Case Report
National Gallery DC

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

Group Members: Andrew Benga, Andrea Larson, Niyi Ayinde, Lindsey Wilson, Nhina Nyirenda & Reece Ellsworth

Table of Contents

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) cases 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.

I. Digitech Inc, found evidence that indicated Tracy was using the alias Coral and that Pat was using the alias Perry.

II. Digitech Inc, found evidence that indicated Tracy was motivated by financial gain in planning the stamp heist due to running into some money troubles.

III. Digitech Inc, also discovered emails between what appeared to be from Tracy's personal email and Pat containing the National Gallery DC stamp letters.

IV. Digitech Inc. found evidence indicating that Tracy was formulating a plan to steal stamps with Pat. Additionally, Digitech Inc, found evidence that indicated Tracy knew that Pat was trying to coerce someone named King to help with the heist.

V. Digitech Inc. found evidence indicating that Tracy helped an individual named Carry for financial gain. The evidence included leaked sensitive security rotation information about the National Gallery to Carry. There is also evidence indicating that Tracy helped Carry smuggle a tablet into the National Gallery. However, there is evidence that indicated Tracy was unaware of the devious plan that Carry had in mind.

Equipment and Tools

The incident Response Team collected a forensic image of the iPhone 3G) In Los Angeles, CA. The forensics image files of the iPhone 3G, Tracy-phone-2020-07-15-final. E01 can be viewed as an exact snapshot of the data present on the iPhone during its acquisition.

These were the following tools used for Forensic analysis:

- Kali Linux VM
- Autopsy
- fcrackzip
- Nano
- DB Browser for SQLite

- Google Maps

Details of Tracy's iPhone

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

Name	Findings	Location in iPhone image file
Model	iPhone 3G	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 19:03:28	/mobile/Library/Logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com tracysumtwelve@nationalgallergydc.org	vol5/mobile/Library/Mail
Phone Number	(703) 340-9661	/logs/lockdownd.log.1
Serial Number	86004482Y7H	/mobile/Library/Logs/AppleSupport/general.log
ICCID	89014103255195342366	/logs/lockdownd.log.1
IMEI	012021003735398	/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: (Coral)

Phone Number: (703) 340-9961
Personal Email: tracysumtwelve@gmail.com
Work Email: tracy.sumtwelve@nationalgallerydc.org
Email: coralbluetwo@hotmail.com
Email: tracysumtwelve@gmail.com
Relationship: Accused - Tracy works as a supervisor at the National Gallery. She is a recently divorced mother in the middle of a child custody battle. Unfortunately, Tracy's daughter is in an expensive private school,which Tracy can no longer afford on her salary. Her ex-husband will only pay for the school if Tracy will give over custody of their daughter to him. Worse, Tracy's daughter, Terry, age 15, has stated that she would rather live with her dad if it comes to staying in school. "After all, you ran dad off in the first place."

Carry contacts Tracy and starts sending her small pieces of data, telling Tracy that she wants to organize a flash mob at the gallery and needs a little help.
Carry offers to give Tracy money for this help. The items transferred are suspicious but not outright illegal. Tracy is having trouble with finances and this allows her to overlook the suspicious nature of the requests.

Pat: (Perry)
Phone Number: 571-308-3236 (we know this because the person texting mentions "sis" in multiple messages. From that we can conclude that the brother - Pat - is texting his sister - Tracy)
Email: perrypatsum@yahoo.com
Email: patsumtwelve@gmail.com
Relationship: Pat is Tracy's brother.He is a corrupt police officer of the D.C. Enforcers Bureau. He holds the status of detective. He is very devoted to his sister and niece Terry, to this point he isn't an outright criminal, but walks the line very closely.

Terry: Phone Number: 703-829-6071 (we know this because the correspondence mentions "I'm going out with dad" so we can conclude that the daughter - Terry - is talking to the mom Tracy)
Email:
Relationship: Terry is the daughter of Tracy and Joe. Terry attends an expensive private school. (Prufrock Preparatory School). She wants to stay in school to avoid having to start over and so that she can keep her current friends despite the fact that her mother can no longer afford to pay the tuition.

Joe: Email: joe.sum.twelve@gmail.com
Relationship: Joe is the father of Terry and is currently going through the divorce with Tracy. Joe is financially well-off and still bitter about the issues in their marriage.
Now that Joe and Tracy are going through a divorce, he has motivation to use the key logger to spy on both Tracy and Terry, their daughter. He previously installed a key logger on the family's MacBook Air in an attempt to keep track of Terry's online behavior.
Joe used to have an account on the MacBook Air, but it was deleted. The home folder may have been preserved.

Carry: Phone Number: 1-202-725-2124 (we know this because Carry wants to organize a flash mob at the gallery and needs a little help from Tracy - the text messages from this number mention the flash mob

