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.

The following findings seems to show that Tracy, Pat Sumtwelves, King Kthings (a friend of Pat), and Carry all conspired to steal Stamps from the National Gallery. Tracy how worked at the national Gallery and communicated via text and email to steal the stamps.

Equipment and Tools

Our team used Kali linux as the operating system for our forensics on Tracy's iphone. We used Autopsy to look at Tracy's IPHONE file system and with this tool we were able to extract files from an image of the phone. We used Sha256 and md5sum to hash the original image of the phone to maintain integrity. We used Sqlitebrowser to view *.db files found on the phone. We also used Vim and Nano to view extracted files on the phone. The use of google maps was integral for mapping out GPS locations.

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	Iphone1. 2	/img_tracy-phone-2012-07-15-final.E01/vol_vol /preferences/SystemConfiguration/com.apple. mobilegestalt.plist
Host Name	Tracy Sumtwelves iPhone	/img_tracy-phone-2012-07-15-final.E01/vol5/$ CarvedFiles/f0463080.plist
OS Version	Iphone OS 4.2.1 (8C148)	/img_tracy-phone-2012-07-15-final.E01/vol5/m obile/library/logs/AppleSupport/general log
Install Time	6/6/2012 19:03:28	/img_tracy-phone-2012-07-15-final.E01/vol5/m obile/library/logs/AppleSupport/general log
User Email	tracysumtwelve@gmail.com coralbluetwo@hotmail.com	/img_tracy-phone-2012-07-15.E01/vol_vol5/m obile/library/mail
Phone Number	1 (703) 340-9661	/img_tracy-phone-2012-07-15-final.E01/vol5/lo gs/lockdownd.log.1
Serial Number	86004482Y7H	/img_tracy-phone-2012-07-15-final.E01/vol5/m obile/library/logs/AppleSupport/general log
ICCID	89014103255195342366	/img_tracy-phone-2012-07-15-final.E01/vol5/lo gs/lockdownd.log.1
IMEI	012021003735398	/img_tracy-phone-2012-07-15-final.E01/vol5/ro ot/library/lockdown/activation_records/wildca rd_record.plist
MD5 Hash	34c4888f095dc3241330462923f6	Image hash
SHA256 Hash	71aed05a86a753dec4ef4033ed7f 52d6577ccb534ca0d1e83ffd2768 3e621607	Og image hash (original image)

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:	Person being accused

Pat:

Phone Number:(571) 308-3236
Email: perrypatsum@yahoo.com
Relationship: Tracy's Brother, Cop, also accomplice

Terry:

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

Joe:

Phone Number: na
Email: na
Relationship: disgruntled ex-husband

Carry:

Phone Number: 202 725-2124
Email: carrysum2012@yahoo.com
Relationship: Tracy's co-conspirator

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.

Figure 1. Email attachment ‘needs.txt’

