

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

[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) 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@nationalgallerydc.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 2 Result

Name	S	C	O	Location	Modified Time	Change Time
sms.db				/img_tracy-phone-2012-07-15-final.E01/vol_vo5/mobile/L...	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_vo5/mobile/L...	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 +15713082396 1339612238 I don't have any big plans. How about you? 3 0 3 0 0 4 0 us 1
9 +170828296071 13295612426 Ok, sounds good. 3 0 4 0 0 4 0 us 1
12 +170828296071 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 +170828296071 1341324272 moving schools at this point would be the worst! I would rather live with dad and stay at prufrock than change schools. 3 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 +15713082396 1341586939 Hey, can you give me a call. 3 0 3 0 0 4 0 us 1
17 +15713082396 1341587317 Sis I'm really busy can we do this later? 2 0 3 0 0 4 0 us 1
18 +15713082396 1341587514

```

No pat this is important I need you to call me soon 3 0 3 0 0 4 0 us 1

19 +15713082396 1341587611 Ok, ok I'll call in. 5 2 0 3 0 0 4 0 us 1

20 +12027252124 1341592096 I have a table inside. 2 0 5 0 0 4 0 us 1

21 +12027252124 1341592070 Okay br. 3 0 5 0 0 4 0 us 1

22 +12069100932 13416187795 Congratulations, your entry in last month's 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 +15713082396 13415933979 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

24 +15713082396 13415935884 Sure thing I'll get on it. 3 0 3 0 0 4 0 us 0

26 +13415982229 33 0 3 0 0 0 0 us 0

27 +170828296071 13415940718 Going to lunch. You want to go????! 3 0 4 0 0 4 0 us 1

28 +170828296071 13415944364 Back at work. 3 0 4 0 0 0 0 us 1

29 +170828296071 13415946704 I'm busy. Maybe this weekend if dad isn't busy. 2 0 4 0 0 0 0 us 1

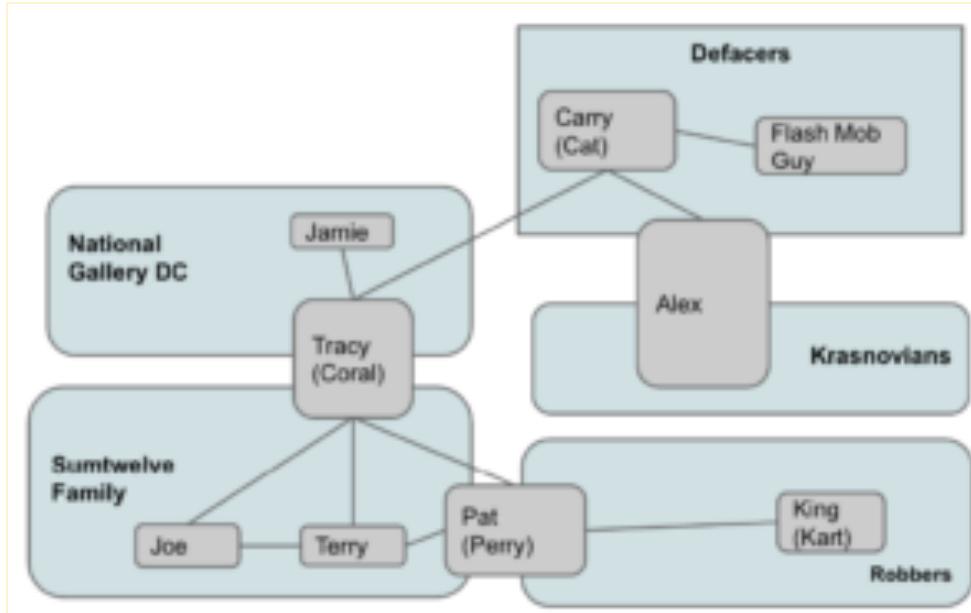
30 +12027252124 1342010505 I'm almost there where should I meet you? 2 0 5 0 0 4 0 us 1

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 +170828296071 13421141330 I really want to go to Dad's this weekend. He said he'll take me shopping for school. 0 0 0 0 0 0 us 0

sqlite_sequence



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 correspondence 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_vo5//\$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_vo5//\$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 else. 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_vo5/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_vo5//\$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_vo5//\$CarvedFiles/f0408520.plist
	7/6/2012 11:49:31	From: patsumtwelve@googlemail.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_vo5//\$/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_vo5//\$/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_vo5//\$/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-

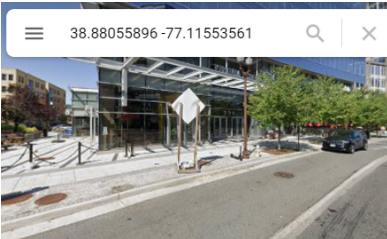
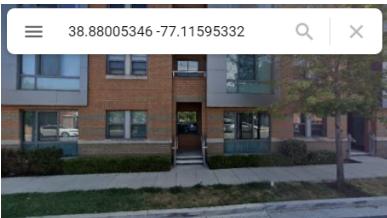
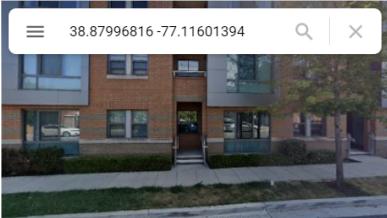
		To: Carry carrysum2012@yahoo.com		07-15-final.E01/vol_vo5//\$/CarvedFiles/f0401136.plist