Email: carrysum2012@gmail.com

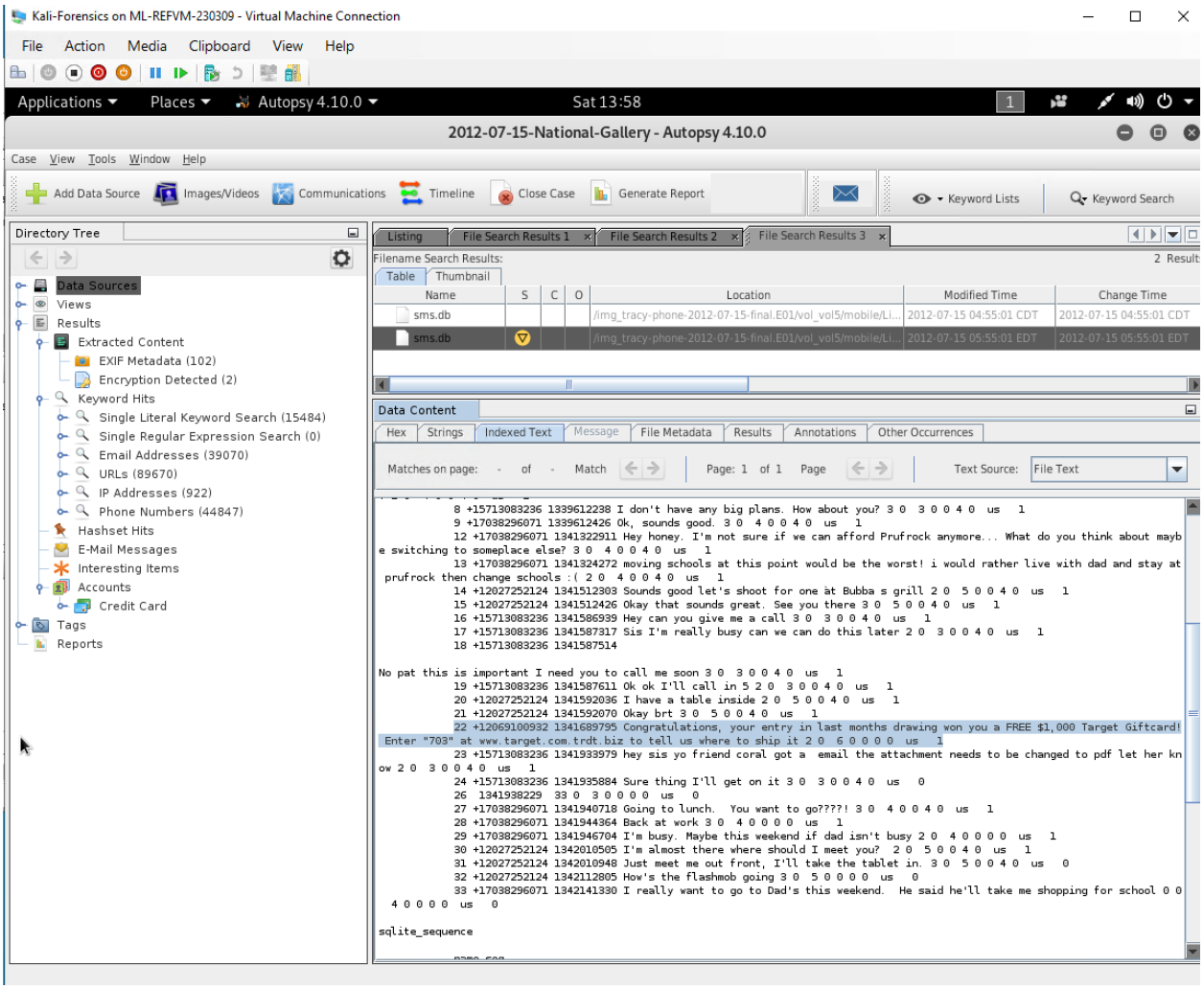
Email: carrysum2012@yahoo.com

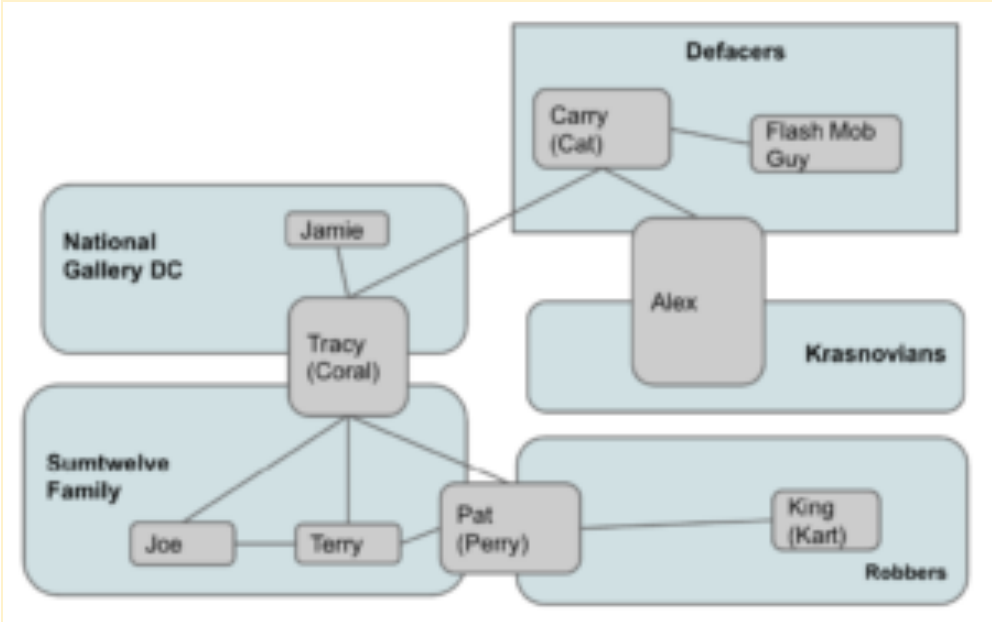
Relationship: Carry is a somewhat criminally involved individual and Krasnovian supporter who shares family ties with Alex. Carry is both technologically savvy and an occasional social media user. She is contacted by Alex in the beginning of the scenario and asked to orchestrate the defacing of the artwork because she is both aligned with Krasnovia and has "connections." She is acquainted with Tracy.

Alex:

Relationship: Alex is a Krasnovian supporter who wishes to embarrass the United States. He knows Carry through extended family connections, and contacts her. He plans to deface foreign works that are on exhibit at the National Gallery in DC. Defacing the artwork will embarrass the United States and possibly degrade the relationship between the United States and the foreign country.

Fraudulent number +1-120-691- 0932: this text is Spam trying to get Tracy to click on the fraudulent link. The link has additional parameters attached at the end which can indicate this is not a legit link to Target (www.target.com.trdt.biz)