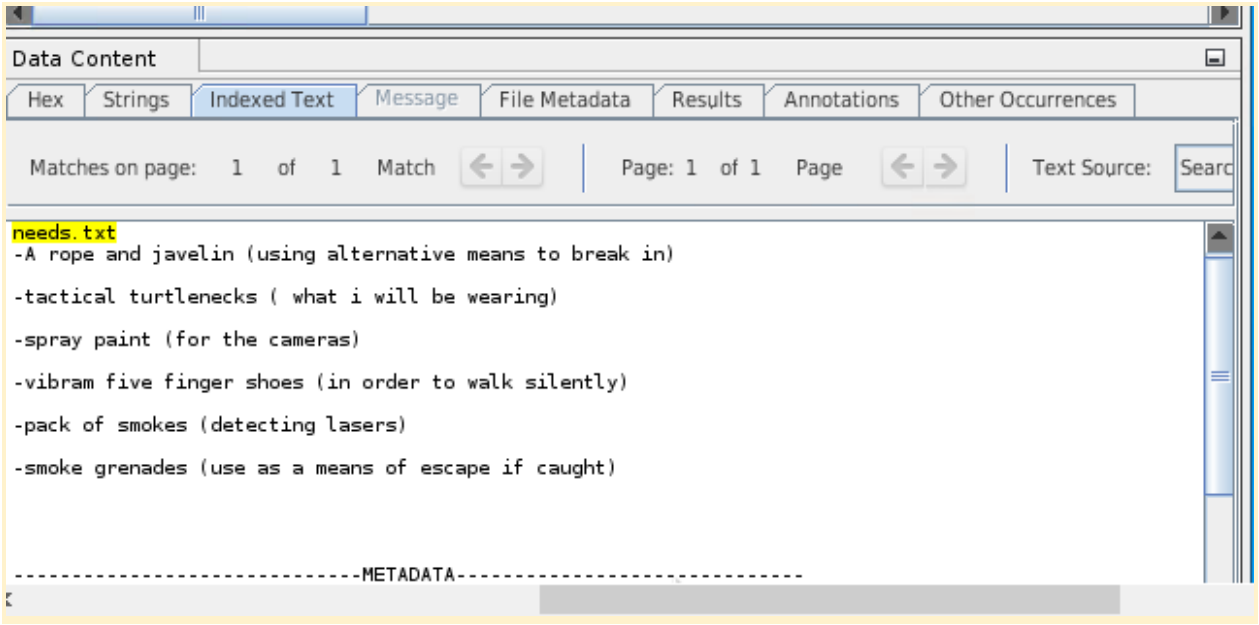
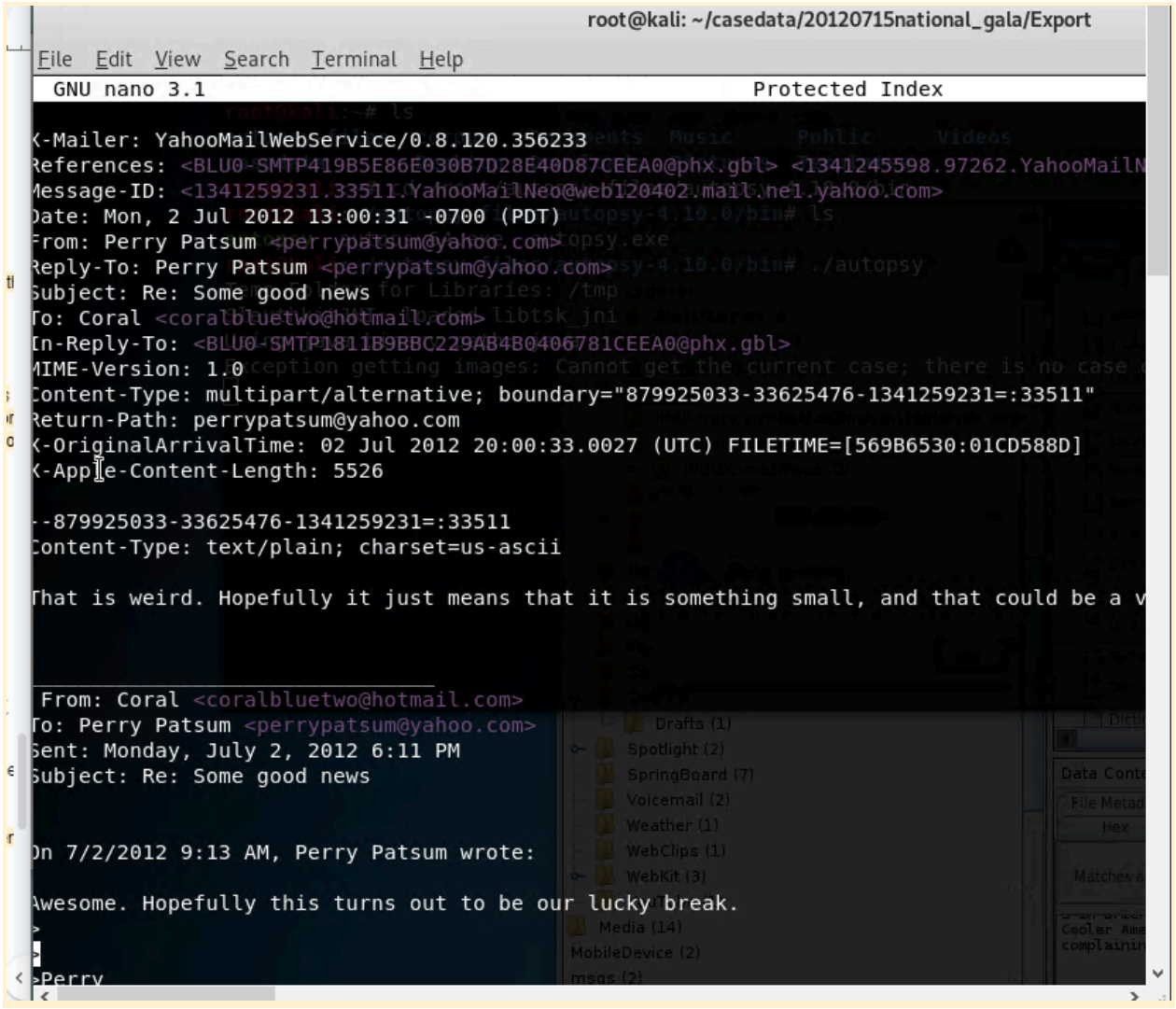
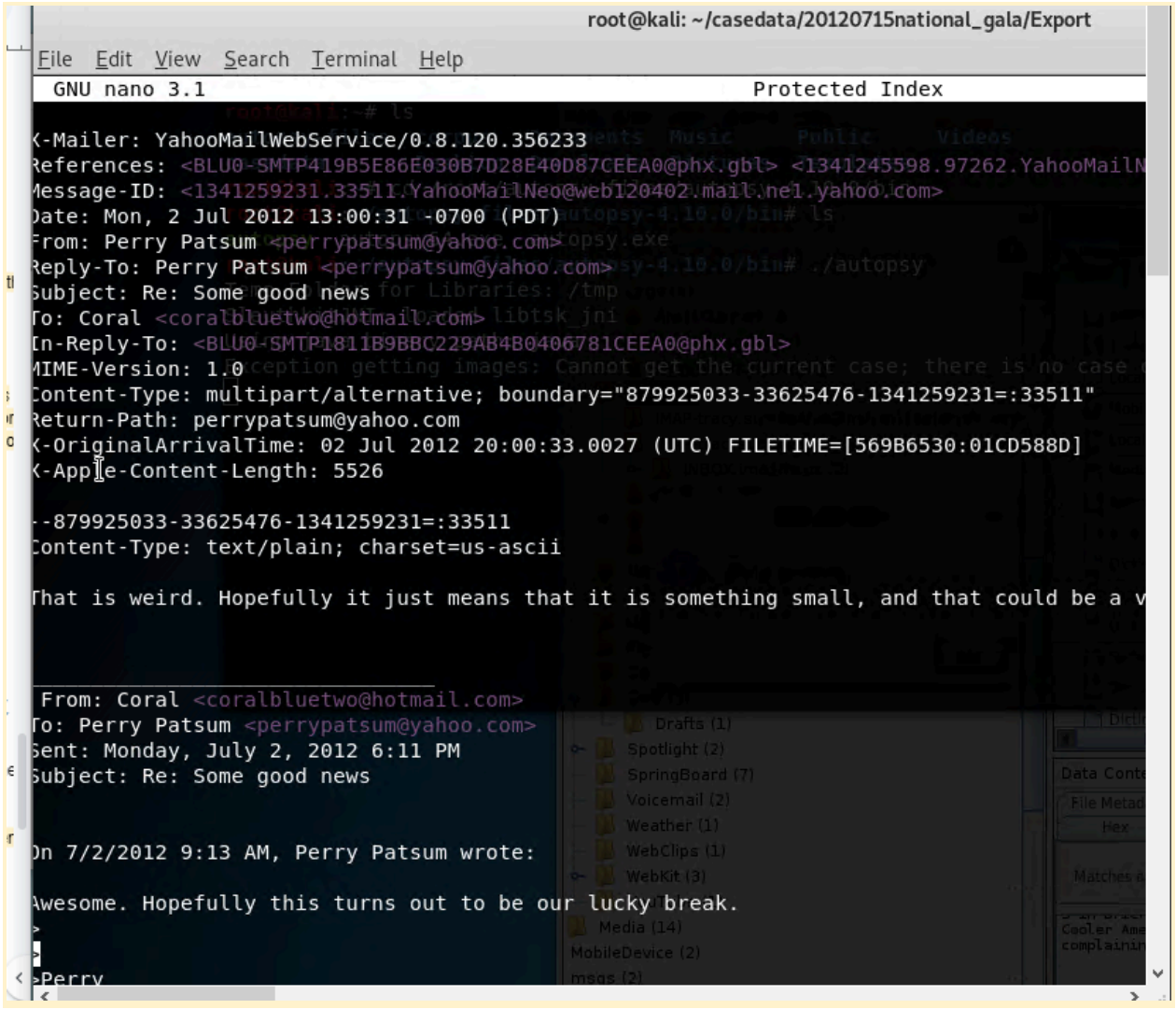