	7/10/2012 11:19AM PTD	From: King throne1966@hotmail.com To: Patsumtwelve@gmail.com Sub: Re: can't pass up	You're too kind...I got you brotha. I need some tools in order to do this job for you. Here are some requirements 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_vo5//\$/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 will be gun	/img_tracy-phone-2012-07-15-final.E01/vol_vo5//\$/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_vo5//\$/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_vo5//\$/CarvedFiles/f0401136.plist

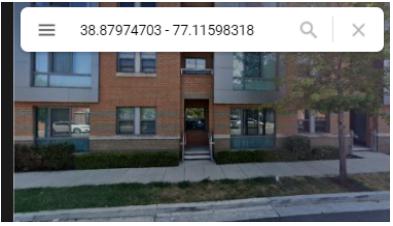
Appendix B: WiFi and GPS Location Information

The screenshot shows the Autopsy 4.10.0 forensic analysis tool interface. The main window title is "2012-07-15-National-Gallery - Autopsy 4.10.0". The left sidebar displays a "Directory Tree" with various forensic findings, including "EXIF Metadata (102)", "Encryption Detected (2)", "Keyword Hits" (with sub-options like "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", and "Reports". The central pane shows a "File Search Results 1" tab with a table titled "Bookmark File Tags" containing one result: "consolidated.db" located at "/img_tracy-phone-2012-07-15-final.E01/vol_vol/root/Library/consolidated.db". Below this is a "Data Content" pane with tabs for "Hex", "Strings", "Indexed Text", "Message", "File Metadata", "Results", "Annotations", and "Other Occurrences". The "File Metadata" tab is selected, showing details for the consolidated.db file. At the bottom of the central pane, there is a "TableInfo" section displaying raw data for tables such as "CompassCalibration", "WifiLocation", and "Location". The "CompassCalibration" table includes columns for MAC, Timestamp, Latitude, Longitude, HorizontalAccuracy, Altitude, VerticalAccuracy, Speed, Course, and Confidence. The "WifiLocation" table includes columns for MAC, Timestamp, Latitude, Longitude, HorizontalAccuracy, Altitude, VerticalAccuracy, Speed, Course, and Confidence.

Table	Column	Value
CompassCalibration	MAC	44:1e:a1:f4:d7f
CompassCalibration	Timestamp	3.61306882473715E8
CompassCalibration	Latitude	88.0055896
CompassCalibration	Longitude	-77.11553561
CompassCalibration	HorizontalAccuracy	281.96
CompassCalibration	Altitude	0.19
CompassCalibration	VerticalAccuracy	0.0
CompassCalibration	Speed	-1.0
CompassCalibration	Course	-1.0
CompassCalibration	Confidence	50
WifiLocation	MAC	0:23:5e:b0:6d:f1
WifiLocation	Timestamp	3.61306882473715E8
WifiLocation	Latitude	88.0106083
WifiLocation	Longitude	-77.11533838
WifiLocation	HorizontalAccuracy	68.0
WifiLocation	Altitude	113.0
WifiLocation	VerticalAccuracy	0.13
WifiLocation	Speed	0.0
WifiLocation	Course	-1.0
WifiLocation	Confidence	50
Location	MAC	0:26:b8:ac:1c:1c
Location	Timestamp	3.61306882473715E8
Location	Latitude	88.0005346
Location	Longitude	-77.11595332
Location	HorizontalAccuracy	42.0
Location	Altitude	103.0
Location	VerticalAccuracy	0.23
Location	Speed	0.0
Location	Course	-1.0
Location	Confidence	50
Cell	MAC	c0:c1:c0:15:66:fa
Cell	Timestamp	3.61306882473715E8
Cell	Latitude	88.08093715
Cell	Longitude	-77.11640596
Cell	HorizontalAccuracy	42.0
Cell	Altitude	134.0
Cell	VerticalAccuracy	0.9
Cell	Speed	-1.0
Cell	Course	-1.0
Cell	Confidence	50
CellLocation	MAC	e0:46:9a:3f:1b:a6
CellLocation	Timestamp	3.61306882473715E8
CellLocation	Latitude	87.87996816
CellLocation	Longitude	-77.11601394
CellLocation	HorizontalAccuracy	42.0
CellLocation	Altitude	104.0
CellLocation	VerticalAccuracy	0.38
CellLocation	Speed	-1.0
CellLocation	Course	-1.0
CellLocation	Confidence	50
CellLocationLocal	MAC	54:75:d0:a5:f1:a3
CellLocationLocal	Timestamp	3.61306882473715E8
CellLocationLocal	Latitude	88.08138395
CellLocationLocal	Longitude	-77.11556851
CellLocationLocal	HorizontalAccuracy	48.0