Kali-Forensics on ML-REFVM-230309 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Autopsy 4.10.0 Sat 13:58
2012-07-15-National-Gallery - Autopsy 4.10.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Timeline Close Case Generate Report
Keyword Lists Keyword Search
Directory Tree
Data Sources
Views
Results
Extracted Content
EXIF Metadata (102)
Encryption Detected (2)
Keyword Hits
Single Literal Keyword Search (15484)
Single Regular Expression Search (0)
Email Addresses (39070)
URLs (89670)
IP Addresses (922)
Phone Numbers (44847)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Credit Card
Tags
Reports
Listing
File Search Results 1
File Search Results 2
File Search Results 3
Filename Search Results:
2 Results
Table Thumbnail
Name S C O Location Modified Time Change Time
sms.db /img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Li... 2012-07-15 04:55:01 CDT 2012-07-15 04:55:01 CDT
sms.db /img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Li... 2012-07-15 05:55:01 EDT 2012-07-15 05:55:01 EDT
Data Content
Hex Strings Indexed Text Message File Metadata Results Annotations Other Occurrences
Matches on page: - of - Match Page: 1 of 1 Page Text Source: File Text
8 +15713083236 1339612238 I don't have any big plans. How about you? 3 0 3 0 0 4 0 us 1
9 +17038296071 1339612426 Ok, sounds good. 3 0 4 0 0 4 0 us 1
12 +17038296071 1341322911 Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else? 3 0 4 0 0 4 0 us 1
13 +17038296071 1341324272 moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools :(2 0 4 0 0 4 0 us 1
14 +12027252124 1341512303 Sounds good let's shoot for one at Bubba s grill 2 0 5 0 0 4 0 us 1
15 +12027252124 1341512426 Okay that sounds great. See you there 3 0 5 0 0 4 0 us 1
16 +15713083236 1341586939 Hey can you give me a call 3 0 3 0 0 4 0 us 1
17 +15713083236 1341587317 Sis I'm really busy can we can do this later 2 0 3 0 0 4 0 us 1
18 +15713083236 1341587514
No pat this is important I need you to call me soon 3 0 3 0 0 4 0 us 1
19 +15713083236 1341587611 Ok ok I'll call in 5 2 0 3 0 0 4 0 us 1
20 +12027252124 1341592036 I have a table inside 2 0 5 0 0 4 0 us 1
21 +12027252124 1341592070 Okay brt 3 0 5 0 0 4 0 us 1
22 +12069100932 1341689795 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 2 0 6 0 0 0 0 us 1
23 +15713083236 1341933979 hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know 2 0 3 0 0 4 0 us 1
24 +15713083236 1341935884 Sure thing I'll get on it 3 0 3 0 0 4 0 us 0
26 1341938229 33 0 3 0 0 0 0 us 0
27 +17038296071 1341940718 Going to lunch. You want to go????! 3 0 4 0 0 4 0 us 1
28 +17038296071 1341944364 Back at work 3 0 4 0 0 0 0 us 1
29 +17038296071 1341946704 I'm busy. Maybe this weekend if dad isn't busy 2 0 4 0 0 0 0 us 1
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
33 +17038296071 1342141330 I really want to go to Dad's this weekend. He said he'll take me shopping for school 0 0 4 0 0 0 0 us 0
sqlite_sequence


Defacers
Carry (Cat)
Flash Mob Guy
National Gallery DC
Jamie
Tracy (Coral)
Alex
Krasnovians
Sumtwelve Family
Joe
Terry
Pat (Perry)
King (Kart)
Robbers

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.

- Insurance Documents - The insurance documents are evidence that Tracy was planning to steal the stamps from the National Gallery of Art

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.

We found the following evidence showing the defacement of the museum art:
-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

Please see the Timeline below for further details and events.

Conclusion

Evidence found on Tracy's iPhone indicated the following:

We found various events from Tracy's iphone via text messages, email and other forms of communication which provided evidence for Tracy's being the main culprit of the crime. We also found a zip file that contained that monetary value of the stamps, known as the Memorandum of Insurance Assurance. We also discover that Tracy went under the alias Coral, and her brother Pat went under the alias Perry to conceal their identities.

We can conclude that Tracy's is guilty of defacing foreign art of a private party and theft.

Appendix A: Correspondence Evidence

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

Correspondence Evidence

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1	5/7/2012 12:58PM PDT	F: Winona.Honril@m57.biz T: coralbluetwo@hotmail.com Sub: Busy	I didn't.	*see note 4
2	6/10/2012 1:06:PM PDT	From: Pat TeeSumTwelve patsumtwelve@gmail.com To: Tracy TeeSumTwelve TracySumtwelve@gmail.com Subject: Paris Speak and answer	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 This translates to: Tracy, I consider your proposal. My r = E9ponse is yes! You said that you have an alias. Send me the email address, and I will provide you additional instructions. caress	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0401136.plist
3	6/19/2012 1:06PM PTD	To: Tracy tracysumtwelve@gmail.com From: Pat - Perry Patsum perrypatsum@yahoo.com Subject: Look me up sometime	Tracy, Talked to your brother about an email. You should have your friend, Alias, send me an email. Thanks Perry	Name /img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0401136.plist
4	6/19/2012 2:28PM PDT	From: Perry Patsum To: Coral bluetwo coralbluetwo@hotmail.com Sub: Crazydave by the VMs	Hey Coral, just got your email. That took longer than expected! Oh well you've to check out this new song by the VMs. I love the base. Tell me what you think.	*see note 2