Figure 2.3

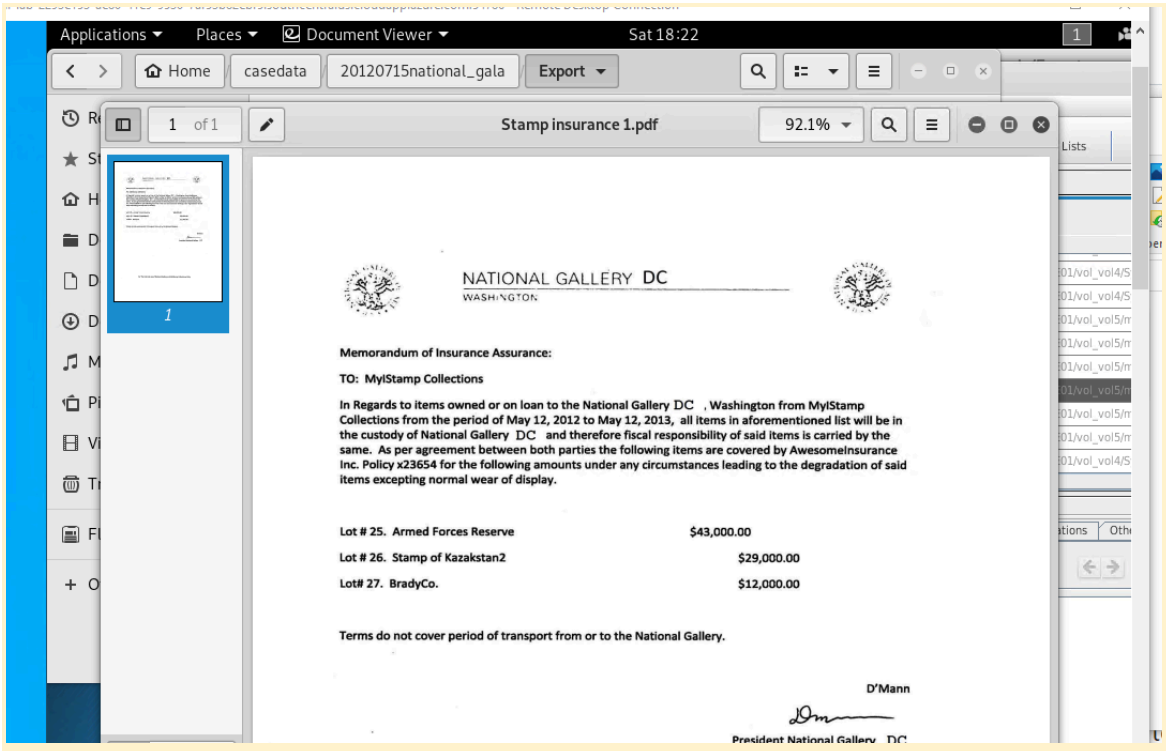
These are emails between (coralbluetwo@hotmail.com)(perrypatsum@yahoo.com) In these emails we see the individuals conspiring and speaking about the stamps exhibit in question.

