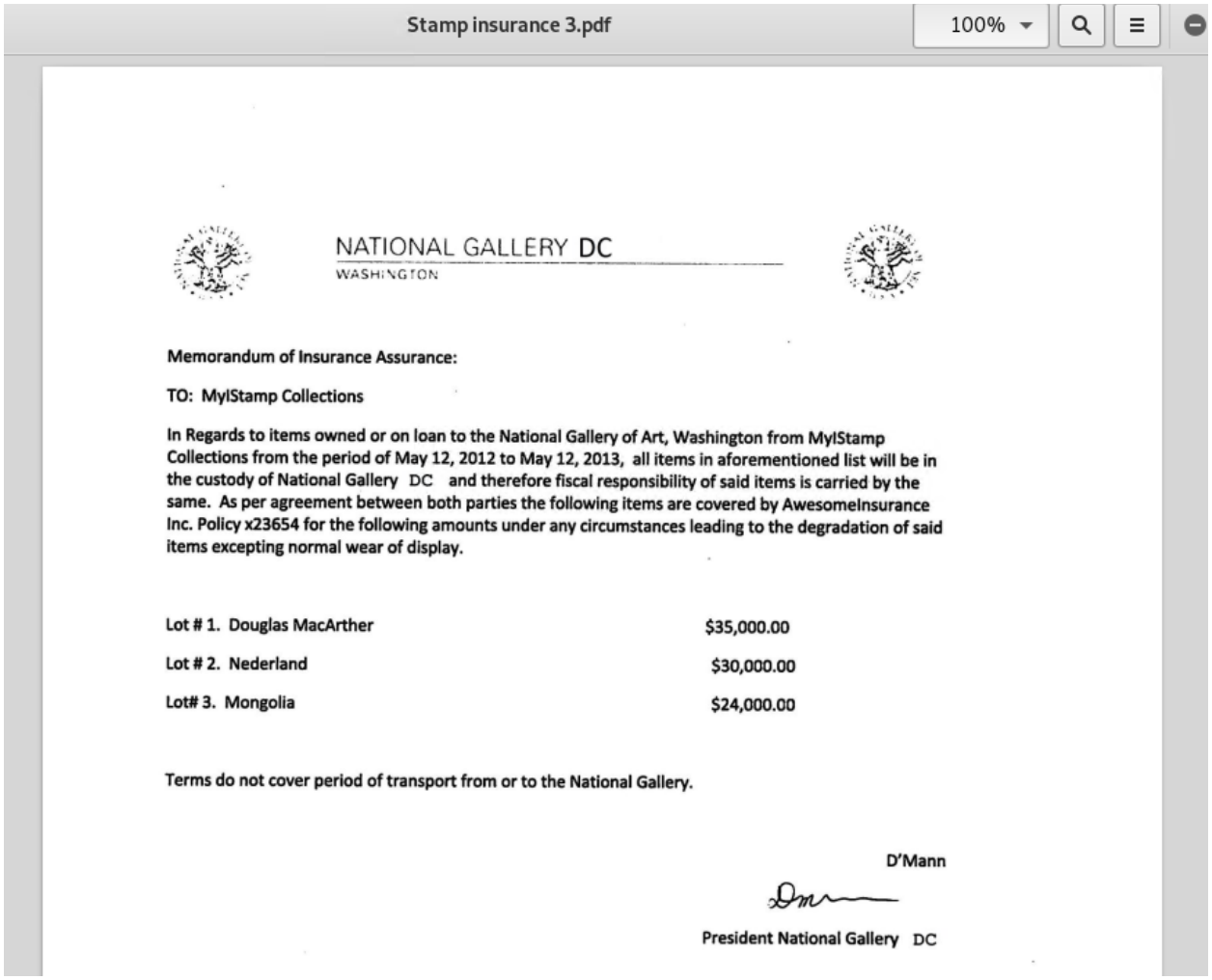
In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. 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


Stamp insurance 3.pdf

100%

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.

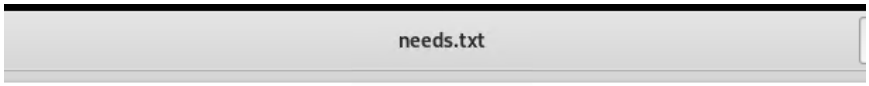
D'Mann

President National Gallery DC

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.