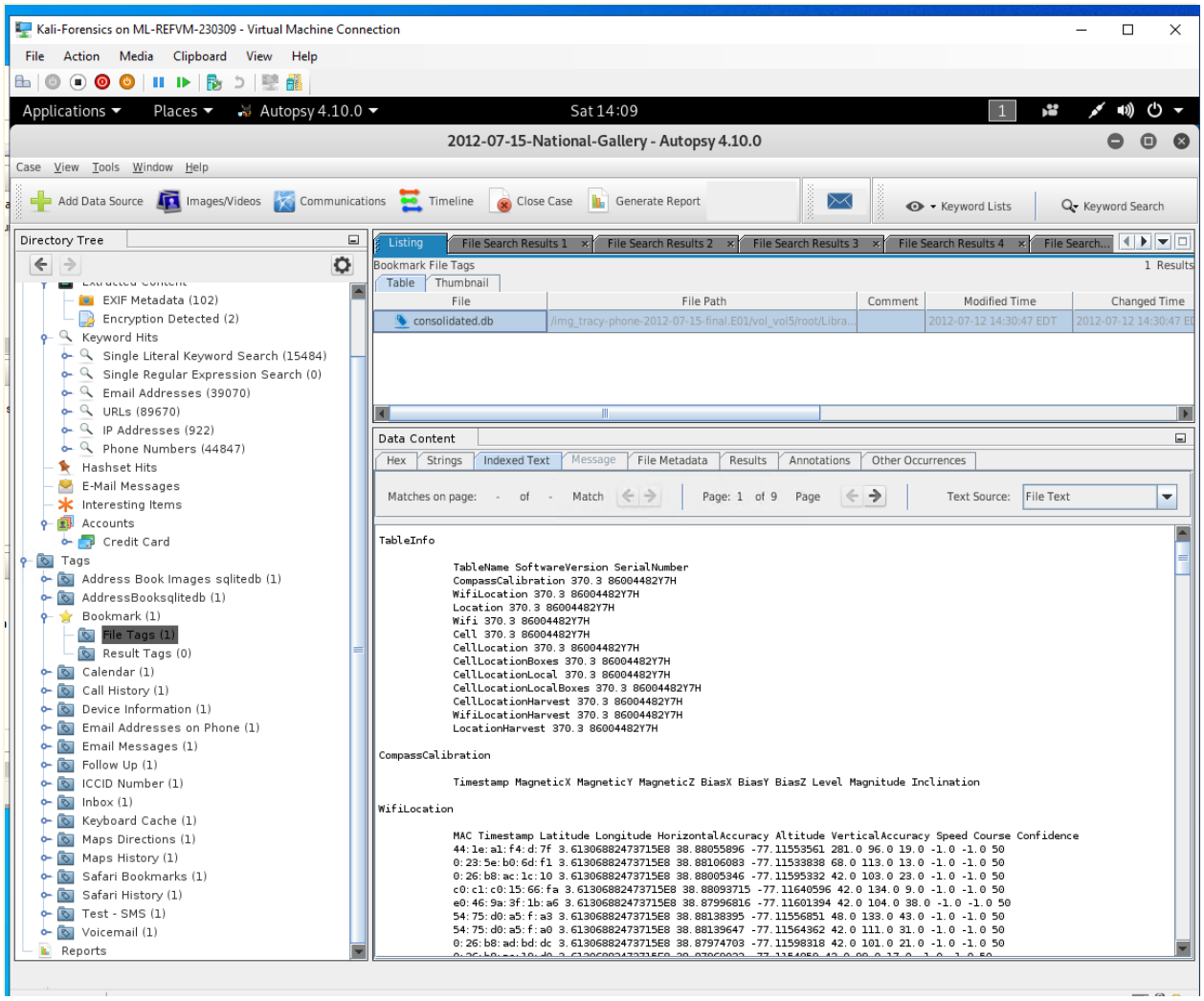
Att.1	6/28/2012 3:40PM PDT	F: King Kthings throne1966@hotmail.com T: Patsumtwelve@gmail.com Attachment: needs.txt	-A rope and javelin (using alternative means to break in) -tactical turtlenecks (what i will be wearing) -spray paint (for the cameras) -vibram five finger shoes (in order to walk silently) -pack of smokes (detecting lasers) -smoke grenades (use as a means of escape if caught)	*see note 1
	7/2/2012	From: Coral coralbluetwo@hotmail.com To: Perry Patsum perrypatsum@yahoo.com Subject: Some good news	Perry, 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'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'll let you know if I found out anything els That is weird. Hopefully it just means that it is something small, and that could be a very good thing for us.	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/Protected Index
	7/5/2012 11:51 AM PDT	From: Carry carrysum2012@yahoo.com To: Tracy tracysumtwelve@gmail.com	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	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0408520.plist
	7/6/2012 10:55 AM PDT	From: Tracy tracysumtwelve@gmail.com To: Carry carrysum2012@yahoo.com	Hey Carry, Just wanted to say thanks for lunch. I had a great time and it was good catching up with you. We should do lunch more often. - Tracy	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0408520.plist
	7/6/2012 11:49:31	From: patsumtewlve@ggmail.com To: Throne1996@hotmail.com CC: coralbluetwo@hotmail.com	King, Long time no see...I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know	*see note 1

		Sub: can't pass this up	that you are on parole right now and are probably hesitant to participate. Me and your parole officer going years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, I feel he wouldn't be too happy. It's very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don't need a search warrant. Well hit me up. You know where to find me.	
	7/9/12 11:19AM PTD	F:Tracy Sumtwelve T:coralbluetwo@hotmail.com Sub: things	ZIP folder containing 3 insurance documents related to stamps.	*See note 5
	7/9/2012 2:18PM PTD	From: Carry carrysum2012@yahoo.com To: Tracy tracysumtwelve@gmail.com(	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.	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0408520.plist
	7/10/2012 6:29AM PTD	From: Tracy tracysumtwelve@gmail.com To: Carry carrysum2012@yahoo.com	Hey, I can definitely help get your tablet in. Our security guards can be pretty ridiculous sometimes! When would you want to get in and take a look around? -Tracy	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0408520.plist
	7/10/2012 06:48AM PDT	From: Carry Sumttwentytwelve carrysum2012@yahoo.com To: tracysumtwelve@gmail.com Subject: Re: Long time no see	Awesome this will be a big help. Can i come in tommorrow, around 9?	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0408520.plist
	7/10/2012 8:15AM PTD	From: Tracy tracysumtwelve@gmail.com	Yea sure, that sounds good. See you tommorow!	/img_tracy-phone-2012-

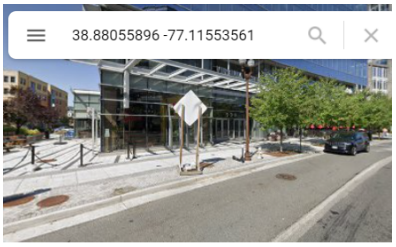
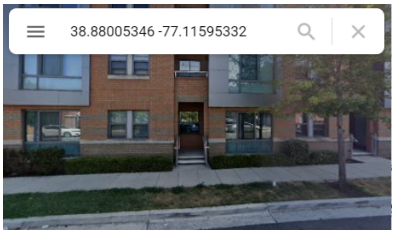
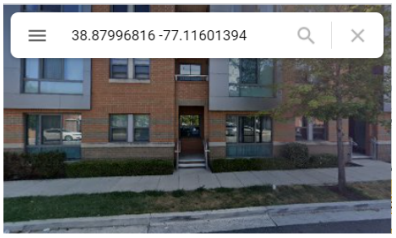
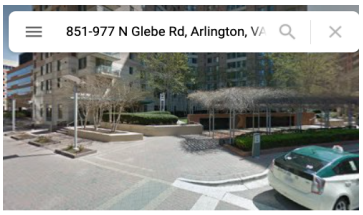
		To: Carry carrysum2012@yahoo.com		07-15-final.E01/vol_vol5//$CarvedFiles/f0401136.plist
	7/10/2012 11:19AM PTD	From: King throne1966@hotmail.com To: Patsumtwelve@gmail.com Sub: Re: can't pass up	You're too kind...I got you brotha. I need some tools in order to do this job for you. Here are some requirements that I will need ATTACHMENT	*see note 1 *see attachment 1
	7/10/2012 11:24:57	F: Patsumtwelve@gmail.com T: coralbluetwo@hotmail.com Sub: Fwd: can't pass up	This is what we need to get for the guy that's going to make our job happen	*see note 1 *see attachment 1
	7/11/2012 1:06 PM PTD	From: Tracy tracysumtwelve@gmail.com To: Carry carrysum2012@yahoo.com	Okay carrie I'm going to send this but you need to make sure no one else >sees it okay I could get in a bunch of trouble. I want to help you and I >could really use some extra cash too but please please be careful.	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0401136.plist
	7/11/2012 1:06 PM PTD	From: Carry carrysum2012@yahoo.com To: Tracy tracysumtwelve@gmail.com	Don't. Worry so much. It willbe gun	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0401136.plist
	7/11/2012 2:53PM PTD	From: Carry carrysum2012@yahoo.com	Hey so i'm putting together this event we talked about and i want to make it as painless as possible. I know that your security folk sometimes get a little out of sorts. Is there a good time or maybe you could just let know the shift changes so you dont have to know when i am going to do this. I have a pretty good budget for the event if you would like a little something for the info.	/img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f0401136.plist
	7/12/2012 1:24 PM PTD	From:Tracy TeeSumTwelve tracysumtwelve@gmail.com To: Carry carrysum2012@yahoo.com	What do you mean by that?	Name /img_tracy-phone-2012-07-15-final.E01/vol_vol5//$CarvedFiles/f040