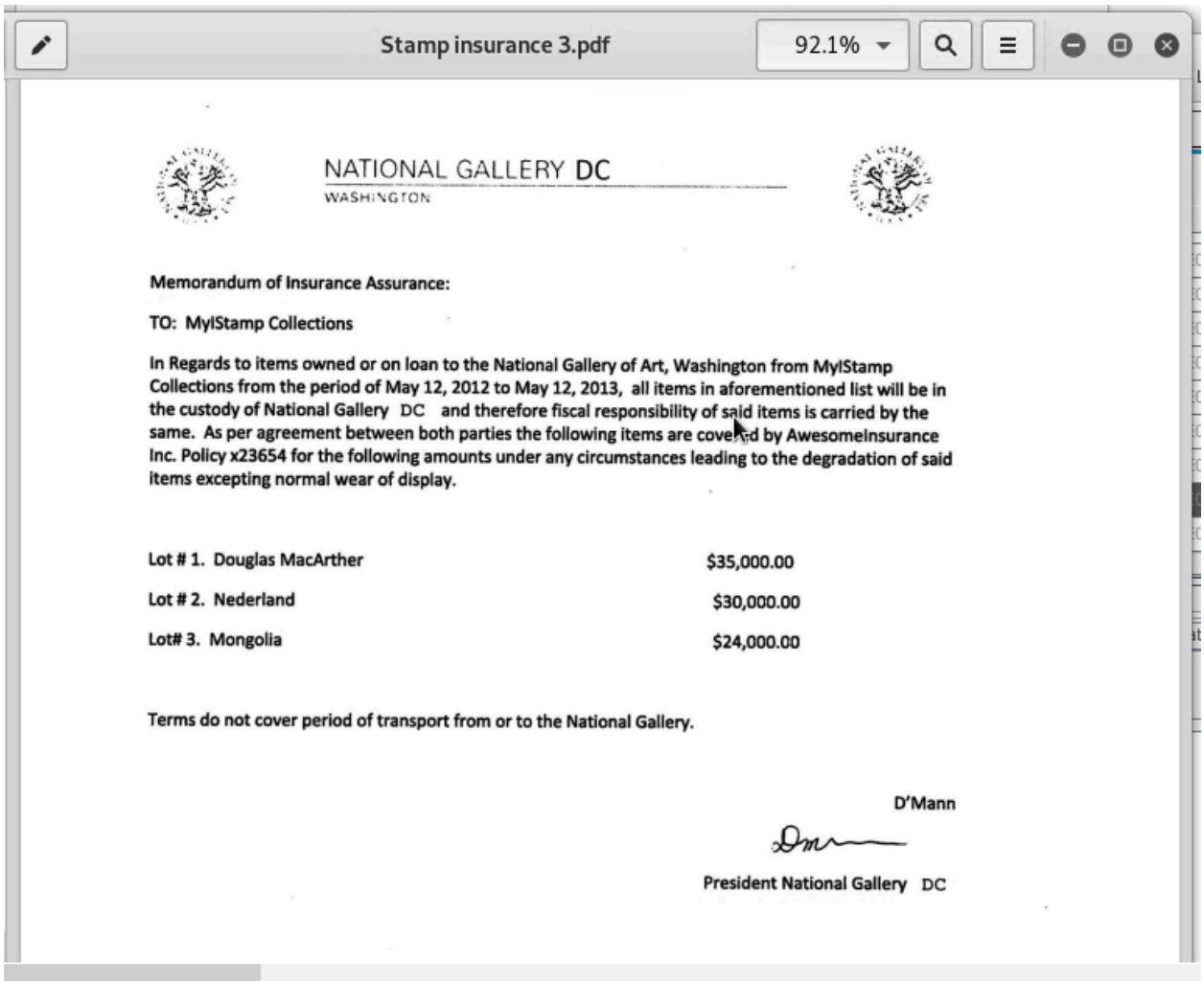

root@kali: ~/casedata/20120715national_gala/Export
File Edit View Search Terminal Help
GNU nano 3.1 Protected Index
X-Mailer: YahooMailWebService/0.8.120.356233
References: <BLU0-SMTP419B5E86E030B7D28E40D87CEEA0@phx.gbl> <1341245598.97262.YahooMailN
Message-ID: <1341259231.33511.YahooMailNeo@web120402.mail.ne1.yahoo.com>
Date: Mon, 2 Jul 2012 13:00:31 -0700 (PDT)
From: Perry Patsum <perrypatsum@yahoo.com>
Reply-To: Perry Patsum <perrypatsum@yahoo.com>
Subject: Re: Some good news
To: Coral <coralbluetwo@hotmail.com>
In-Reply-To: <BLU0-SMTP1811B9BBC229AB4B0406781CEEA0@phx.gbl>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="879925033-33625476-1341259231=:33511"
Return-Path: perrypatsum@yahoo.com
X-OriginalArrivalTime: 02 Jul 2012 20:00:33.0027 (UTC) FILETIME=[569B6530:01CD588D]
X-Apple-Content-Length: 5526
--879925033-33625476-1341259231=:33511
Content-Type: text/plain; charset=us-ascii
That is weird. Hopefully it just means that it is something small, and that could be a v
From: Coral <coralbluetwo@hotmail.com>
To: Perry Patsum <perrypatsum@yahoo.com>
Sent: Monday, July 2, 2012 6:11 PM
Subject: Re: Some good news
On 7/2/2012 9:13 AM, Perry Patsum wrote:
Awesome. Hopefully this turns out to be our lucky break.
>Perry