During our search we found evidence of what is needed to get into the museum including spray paint to deal with the cameras.



-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)

Plot Timeline

[Provide an outline of the key events in the order they occurred. Note the date of each event.]

Date	Key Information
June 19th, 2012	Pat sends Tracy information about a virtual machine.
July 5th, 2012	Text messages between Tracy and Carry about meeting up at Buuba's Grill for lunch.
July 6th, 2012	Tracy and Carry meet for lunch at Bubba's Grill.
July 6th, 2012 through July 10th, 2012	Correspondences between Pat, Tracy, and King about the upcoming stamp heist.
July 8th, 2012	Tracy photographed several stamps they're interested in stealing.
July 9th, 2012	Tracy makes copies of memos containing insurance information for the stamps they plan to steal.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Email between "coralbluetwo@hotmail.com" and Tracy
- [For example: Tracy used the alias Coral and Pat used the alias Perry.]
- There was an MP3 file uncovered in an attachment sent from Pat to Tracy informing her on how to create a Virtual Machine.
- There were 3 different documents on Tracys phone regarding insurance information on the stamps.

Appendix A: Correspondence Evidence

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

https://docs.google.com/document/d/1A2EoSubgCoM7sbAtMnoKeWn3MHQdL4fHHPHWHEO3jlA/edit?usp=sharing

Correspondence Evidence

Group members:

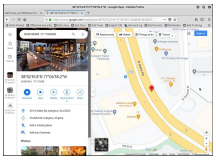
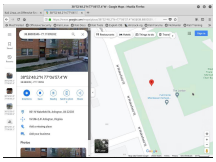
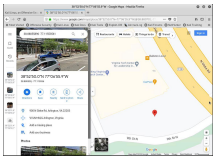
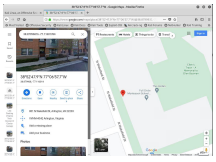
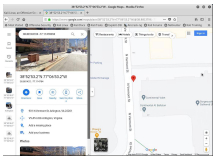
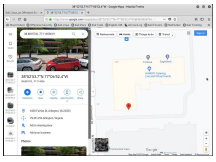
Brandon Dash Patrick Evan Michael Matthew