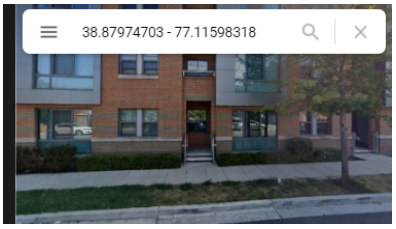
				1136.plist

Appendix B: WiFi and GPS Location Information

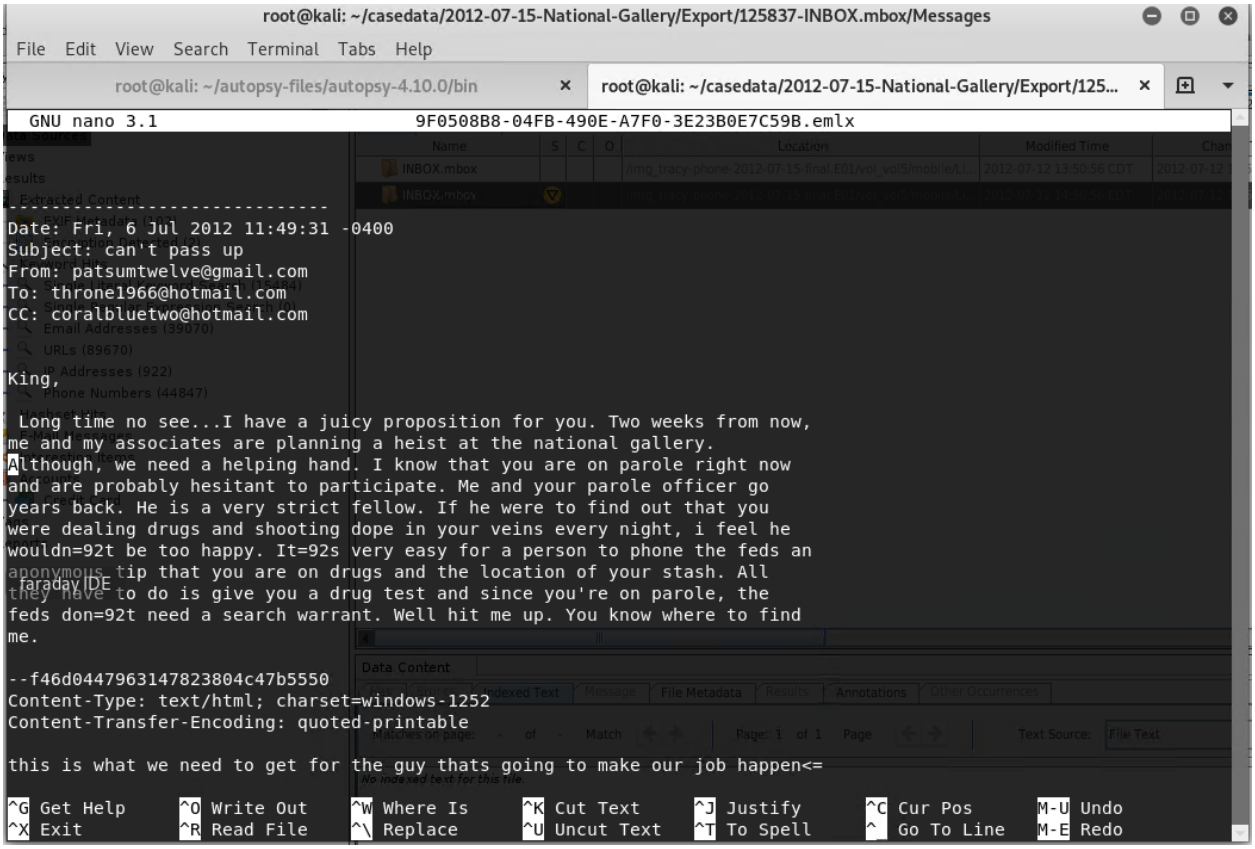


Location Information Worksheet

Location Information		
Coordinates	Address	Image
38.88055896 -77.11553561	900 N Glebe Rd, Arlington, VA 22203	
38.88106083 -77.11533838	N Glebe Rd, Arlington, VA 22203	
38.88005346 -77.11595332	801 N Wakefield St, Arlington, VA 22203	
38.88093715 - 77.11640596	Bluemont, Arlington, VA 22203	
38.87996816 -77.11601394	801 N Wakefield St, Arlington, VA 22203	
38.88138395 - 77.11556851	851-977 N Glebe Rd, Arlington, VA 22203	

38.87974703 - 77.11598318	801 N Wakefield St, Arlington, VA 22203	

Screenshot of email to King from PatSumTwelve: 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx



Note 1:

Message File Path: /casedata/2012-07-15-National-Gallery/Export/125837-INBOX.mbox/Messages/9F0508B8-0490E-490E-A7F0-3E23B0E7C59B.emlx

Attachment File Path: /casedata/2012-07-15-National-Gallery/Export/125837-INBOX.mbox/Attachments/60/2/needs.txt