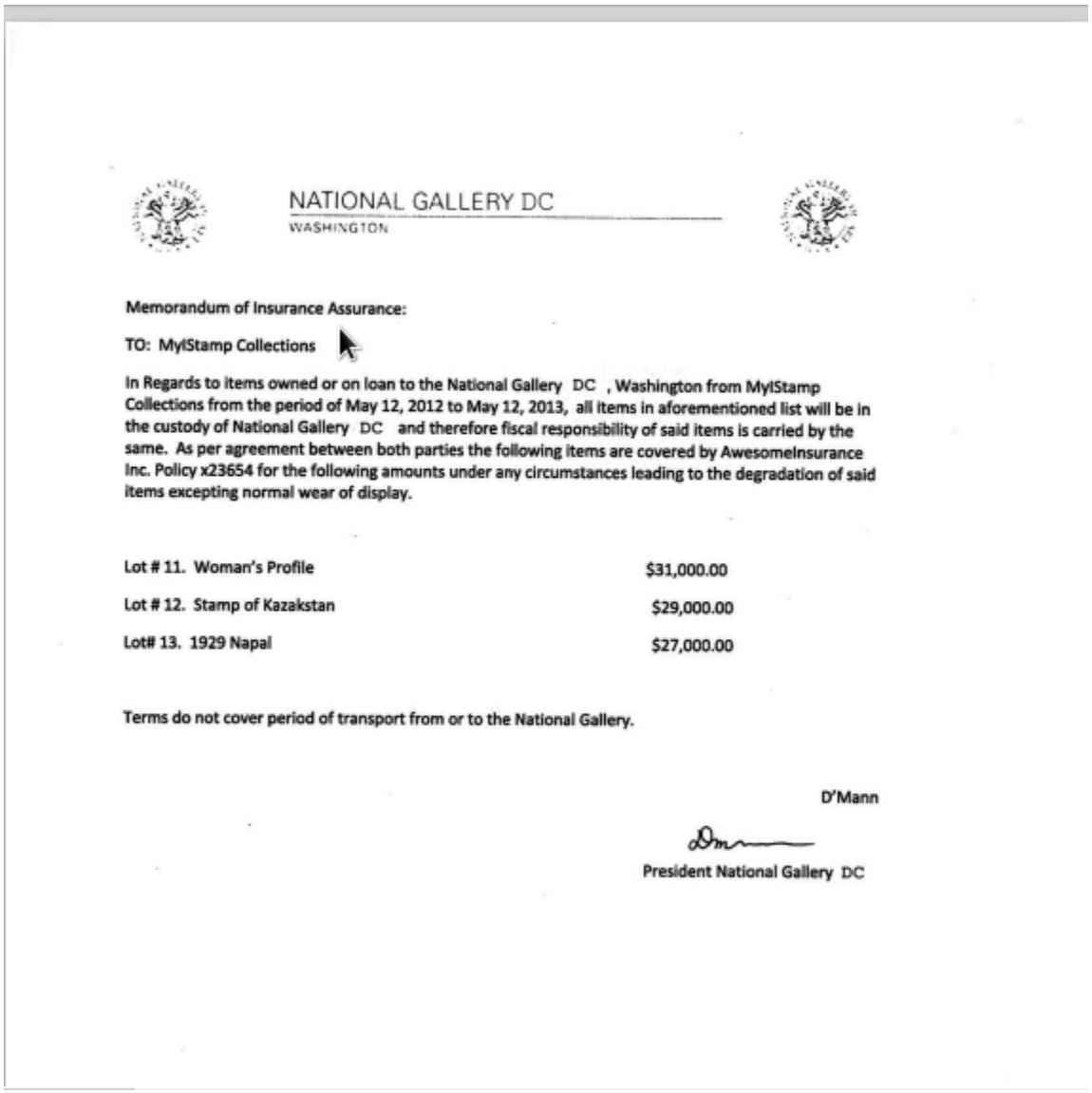

root@kali: ~/casedata/20120715national_gala/Export
File Edit View Search Terminal Help
GNU nano 3.1 Protected Index
X-Mailer: YahooMailWebService/0.8.120.356233
References: <BLU0-SMTP419B5E86E030B7D28E40D87CEEA0@phx.gbl> <1341245598.97262.YahooMailN
Message-ID: <1341259231.33511.YahooMailNeo@web120402.mail.ne1.yahoo.com>
Date: Mon, 2 Jul 2012 13:00:31 -0700 (PDT)
From: Perry Patsum <perrypatsum@yahoo.com>
Reply-To: Perry Patsum <perrypatsum@yahoo.com>
Subject: Re: Some good news
To: Coral <coralbluetwo@hotmail.com>
In-Reply-To: <BLU0-SMTP1811B9BBC229AB4B0406781CEEA0@phx.gbl>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="879925033-33625476-1341259231=:33511"
Return-Path: perrypatsum@yahoo.com
X-OriginalArrivalTime: 02 Jul 2012 20:00:33.0027 (UTC) FILETIME=[569B6530:01CD588D]
X-Apple-Content-Length: 5526
--879925033-33625476-1341259231=:33511
Content-Type: text/plain; charset=us-ascii
That is weird. Hopefully it just means that it is something small, and that could be a v
From: Coral <coralbluetwo@hotmail.com>
To: Perry Patsum <perrypatsum@yahoo.com>
Sent: Monday, July 2, 2012 6:11 PM
Subject: Re: Some good news
On 7/2/2012 9:13 AM, Perry Patsum wrote:
Awesome. Hopefully this turns out to be our lucky break.
>Perry

```
    </font> </div>
  <br>
  Perry,<br>
  <br>
  I think I may have come across something interesting.
  Everybody around the office seems to be buzzed about a
  foreign exhibit that is supposed to be coming over. There
  hasn&#39;t been any official release in writing but we have been
  going through quite an ordeal with all this paperwork. From
  what I can tell, this exhibit has to be a big deal. I&#39;ll let
  you know if I found out anything else.<br>
  <br>
  Coral<br>
  <br>
  <br>
 </div>
</div>
div>
ockquote>
```

In figure 3.1-3 We can see the stamps value and market price through the insurance.




Stamp insurance 3.pdf
92.1%
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



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.

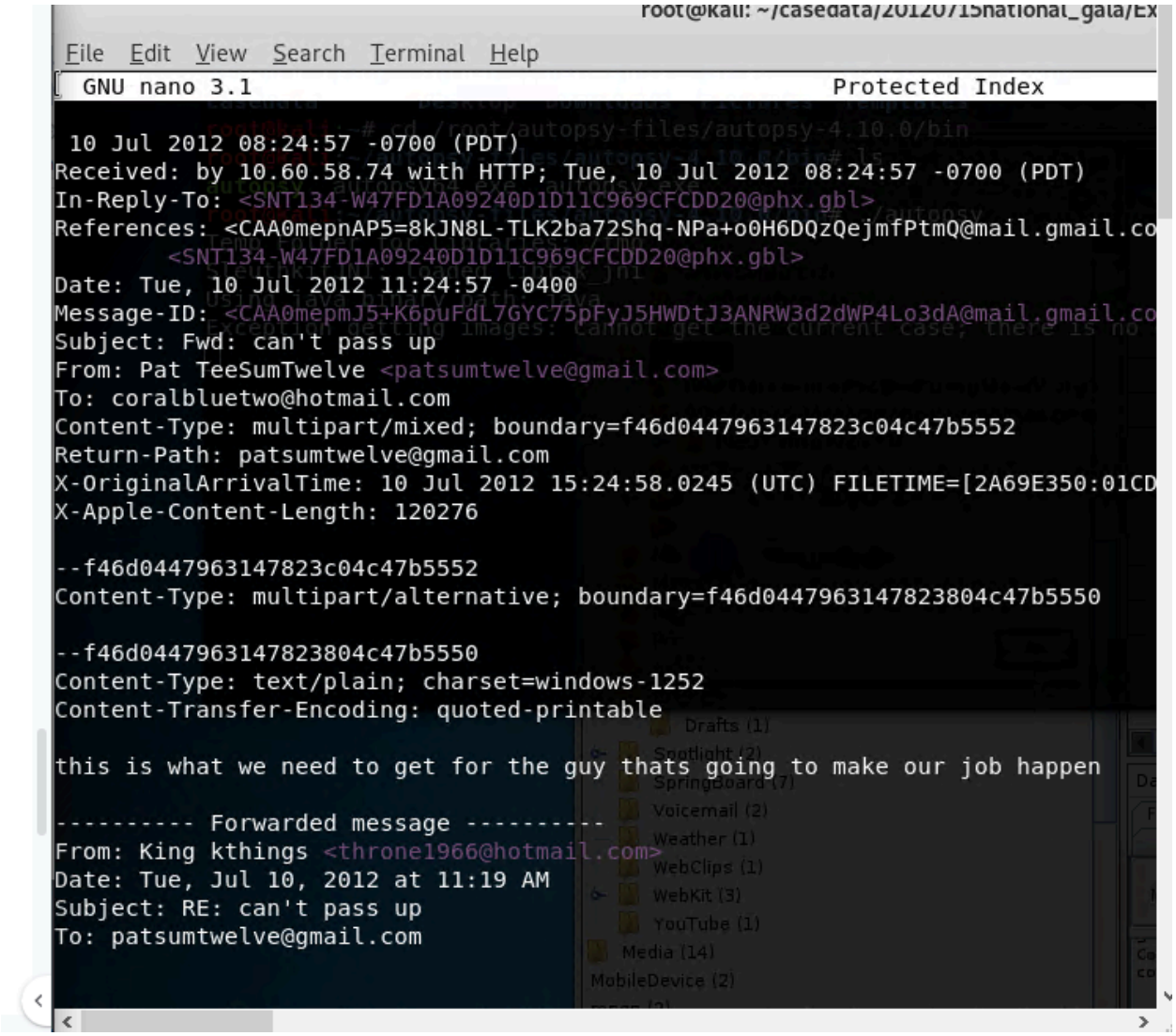
Lot # 11. Woman's Profile	$31,000.00
Lot # 12. Stamp of Kazakstan	$29,000.00
Lot# 13. 1929 Napal	$27,000.00