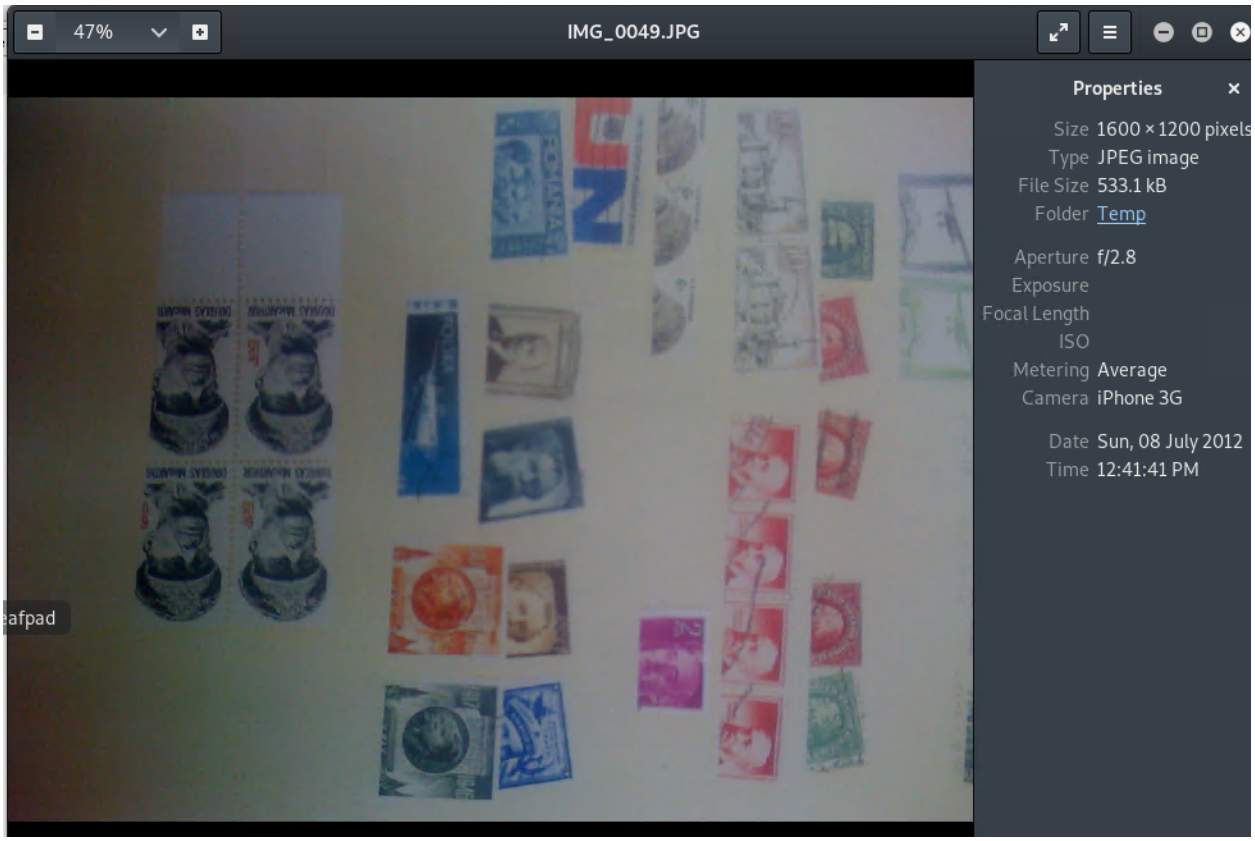
Master Timeline of NGDC				
Artifact #	**Timestamp**	**Header Information**	**Key Information**	**Evidence Location**
1.	07/11/12 @ 4:18 am	microsoft@reply.digitalriver.com Sub: Only 30 days left! Start a free office training course now. coralbluetwo@hotmail.com	Scam email	01fe9965-a903-40cf-a78a-72ce3bd26571.emlx
2.	07/10/12 @ 8:24 am -0700	from:patsumtwelve@gmail.com SUB: FWD can't pass up to : coralbluetwo@hotmail.com	Pat relayed the information to tracy regarding the tools needed for the heist.	9f0508b8-04fb-490-a7f0-3e23b0e7c59b.emlx
3.	07/10/12 @	From :throne1966@hotmail.com	King responds with an attachment indicating	9f0508b8-04fb-