Screenshot of Perry Patsum Email: 3896FC6F-A0836-4D39-B0A2-CE68368D44CA.emlx

```
Subject: Crazydave by the VMs
To: Coral Bluetwo <coralbluetwo@hotmail.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="879925033-562466984-1340141940=:2892"
Return-Path: perrypatsum@yahoo.com
X-OriginalArrivalTime: 19 Jun 2012 21:39:04.0552 (UTC) FILETIME=[F2C7C680:01CD4E63]

--879925033-562466984-1340141940=:2892
Content-Type: multipart/alternative; boundary="879925033-469252838-1340141940=:2892"

--879925033-469252838-1340141940=:2892
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

Hey Coral,=A0=0A=0AJust got your email. That took longer than expected! Oh =
well! =0A=0A=0AYou've got to check out this new song by the VMs. I love the=
 base. Tell me what you think!=0A=0APerry=0A
--879925033-469252838-1340141940=:2892
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

<html><body><div style=3D"color:#000; background-color:#fff; font-family:ti=
mes new roman, new york, times, serif;font-size:12pt"><div>Hey Coral, =
</div><div><br></div><div>Just got your email. That took longer than expect=
ed! Oh well! <br></div><div><br></div><div>You've got to check out this new=
 song by the VMs. I love the base. Tell me what you think!</div><div><br></=
div><div>Perry<br></div></div></body></html>
--879925033-469252838-1340141940=:2892--
--879925033-562466984-1340141940=:2892
Content-Type: audio/mpeg; name="Crazydave1.mp3"
Content-Transfer-Encoding: base64

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit       ^R Read File   ^\ Replace    ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo
```

Note 2: /casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/

```
root@kali:~/casedata/Andy-First-Case/Export/43149-INBOX.mbox/Messages# ls
01FE9965-A923-40CF-A78A-72CE3BD26571.emlx        8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx-slack
01FE9965-A923-40CF-A78A-72CE3BD26571.emlx-slack  9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx        9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx-slack
3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx-slack  F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx        F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx-slack
root@kali:~/casedata/Andy-First-Case/Export/43149-INBOX.mbox/Messages# nano 3896FC6F-A083-4D39-B0A2-CE68368D44CA.eml
x
root@kali:~/casedata/Andy-First-Case/Export/43149-INBOX.mbox/Messages# nano 3896FC6F-A083-4D39-B0A2-CE68368D44CA.eml
x
root@kali:~/casedata/Andy-First-Case/Export/43149-INBOX.mbox/Messages#
```

Nano 3896FCF-A083-4D39-B0A2-CE68368D44CA.EMLX

Note 3: /casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2

```
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2# ls
documents.zip  documents.zip-slack
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2# nano documents.zip
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2# unzip documents.zip

Archive:  documents.zip
   creating: docs/
[documents.zip] docs/.DS_Store password: root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.m
box/Attachments/61/2#
```

Documents.zip file password crack

```
root@kali: ~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments...
File  Edit  View  Search  Terminal  Tabs  Help
root@kali: ~/autopsy-fil...   root@kali: ~/casedata/2...   root@kali: ~/casedata/2...
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachm
ents/61/2# fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt documents.zip

PASSWORD FOUND!!!!: pw == Hercules
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachm
ents/61/2#
```

PDF Files from Documents.zip

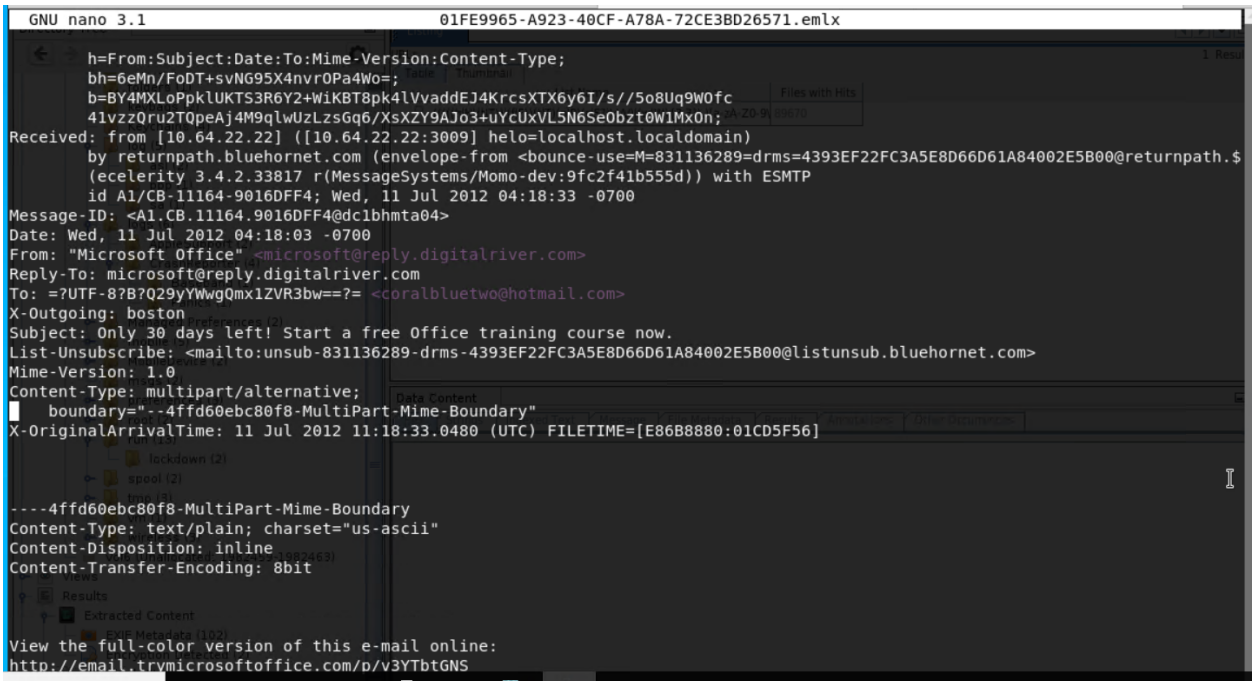
Note 4:

