Forensic Case Report
National Gallery DC

By Gerald Blackmon

Description of Project

- The 2012 National Gallery DC scenario spans approximately 10 days and encompasses two distinct yet intertwined story arcs. The scenario is centered around an employee at the National Gallery DC Art Gallery. Criminal plans for both theft and defacement are discussed amongst actors during the scenario, and evidence may remain across the digital devices they used. The scenario is terminated upon suspicious activity being reported to law enforcement at which point certain devices are seized and network traffic logs are requested. The scenario materials can be used as both teaching material and for forensics research. **Participants are instructed to gather as much evidence as possible to establish the case for prosecution using Kali Linux OS with Autopsy**. Like the 2009-M57-Patents scenario, images were taken at the end of every day of the scenario. The materials include disk images of hard drives and both logical and physical images of mobile devices. Network captures were performed using the SSLstrip tool, allowing for capture files to be available with and without encrypted SSL traffic.

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.

1. Evidence was discovered in personal communications (email, SMS) that indicated Tracy was motivated by monetary gain as a result of increased financial difficulty.
2. Evidence uncovered steps to begin using an alias with her brother Pat (aka Perry) and her alias (Coral)
3. Communications between Tracy and Pat indicates a plot to steal valuable stamps based on insurance records Pat comes into contact with.
4. Evidence indicates Tracy was aware of Pat's communications with a man by the name of "King". This correspondence included emails with an attached file (needs.txt) which requested items for the crime as well as their purpose.

5. Evidence of correspondence detailing a plot to allow access to the building between Carry and Tracy. Tracy agreed to assist with security schedules and smuggle a tablet into the Gallery.

Equipment and Tools

The Equipment and Applications listed were used to analyze images of the data present on Tracys iphone. The file tracy-phone-2012-07-15-final.E01 was examined and relevant data was examined and extracted.

Autopsy Application within Kali-Linux OS
SQLite Database browser
Google Earth GPS
GUNZIP
Evince Pdf reader

The evidence found on Tracy's iphone was gathered and extracted to the Directory listed below for further review:

:~/casedata/2012-07-15-National-Gallery/Export/

Details of Tracy's iPhone

Artifact 1

Name	Findings	Location in iPhone image file
Model	Iphone 3G	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelves iPhone	/logs/lockdown.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	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	01202100373539	/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: Alias:Coral
Phone Number: (703) 340-9961
Personal Email: tracysumtwelve@gmail.com coralbluetwo@hotmail.com
Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused

Pat: Alias: Perry
Phone Number: 15713083236
Email: patsumtwelve@gmail.com perrypatsum@yahoo.com
Relationship: Brother of Tracy - DC detective (accomplice)

Terry:
Phone Number: 17038296071
Email: N/A
Relationship: Daughter of Tracy

Joe:
Phone Number:
Email:
Relationship: Ex husband of Tracy - father of Terry

Carry:
Phone Number: 12027252124
Email: carrysum2021@yahoo.com
Relationship: Aquaintance of Tracy (accomplice in plot to deface National Gallery)

King: Phone number:
Email: throne1966@hotmail.com
Relationship: Acquaintance of Pat (accomplice)

Tracy and Pat communicated using both their names and aliases but continued to use familiar language to reassert the nature of their relationship such as “bro” and “Sis” in speaking. Carry is named as a friend of tracy in her SMS messages. King is an acquaintance of Pat and confirms their prior relationship in his familiar language used stating “long time no see”. Terry is the daughter of Tracy and Joe and shows up in multiple data sets as the topic of finances and custody. Terry is not connected to any criminal activity by the evidence listed within.