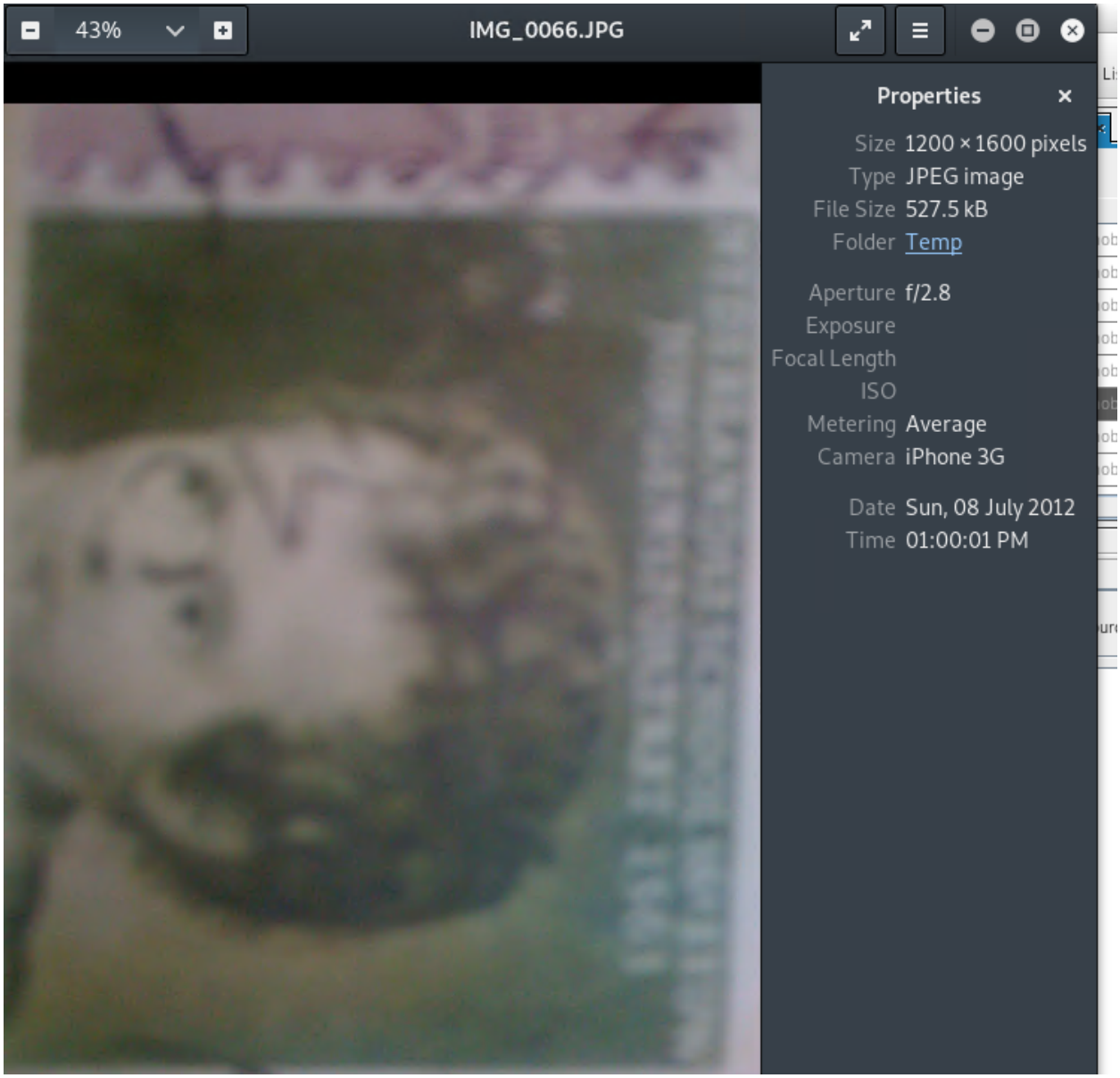
	11:19 am	Sub: re- Can't pass up to : Patsumtwelve@gmail.com	tools to do the job	490-a7f0-3e23b 0e7c59b.emlx
4.	07/06/12 @ 11:49 am	from : patsumtwelve@gmail.com Sub: Can't pass up to : Throne1966@hotmail.com CC: coralbluetwo@hotmail.com	Pat is blackmailing king to assist in getting tools for a heist	9f0508b8-04fb- 490-a7f0-3e23b 0e7c59b.emlx
5.	Rec: 07/09/12 @ 7:47 am	From tracysumtwelve@gmail.com Sub: things To: coralbluetwo@hotmail.com	Attachments including password protected documents.	8a3bd06f-cbd1- 4453-9c69-77e 06823f2ae.emlx
6.	6/12/12 9:25 pm	From: Pat 571-308-3236 To: Tracy	Pat asked "what are you up to this weekend?"	SMS.db
7.	6/13/12 6:30 pm	From: Tracy To: Pat	Tracy replied " I don't have any big plans. How about you?"	SMS.db
8.	7/5/12 6:18 pm	From: Carry 202-725-2124 To: Tracy	Carry set up a meeting plan to be at Bubbas Grill at 1pm	SMS.db
9.	7/5/12 6:20 pm	From: Tracy To: Carry	Tracy has agreed to the meeting	SMS.db
10.	7/6/12 3:02 pm	From: Tracy To: Pat	"Hey can you give me a call"	SMS.db
11.	7/6/12 3:08 pm	From: Pat To: Tracy	"Sis I'm really busy can we do this later"	SMS.db
12	7/6/12 3:11 pm	From: Tracy To: Pat	"No Pat this is important i need you to call me soon"	SMS.db
13	7/6/12	From: Pat	" ok ok I'll call in 5"	SMS.db