Email: F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx

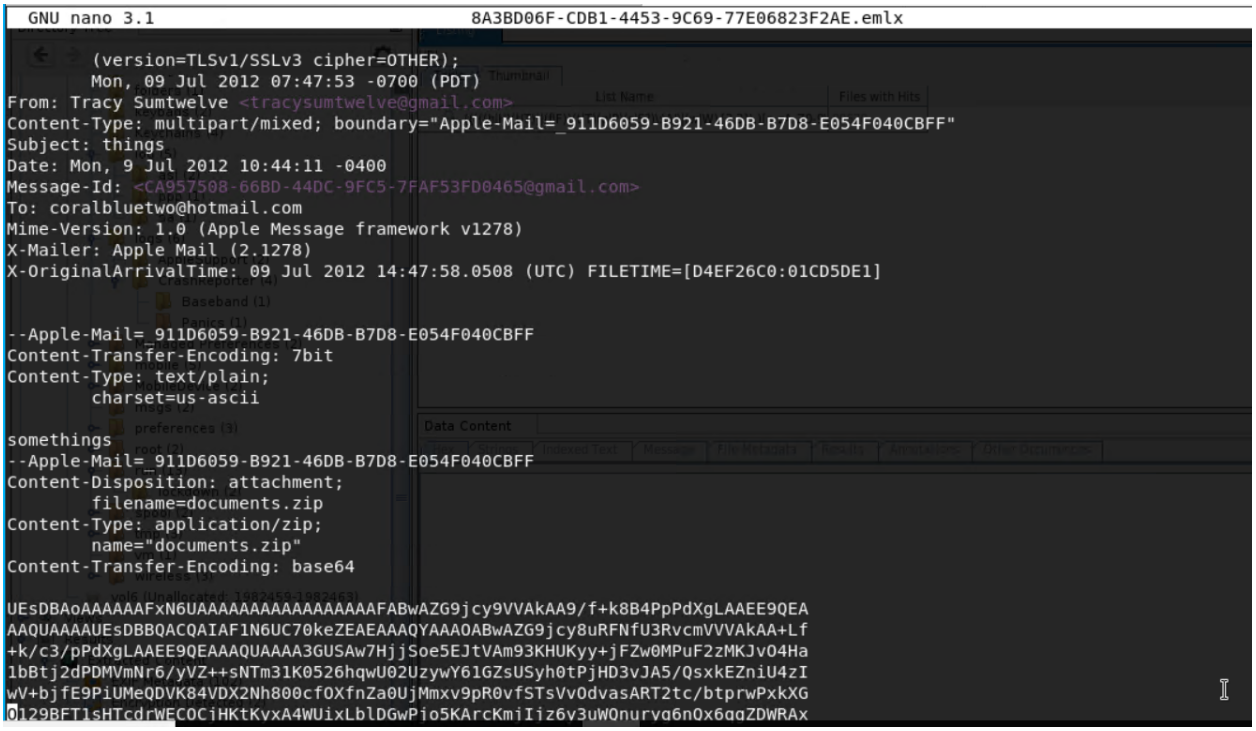
```
GNU nano 3.1                    F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx

        by homiemail-a15.g.dreamhost.com (Postfix) with ESMTPSA id A5EE576C058
        for <coralbluetwo@hotmail.com>; Thu,  5 Jul 2012 12:58:41 -0700 (PDT)
Content-Type: multipart/alternative;
 boundary="===============7630960988326475069=="
MIME-Version: 1.0
Subject: Busy
From: Woina.Honril@m57.biz
To: coralbluetwo@hotmail.com
Cc:
Message-Id: <20120705195841.A5EE576C058@homiemail-a15.g.dreamhost.com>
Date: Thu,  5 Jul 2012 12:58:41 -0700 (PDT)
Return-Path: Woina.Honril@m57.biz
X-OriginalArrivalTime: 05 Jul 2012 19:58:42.0680 (UTC) FILETIME=[94130780:01CD5AE8]

--===============7630960988326475069==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

I didn't.
--===============7630960988326475069==
Content-Type: application/octet-stream
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="000001.doc"

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAASwAAAAAAAAA
EAAATQAAAAEAAAD+////AAAAAEoAAAD/////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
```

Message File Path: /casedata/2012-07-15-National-Gallery/Export/125837-INBOX.mbox/Messages/F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx

Email: 01FE9965-A923-A78A-72CE3BD26571.emlx



Email:8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx



Note 5: These insurance documents are evidence that Tracy was planning to steal the stamps from the National Gallery of Art:

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

For The internal use of National Gallery and MyIStamp Collections Only.

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

For The Internal use of National Gallery and MyIStamp Collections Only.

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**

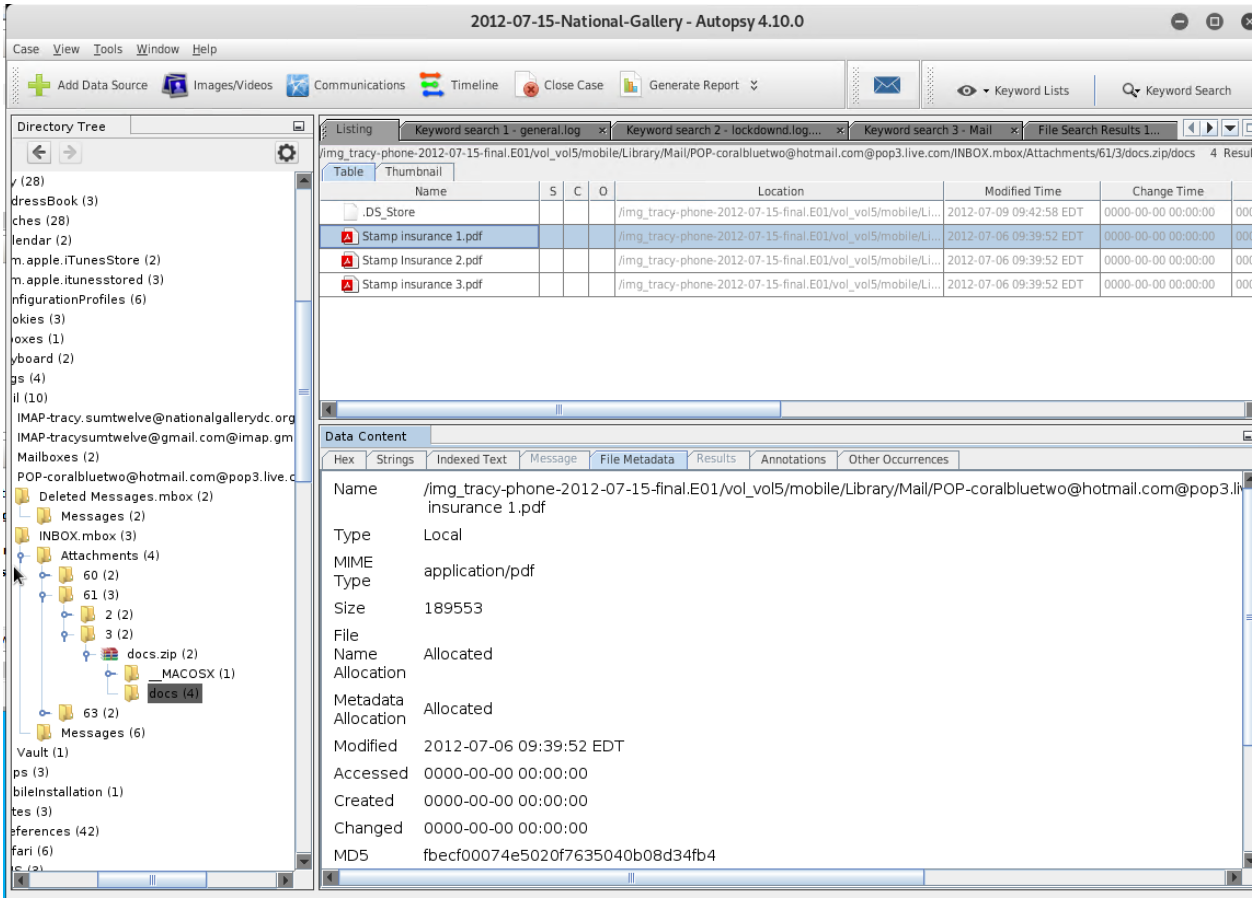
Terms do not cover period of transport from or to the National Gallery.