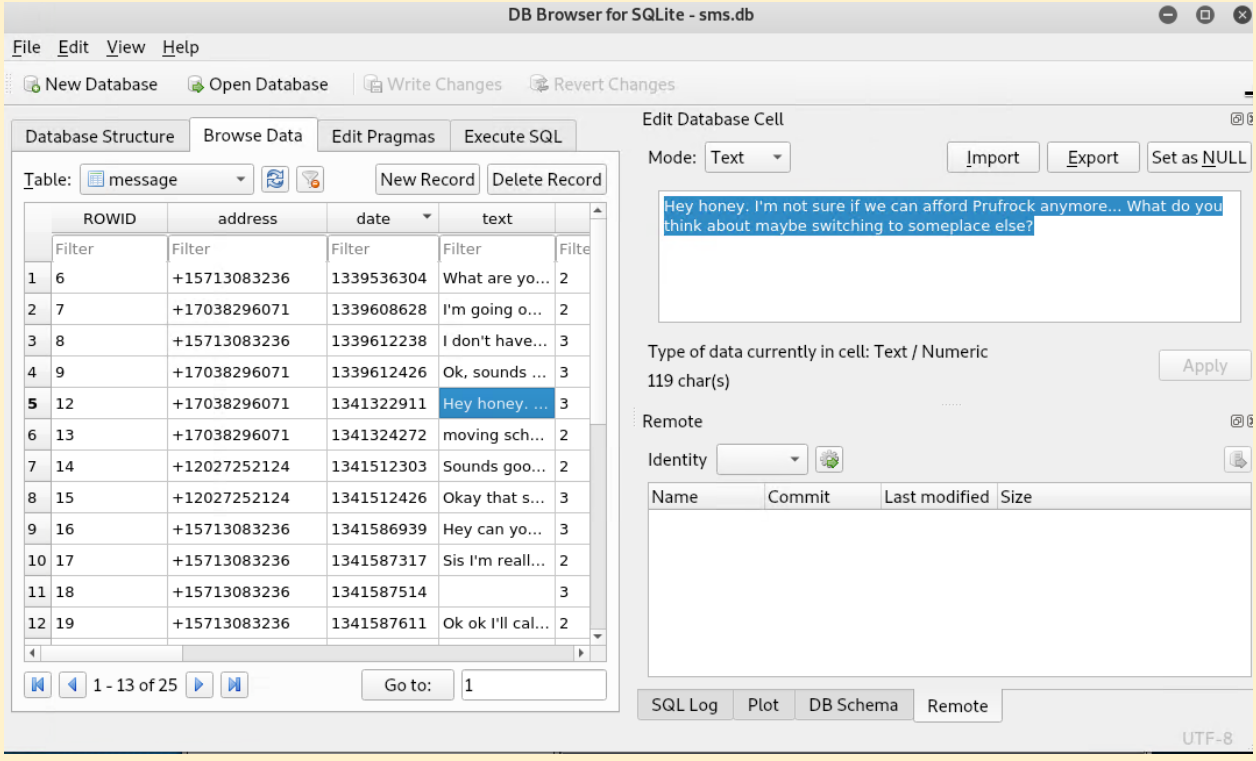
Correspondence Evidence

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.

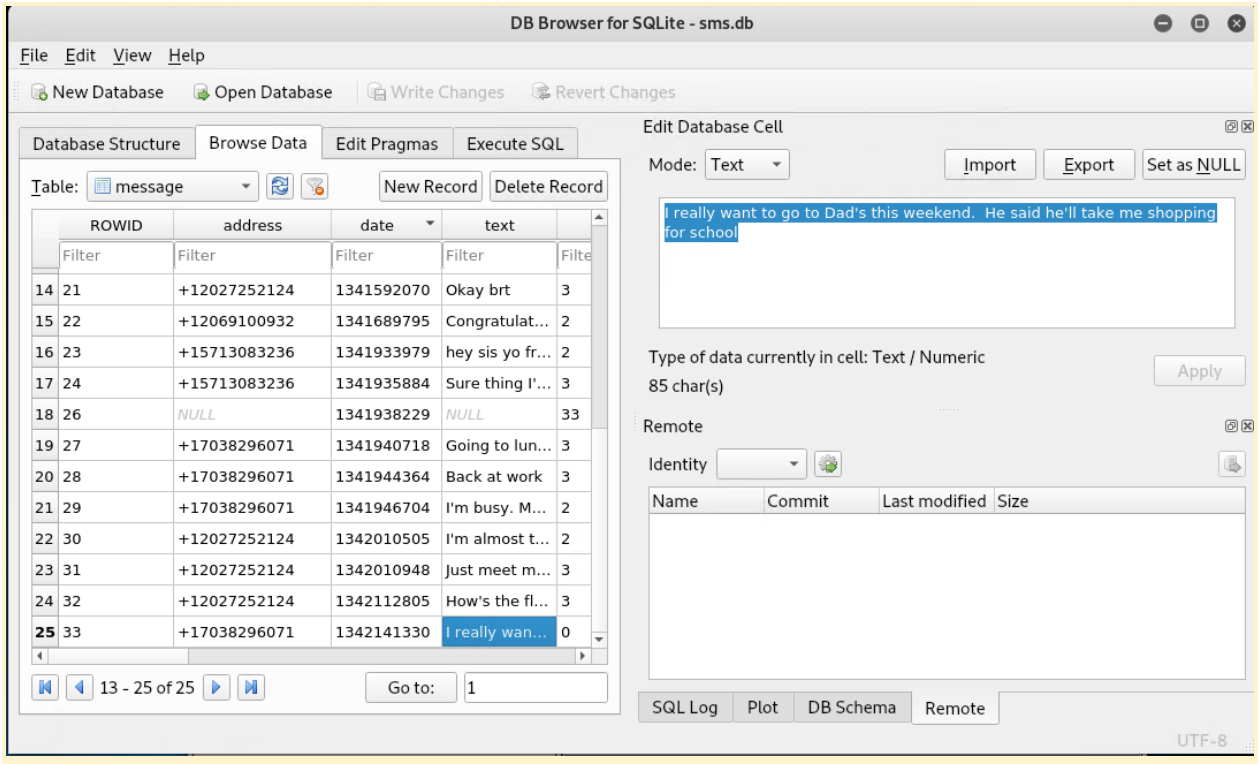
SMS reveals Money troubles for Tracy
Terry to Tracy