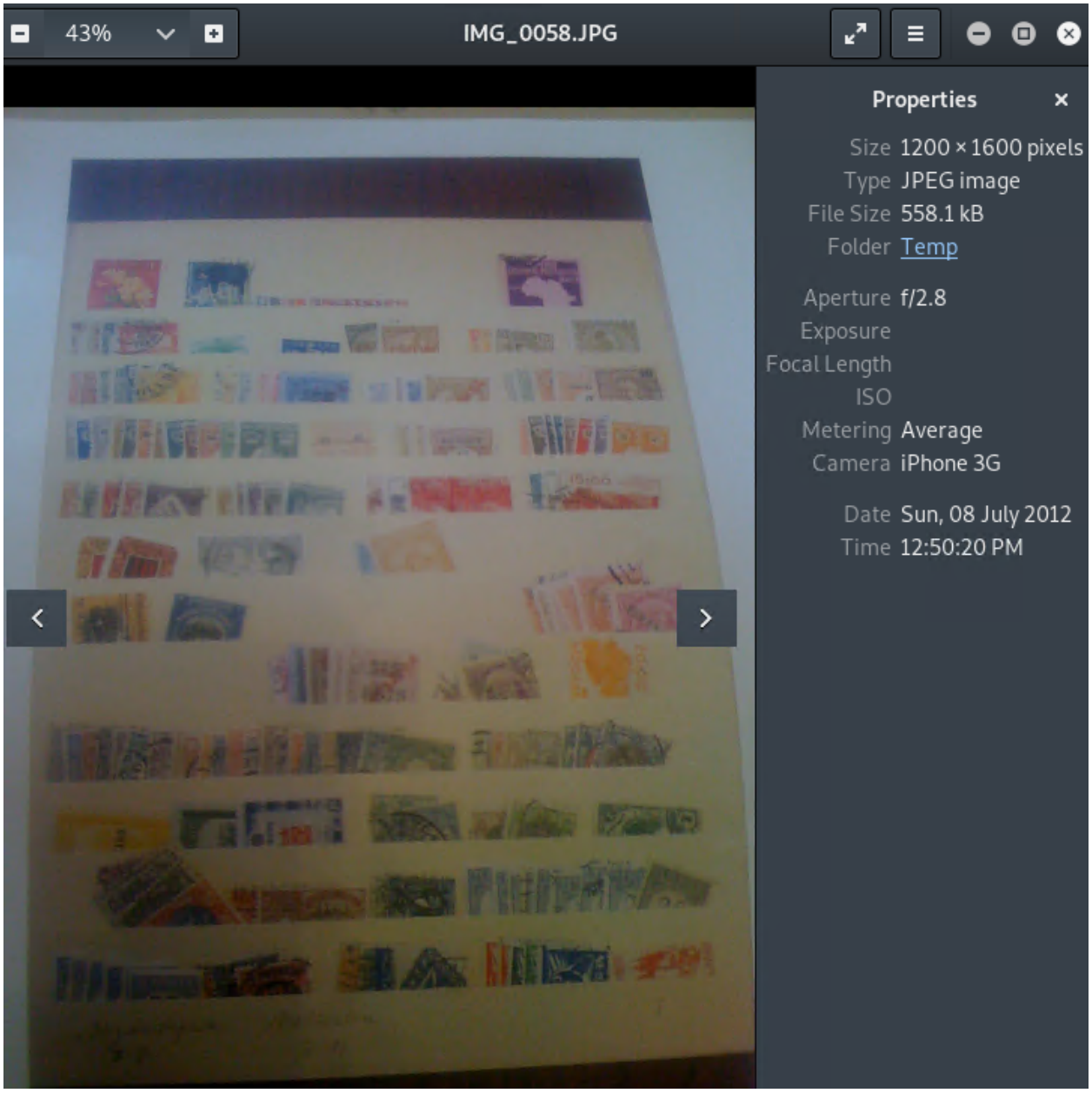
	3:13pm	To: Tracy		
14	7/6/12 3/18/12	Call from Pat	This call lasted 4 minutes and 4 seconds	Call_history.db
15	7/10/12 3:26 pm	From: Pat To: Tracy	"Hey sis yo friend coral got a email the attachment needs changed to pdf let her know"	SMS.db
16	7/10/12 3:58 pm	From: Tracy To: Pat	"Sure thing I'll get on it"	SMS.db
17	7/11/12 12:41 pm	From: Carry To: Tracy	"I'm almost there where should I meet you?"	SMS.db
18	7/11/12 12:49 pm	From Tracy To Carry	"Just meet me out front. I'll take the tablet in"	SMS .db
19	7/12/12 5:06 pm	From: Tracy To: Carry	" How's the flashmob going"	SMS.db
20	7/7/12 7:36 pm	From 206-910-0932 Unknown To : Tracy	"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"	SMS.db