CellLocationLocal	Altitude	133.0
CellLocationLocal	VerticalAccuracy	0.43
CellLocationLocal	Speed	-1.0
CellLocationLocal	Course	-1.0
CellLocationLocal	Confidence	50
CellLocationLocalBoxes	MAC	0:26:b8:ad:bd:dc
CellLocationLocalBoxes	Timestamp	3.61306882473715E8
CellLocationLocalBoxes	Latitude	88.07974703
CellLocationLocalBoxes	Longitude	-77.11598318
CellLocationLocalBoxes	HorizontalAccuracy	42.0
CellLocationLocalBoxes	Altitude	101.0
CellLocationLocalBoxes	VerticalAccuracy	0.21
CellLocationLocalBoxes	Speed	-1.0
CellLocationLocalBoxes	Course	-1.0
CellLocationLocalBoxes	Confidence	50
CellLocationHarvest	MAC	0:26:b8:ad:bd:dc
CellLocationHarvest	Timestamp	3.61306882473715E8
CellLocationHarvest	Latitude	88.07974703
CellLocationHarvest	Longitude	-77.11598318
CellLocationHarvest	HorizontalAccuracy	42.0
CellLocationHarvest	Altitude	101.0
CellLocationHarvest	VerticalAccuracy	0.21
CellLocationHarvest	Speed	-1.0
CellLocationHarvest	Course	-1.0
CellLocationHarvest	Confidence	50
LocationHarvest	MAC	0:26:b8:ad:bd:dc
LocationHarvest	Timestamp	3.61306882473715E8
LocationHarvest	Latitude	88.07974703
LocationHarvest	Longitude	-77.11598318
LocationHarvest	HorizontalAccuracy	42.0
LocationHarvest	Altitude	101.0
LocationHarvest	VerticalAccuracy	0.21
LocationHarvest	Speed	-1.0
LocationHarvest	Course	-1.0
LocationHarvest	Confidence	50

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

root@kali: ~/casedata/2012-07-15-National-Gallery/Export/125837-INBOX.mbox/Messages

File Edit View Search Terminal Tabs Help

root@kali: ~/autopsy-files/autopsy-4.10.0/bin x root@kali: ~/casedata/2012-07-15-National-Gallery/Export/125... x

GNU nano 3.1 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

Name	S	C	O	Location	Modified Time	Char
INBOX.mbox				/img/tracy-phone-2012-07-15-final.E01\vol.vol5/mobile/t...	2012-07-12 13:50:56 CDT	2012-07-12 13:50:56 CDT
INBOX.mbox				/img/tracy-phone-2012-07-15-final.E01\vol.vol5/mobile/t...	2012-07-14 14:50:56 EDT	2012-07-14 14:50:56 EDT

Date: Fri, 6 Jul 2012 11:49:31 -0400
Subject: can't pass up
From: patsumtwelve@gmail.com
To: throne1966@hotmail.com
CC: coralbluetwo@hotmail.com
Email Addresses (39070)
URLs (89670)
King,
Phone Numbers (44847)

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 that you are on parole right now and are probably hesitant to participate. Me and your parole officer go 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.

--f46d0447963147823804c47b5550
Content-Type: text/html; charset=windows-1252
Content-Transfer-Encoding: quoted-printable
this is what we need to get for the guy that's going to make our job happen<=No indexed text for this file.

^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 ^A Go To Line M-E Redo

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
[REDACTED]
Hey Coral,=A0=A0=A0Just got your email. That took longer than expected! Oh =
well! =A0=A0=A0You've got to check out this new song by the VMs. I love the=
base. Tell me what you think!=A0=A0APerry=A0
--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,&nbsp;=
</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>Perry<br></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@casedata:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2# ls  
documents.zip  documents.zip-slack  
root@casedata:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2# nano documents.zip  
root@casedata:~/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@casedata:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Attachments/61/2#
```