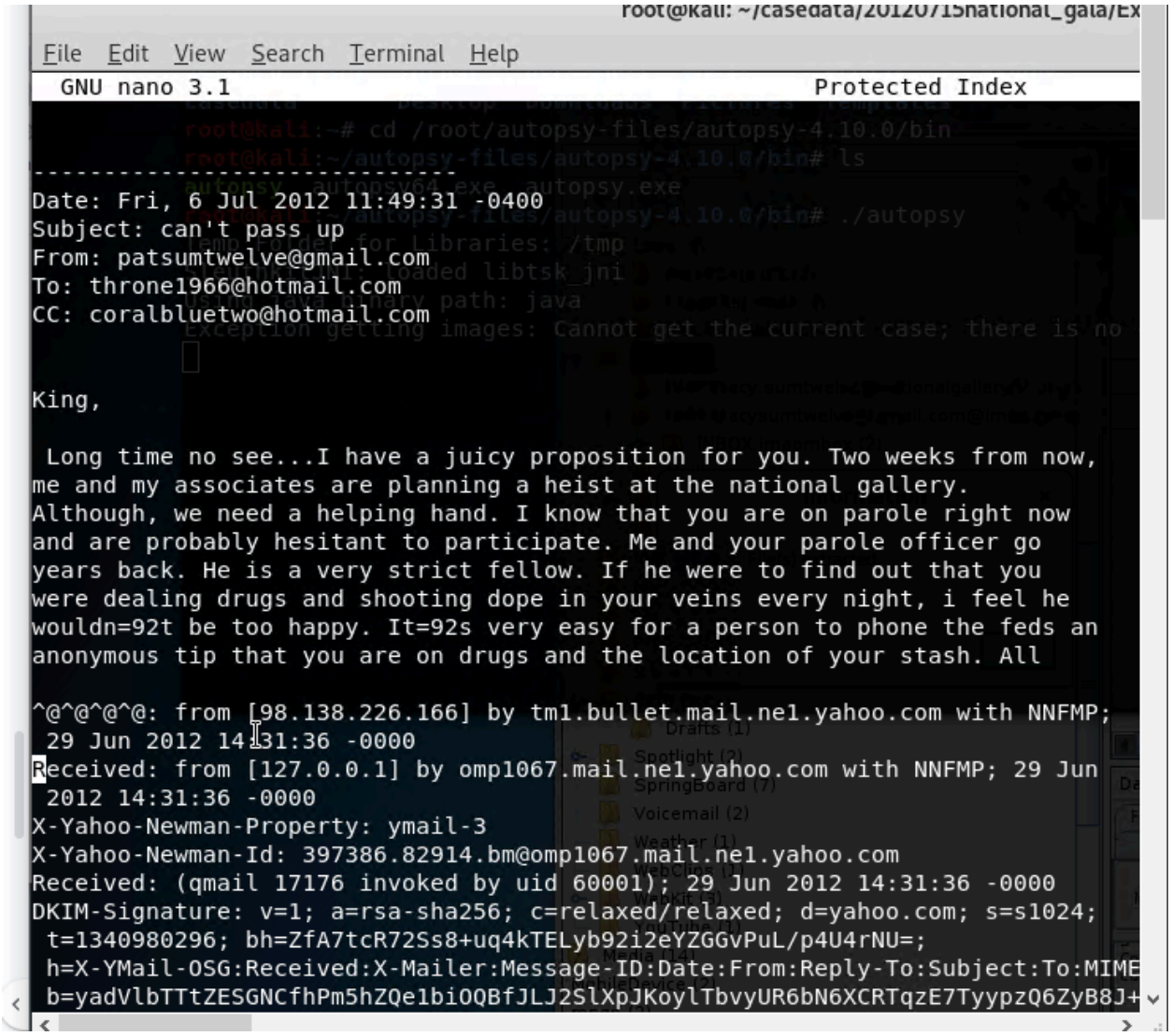
Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

In the final figure 4.1.2.3 we can see King being recruited in.


root@kali: ~/casedata/20120715national_gala/Ex
File Edit View Search Terminal Help
GNU nano 3.1 Protected Index
10 Jul 2012 08:24:57 -0700 (PDT)
Received: by 10.60.58.74 with HTTP; Tue, 10 Jul 2012 08:24:57 -0700 (PDT)
In-Reply-To: <SNT134-W47FD1A09240D1D11C969CFCDD20@phx.gbl>
References: <CAA0mepnAP5=8kJN8L-TLK2ba72Shq-NPa+o0H6DQzQejmfPtmQ@mail.gmail.co
<SNT134-W47FD1A09240D1D11C969CFCDD20@phx.gbl>
Date: Tue, 10 Jul 2012 11:24:57 -0400
Message-ID: <CAA0mepmJ5+K6puFdL7GYC75pFyJ5HWDtJ3ANRW3d2dWP4Lo3dA@mail.gmail.co
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=[2A69E350:01CD
X-Apple-Content-Length: 120276
--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
---------- Forwarded message ----------
From: King kthings <throne1966@hotmail.com>
Date: Tue, Jul 10, 2012 at 11:19 AM
Subject: RE: can't pass up
To: patsumtwelve@gmail.com



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.

Other than planning a heist, and a flash mob, I do not see any defacement.