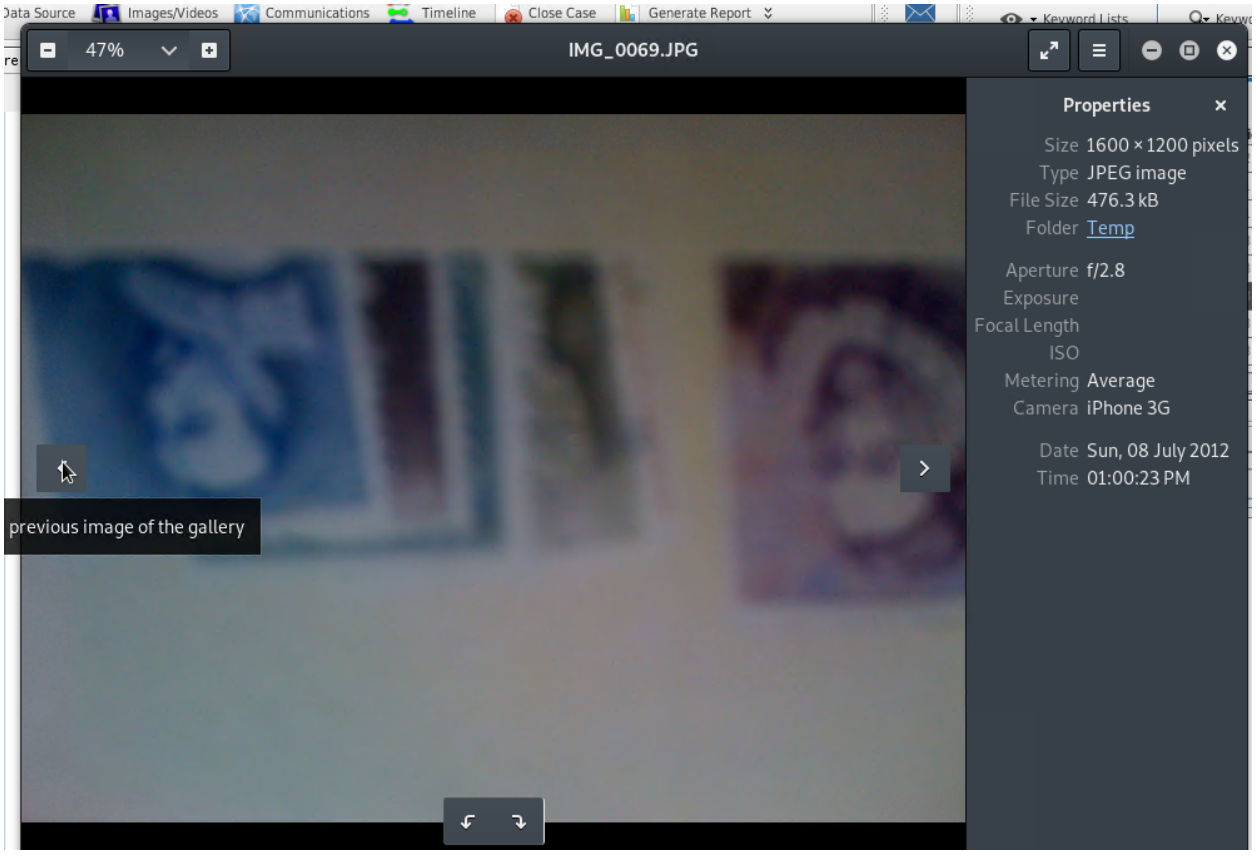
Appendix B: WiFi and GPS Location Information