Documents.zip file password crack

PDF Files from Documents.zip

Note 4:

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

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

```

GNU nano 3.1                                         01FE9965-A923-40CF-A78A-72CE3BD26571.emlx
h=From:Subject:Date:To:Mime-Version:Content-Type;
bh=6eMn/FoDT+svNG95X4nvr0Pa4Wos;                                Table   Thumnbail   1 Result
b=BY4MXLoPpkluUKTS3R6Y2+WlKBT8pk4lVvaddEJ4KrcsXTX6yGI/s//5o8Uq9Wofc
41vzzQru2TQpeAj4M9qlwLzLzsGg6/XsXZY9Ajo3+uYcUxVL5N6seObzt0W1MxOn;    Files with Hits
Received: from [10.64.22.22] ([10.64.22.22:3009] helo=localhost.localdomain)
by returnpath.bluehornet.com (envelope-from <bounce-use=M=831136289=drms=4393EF22FC3A5E8D66D61A84002E5B00@returnpath.$
(ecelerity 3.4.2.3381 r(MessageSystems/Momo-dev:9fc2f41b555d)) with ESMTP
id A1/CB-11164-9016dff4; Wed, 11 Jul 2012 04:18:33 -0700
Message-ID: <A1.CB.11164.9016dff4@dc1bhmta04>
Date: Wed, 11 Jul 2012 04:18:03 -0700
From: "Microsoft Office" <microsoft@reply.digitalriver.com>
Reply-To: microsoft@reply.digitalriver.com
To:=?UTF-8?B?Q29yYWwgmx1ZVR3bw==?= <coralbluetwo@hotmail.com>
X-Outgoing: boston
Subject: Only 30 days left! Start a free Office training course now.
List-Unsubscribe: <mailto:unsub-831136289-drms-4393EF22FC3A5E8D66D61A84002E5B00@listunsub.bluehornet.com>
Mime-Version: 1.0
Content-Type: multipart/alternative;
boundary="----4ffd60ebc80f8-MultiPart-Mime-Boundary"
X-OriginalArrivalTime: 11 Jul 2012 11:18:33.0480 (UTC) FILETIME=[E86B8880:01CD5F56]

Data Content
lockdown (2)
spool (2)
tmp (3)
----4ffd60ebc80f8-MultiPart-Mime-Boundary
Content-Type: text/plain; charset="us-ascii"
Content-Disposition: inline
Content-Transfer-Encoding: 8bit
Views
Results
Extracted Content
Metadatas (102)
View the full-color version of this e-mail online:
http://email.trymicrosoftoffice.com/p/v3YTbtGNS