Plot Timeline

- In a message set to Tracy's ex that she is unable to pay tuitions for her daughter and this I believe is the motive for her to steal the stamps.
- On July 2, 2012 We see that Patsumtwelve@gmail.com and Coralbluetwo@hotmail.com were seen conversing and alluding to taking the stamps and hoping for a lucky break.
- Then on July July 6 we see that Pat is speaking to the king about the heist.
- Pat also speaks to King and about what supplies are needed.
- We also see that Tracy knows that stamps to be yet reviled and willing to see the crime

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy and Pat seemed to be the ones to come up with the plan to steal the stamps. Tracy used 'coralbluetwo@hotmail.com and Pat used 'perrypatsum@yahoo.com. They used alias, encrypted files, and french to organize the heist.
- Pat worked with King via email. Kings email throne1966@hotmail.com to steal the stamps. Pat also seems to mention King being on Parole and could be using that knowledge to leverage information.
- Tracy and Cary tries to take a tablet past security contents are unknown but content seems relevant to the heist. Both Tracy and Cary both organized a flash mob

Appendix A: Correspondence Evidence

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

Master Timeline of NGDC

Artifact #	Timestamp	Header Information	Key Information	Evidence Location
01FE9965	July 11 2012	From: Microsoft@reply.digital.river.com	na	
8A3BD06	9 July 2012	From: Tracy Sumtwelve To: coralbluetwo@hotmail.com Message contained an encoded file	Apple-Mail=_911D6059-B921-46DB-B7D8-E054F040CBFF– Encoded in base64 Document is named documents.zip Content type is application/zip	email.
		Sender IP 209.85.214.18 throne1966@hotmail.com patsumtwelve@gmail.com July 10 2012	Both parties discussing a heist and there preparations for the heist. A document named needs.txt was found. It was also encoded in based 64 email. In a pdf. Labled named needs.txt: - Rope and vaseline (using alternative means to break in) - Tactical Turtlenecks (what i will be wearing) - Vibram five finger shoes (in order to walk silently) - Pack of smokes (detecting lasers)	

F3F4EB95	July 5, 2012	Woina.honril@m57.biz coralbluetwo@hotmail.com	Suspisious email with a file named 000001.doc. Also encrypted in based 64 Sender 208.97.132.83 Subject line: busy When searching for 000001.doc I was able to find the full email of of king talking with Tracys brother and speaking about the heist.	Email And Protected Index