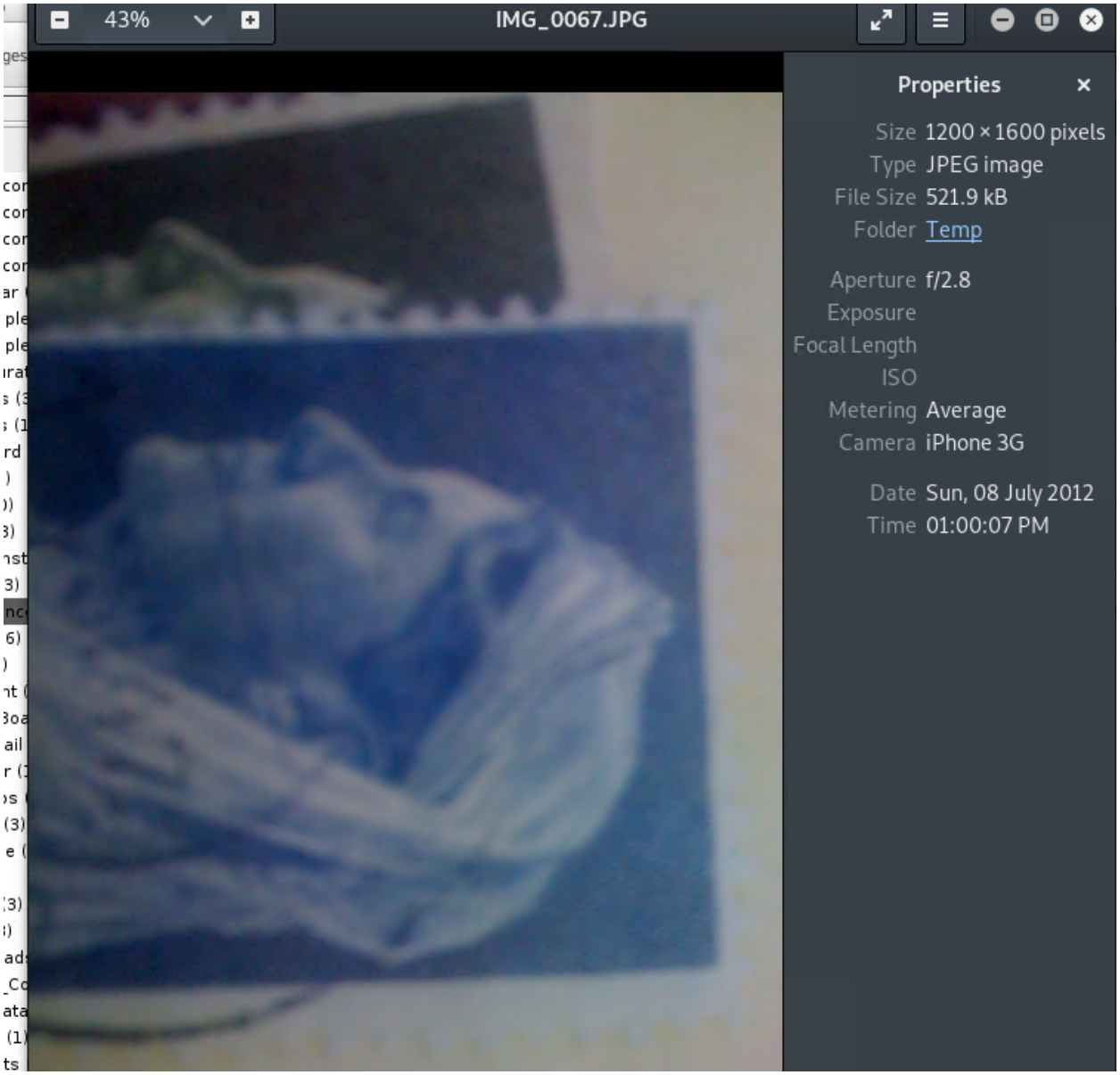
Location Information	
Location and Coordinates	**Map Screenshot**
38.88106083 -77.11533838 (PF Changs)	
38.88005346 -77.11595332 (Montessori school)	
38.88055896 -77.11553561 (Carpool Bar)	
38.87996816 -77.11601394 (Montessori school 2nd photol)	
38.88143724 -77.11478394 (Continental Valet)	
38.8815732 -77.11455619 (Hungry catering)	