```

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

```

GNU nano 3.1                                         8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
(version=TLSv1/SSLv3 cipher=OTHER);
Mon, 09 Jul 2012 07:47:53 -0700 (PDT) Thumnbail   List Name   Files with Hits
From: Tracy Sumtwelve <tracysumtwelve@gmail.com>
Content-Type: multipart/mixed; boundary="Apple-Mail=_911D6059-B921-46DB-B7D8-E054F040CBFF"
Subject: things
Date: Mon, 9 Jul 2012 10:44:11 -0400
Message-Id: <CA957508-66BD-44DC-9FC5-7FAF53FD0465@gmail.com>
To: coralbluetwo@hotmail.com
Mime-Version: 1.0 (Apple Message framework v1278)
X-Mailer: Apple Mail (2.1278)
X-OriginalArrivalTime: 09 Jul 2012 14:47:58.0508 (UTC) FILETIME=[D4EF26C0:01CD5DE1]
Crashreporter (4)
Baseband (1)
--Apple-Mail=_911D6059-B921-46DB-B7D8-E054F040CBFF
Content-Transfer-Encoding: 7bit
Content-Type: text/plain;
charset=us-ascii
msg (2)
preferences (3)
somethings
--Apple-Mail=_911D6059-B921-46DB-B7D8-E054F040CBFF
Content-Disposition: attachment;
filename=documents.zip
Content-Type: application/zip;
name="documents.zip"
Content-Transfer-Encoding: base64
Wireless (5)
UEsDBAoAAAAAAFXN6UAaaaaaaaaaaaaAAAABwAZG9jcy9VVAkAA9/f+k8B4PpPdXgLAEE9QEAAQAAAUEsDBBQACQAIAF1N6UC70keZEAAAQYAAAABwAZG9jcy8URFnfU3RvcVVVAkAA+l.f+k/c3/pPdXgLAAE9QEAQAAA3GUsAw7HjSoe5EJtVAm93KHUKyy+jFZw0MPuF2zMKJv04Ha1bBtj2dPDMVmNr6/yVZ++sNm31K0526hqwU02UzywY61GzsUsyh0tPjHD3vJA5/QsxKEZniU4zIwV+bjfE9PiUMeqDVK84VDX2Nh800cf0XfnZa0UjMmxv9pR0vfSTsVv0dvasART2tc/bptrwPxkXG0129BFT1sHTcdrWECoCiHKtKvxA4WUixlblDGwPio5KArckMiIiz6v3uWOnurva6n0x6aaZDWRAx

```

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: MyStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MyStamp 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 MacArthur	\$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

A handwritten signature in black ink, appearing to read "D'Mann".

President National Gallery DC

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

NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MyStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyStamp 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 Nepal	\$27,000.00

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

D'Mann

A handwritten signature of D'Mann.

President National Gallery DC

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



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MyStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyStamp 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	\$49,000.00
Lot # 26. Stamp of Kazakhstan2	\$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 MyStamp Collections Only.

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

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

Listing Keyword search 1 - general.log Keyword search 2 - lockdownd.log... Keyword search 3 - Mail File Search Results 1... 4 Results

Name	S	C	O	Location	Modified Time	Change Time
DS_Store				/img_tracy-phone-2012-07-15-final.E01/vol_vo1/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs	2012-07-09 09:42:58 EDT	0000-00-00 00:00:00 00
Stamp insurance 1.pdf				/img_tracy-phone-2012-07-15-final.E01/vol_vo1/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs	2012-07-06 09:39:52 EDT	0000-00-00 00:00:00 00
Stamp Insurance 2.pdf				/img_tracy-phone-2012-07-15-final.E01/vol_vo1/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs	2012-07-06 09:39:52 EDT	0000-00-00 00:00:00 00
Stamp insurance 3.pdf				/img_tracy-phone-2012-07-15-final.E01/vol_vo1/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs	2012-07-06 09:39:52 EDT	0000-00-00 00:00:00 00

Data Content

Hex Strings Indexed Text Message File Metadata Results Annotations Other Occurrences

Name /img_tracy-phone-2012-07-15-final.E01/vol_vo1/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs

Type Local

MIME application/pdf

Type

Size 189553

File Name Allocated

Allocation

Metadata Allocation

Allocation

Modified 2012-07-06 09:39:52 EDT

Accessed 0000-00-00 00:00:00

Created 0000-00-00 00:00:00

Changed 0000-00-00 00:00:00

MD5 fbef00074e5020f7635040b08d34fb4

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

...ak Keyword search 7 - Name /img_trac... x Keyword search 8 - get my tablet x 8 Results

Keyword search

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.nel.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 Sumtwise 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 Sumtwise 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

```