Case Name: 2012-07-15-National-Gallery

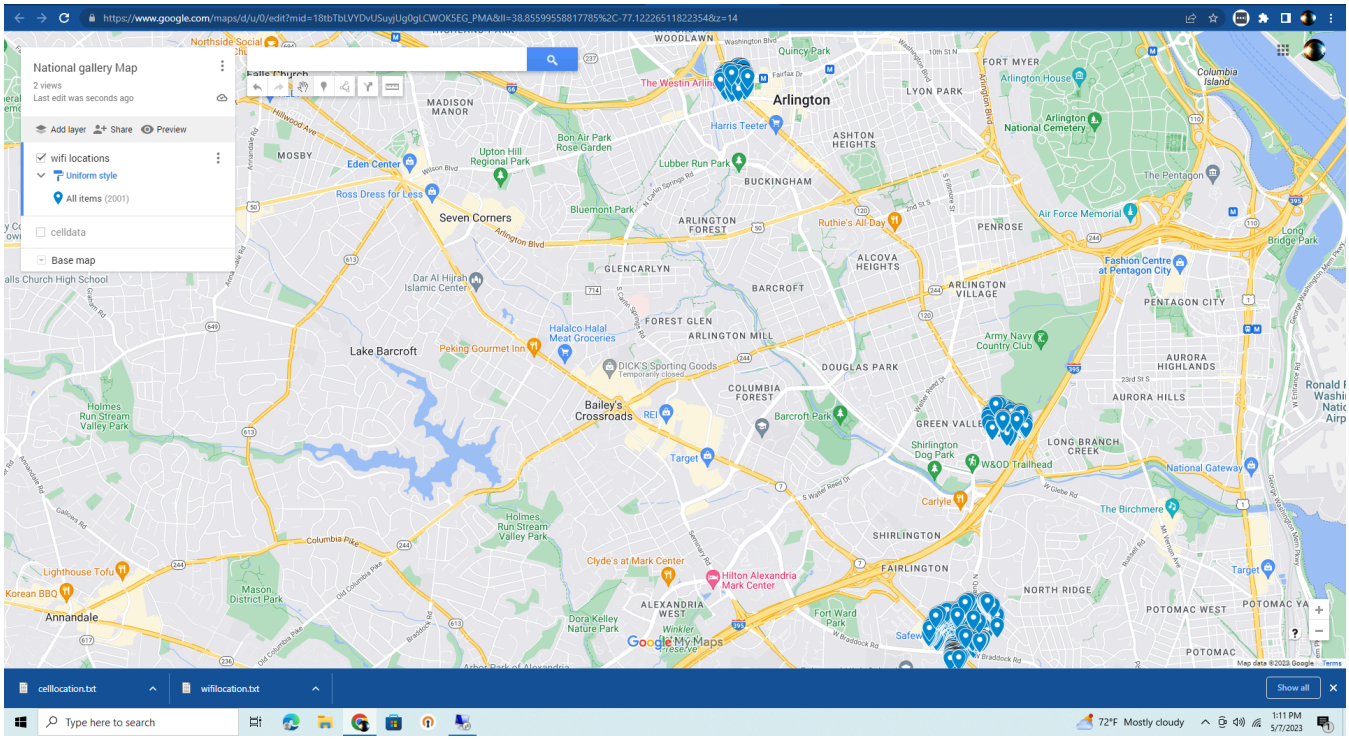
Case #: 1EZ215-P

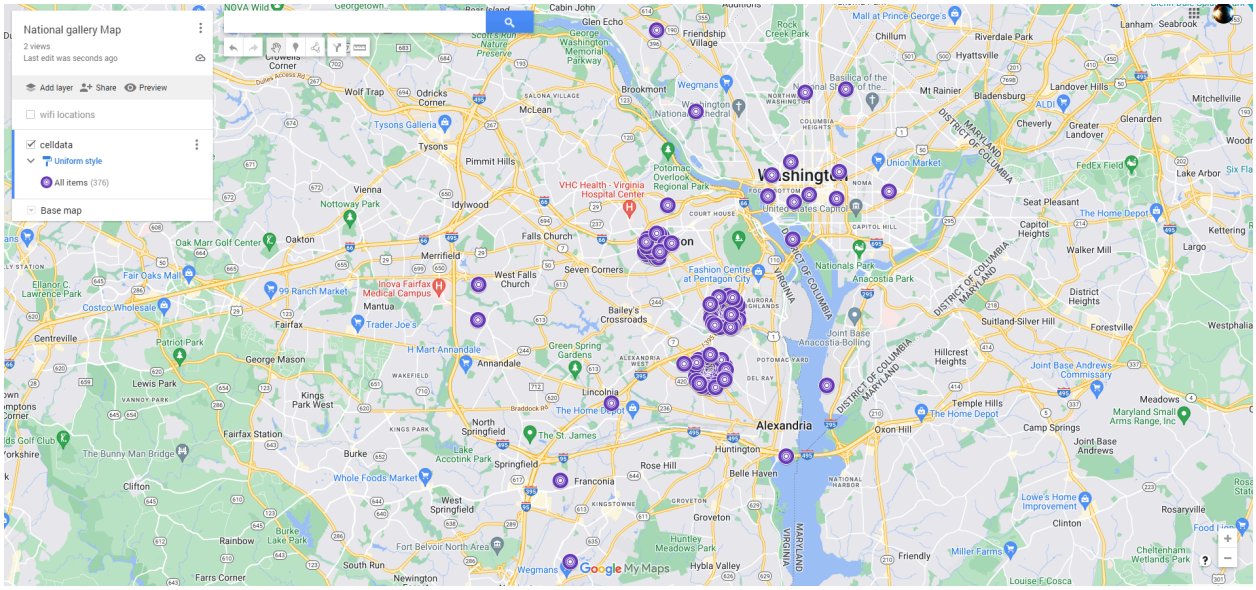
Details of Tracy's iPhone

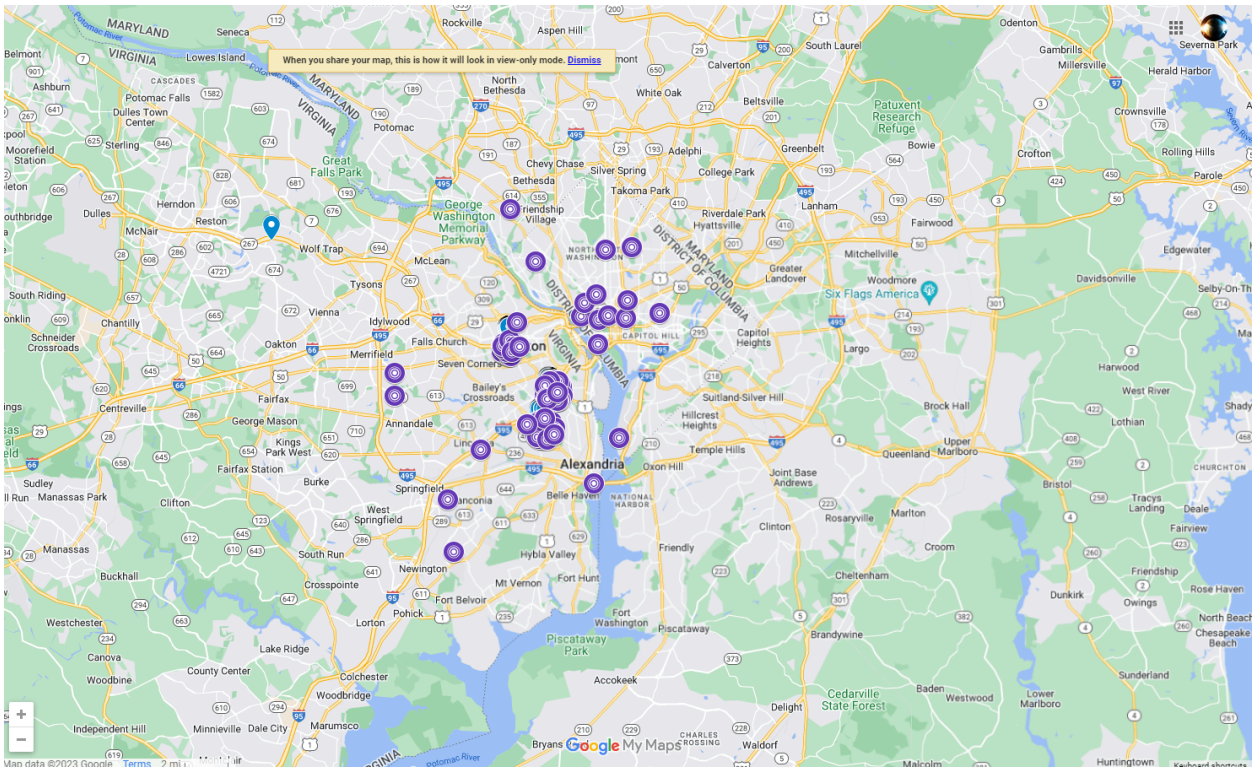
Name	Findings	Location in iPhone image file
Model	Iphone1. 2	/img_tracy-phone-2012-07-15-final.E01/vol_vol /preferences/SystemConfiguration/com.apple. mobilegestalt.plist
Host Name	Tracy Sumtwelves iPhone	/img_tracy-phone-2012-07-15-final.E01/vol5/$ CarvedFiles/f0463080.plist
OS Version	Iphone OS 4.2.1 (8C148)	/img_tracy-phone-2012-07-15-final.E01/vol5/m obile/library/logs/AppleSupport/general log
Install Time	6/6/2012 19:03:28	/img_tracy-phone-2012-07-15-final.E01/vol5/m obile/library/logs/AppleSupport/general log
User Email	tracysumtwelve@gmail.com coralbluetwo@hotmail.com	/img_tracy-phone-2012-07-15.E01/vol_vol5/m obile/library/mail

Phone Number	1 (703) 340-9661	/img_tracy-phone-2012-07-15-final.E01/vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	/img_tracy-phone-2012-07-15-final.E01/vol5/mobile/library/logs/AppleSupport/general log
ICCID	89014103255195342366	/img_tracy-phone-2012-07-15-final.E01/vol5/logs/lockdownd.log.1
IMEI	012021003735398	/img_tracy-phone-2012-07-15-final.E01/vol5/root/library/lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6	Image hash
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	Og image hash (original image)

Appendix B: WiFi and GPS Location Information


National gallery Map
2 views
Last edit was seconds ago
Add layer
Share
Preview
wifi locations
Uniform style
All items (2001)
celldata
Base map
Arlington
Seven Corners
Lake Barcroft
Bailey's Crossroads
Annandale
Google My Maps
celllocation.txt
wifilocation.txt
Show all
Type here to search
72°F Mostly cloudy
1:11 PM
5/7/2023


National gallery Map
2 views
Last edit was seconds ago
Add layer
Share
Preview
wifi locations
celldata
Uniform style
All items (376)
Base map
Google My Maps


When you share your map, this is how it will look in view-only mode. Dismiss
Google My Maps