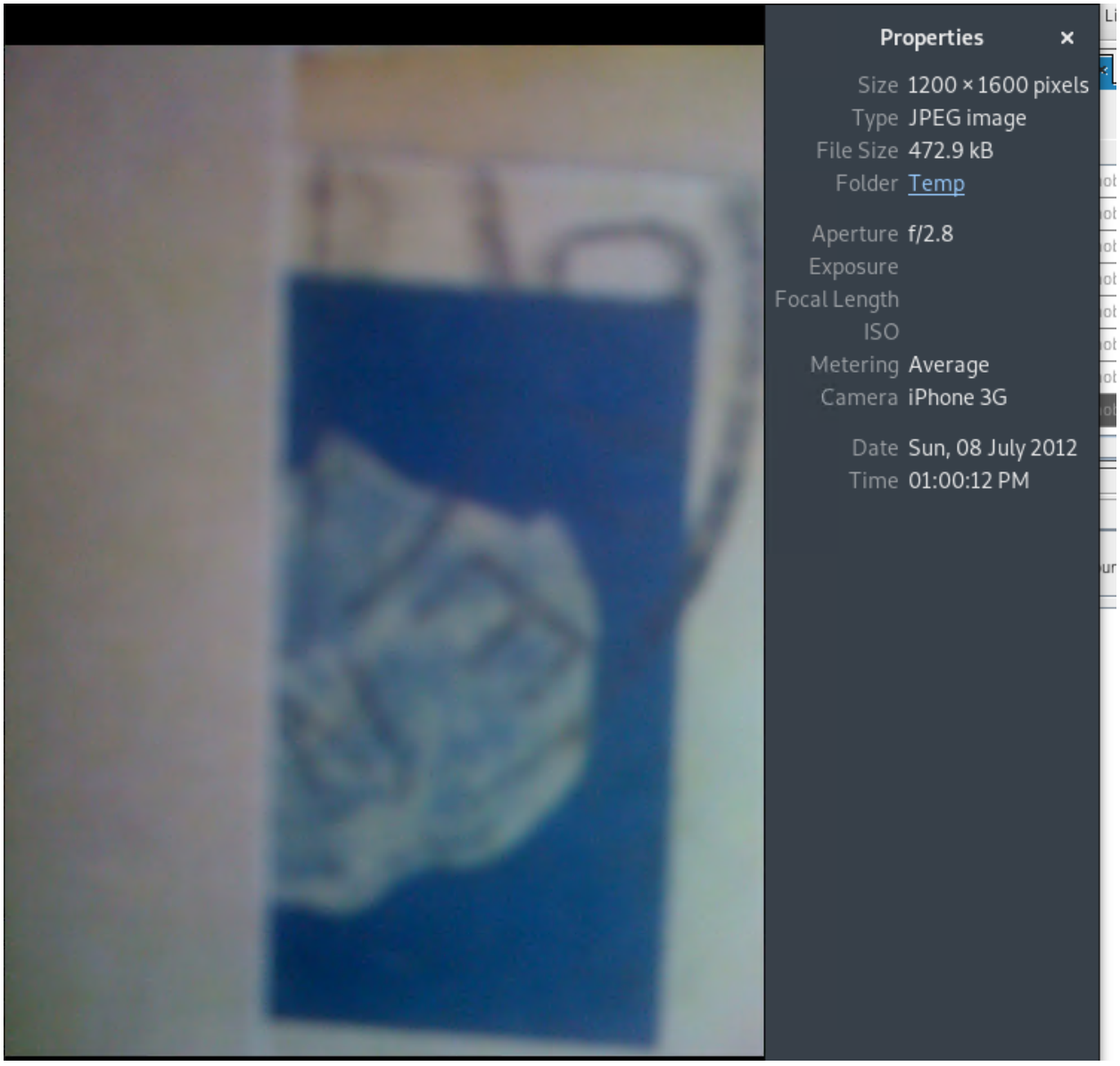

47%
IMG_0049.JPG
Properties
Size 1600 × 1200 pixels
Type JPEG image
File Size 533.1 kB
Folder Temp
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 12:41:41 PM
afpad


43%
IMG_0066.JPG
Properties
Size 1200 × 1600 pixels
Type JPEG image
File Size 527.5 kB
Folder Temp
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 01:00:01 PM


43%
IMG_0058.JPG
Properties
Size 1200 × 1600 pixels
Type JPEG image
File Size 558.1 kB
Folder Temp
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 12:50:20 PM


Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
47%
IMG_0069.JPG
Properties
Size 1600 × 1200 pixels
Type JPEG image
File Size 476.3 kB
Folder Temp
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 01:00:23 PM
previous image of the gallery


43%
IMG_0067.JPG
Properties
Size 1200 × 1600 pixels
Type JPEG image
File Size 521.9 kB
Folder Temp
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 01:00:07 PM


Properties
Size 1200 × 1600 pixels
Type JPEG image
File Size 472.9 kB
Folder Temp
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 01:00:12 PM