D'Mann

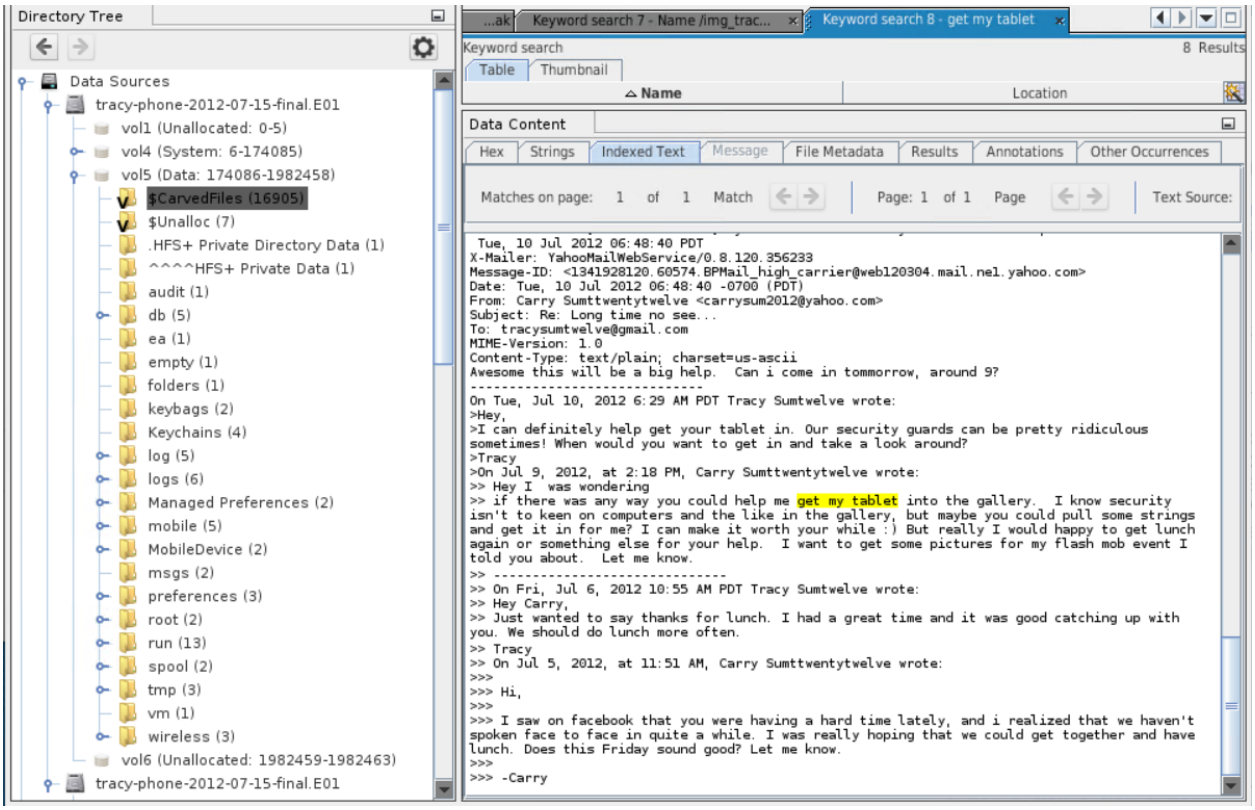
President National Gallery DC

For The Internal use of National Gallery and MyIStamp Collections Only.

The timestamp on the Stamp Insurance pdfs is 7/6/2012 9:39:52 EDT



Additional Images:


Directory Tree
Data Sources
tracy-phone-2012-07-15-final.E01
vol1 (Unallocated: 0-5)
vol4 (System: 6-174085)
vol5 (Data: 174086-1982458)
$CarvedFiles (16905)
$Unalloc (7)
.HFS+ Private Directory Data (1)
^^^^HFS+ Private Data (1)
audit (1)
db (5)
ea (1)
empty (1)
folders (1)
keybags (2)
Keychains (4)
log (5)
logs (6)
Managed Preferences (2)
mobile (5)
MobileDevice (2)
msgs (2)
preferences (3)
root (2)
run (13)
spool (2)
tmp (3)
vm (1)
wireless (3)
vol6 (Unallocated: 1982459-1982463)
tracy-phone-2012-07-15-final.E01
Keyword search 7 - Name /img_trac...
Keyword search 8 - get my tablet
Keyword search
8 Results
Table
Thumbnail
Name
Location
Data Content
Hex
Strings
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Matches on page: 1 of 1 Match
Page: 1 of 1 Page
Text Source:
Tue, 10 Jul 2012 06:48:40 PDT
X-Mailer: YahooMailWebService/0.8.120.356233
Message-ID: <1341928120.60574.BPMail_high_carrier@web120304.mail.ne1.yahoo.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?
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
>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.
>> ----------
>> On Fri, Jul 6, 2012 10:55 AM PDT Tracy Sumtwelve wrote:
>> Hey Carry,
>> Just wanted to say thanks for lunch. I had a great time and it was good catching up with you. We should do lunch more often.
>> Tracy
>> On Jul 5, 2012, at 11:51 AM, Carry Sumttwentytwelve 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