Artifact 2



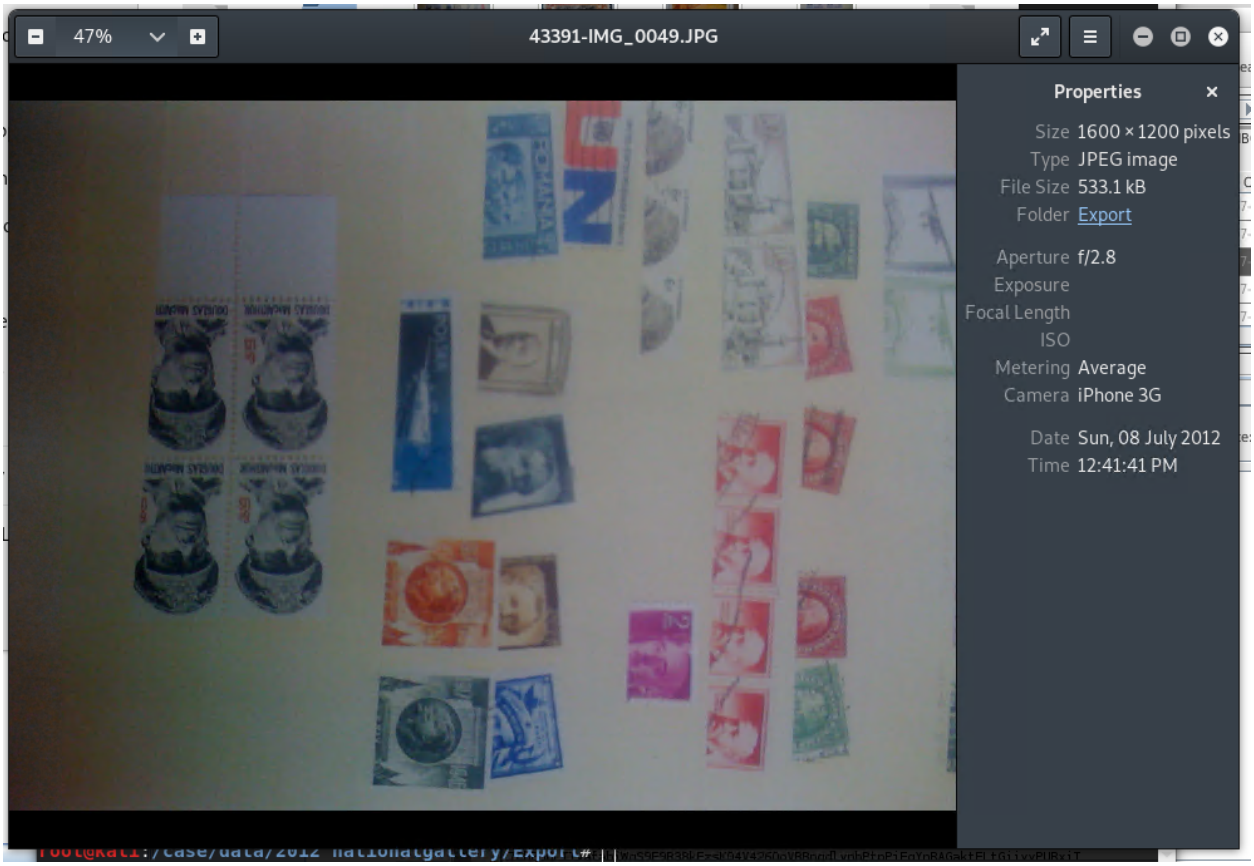
Additional supporting evidence of financial hardship
Terry to Tracy

Artifact 3

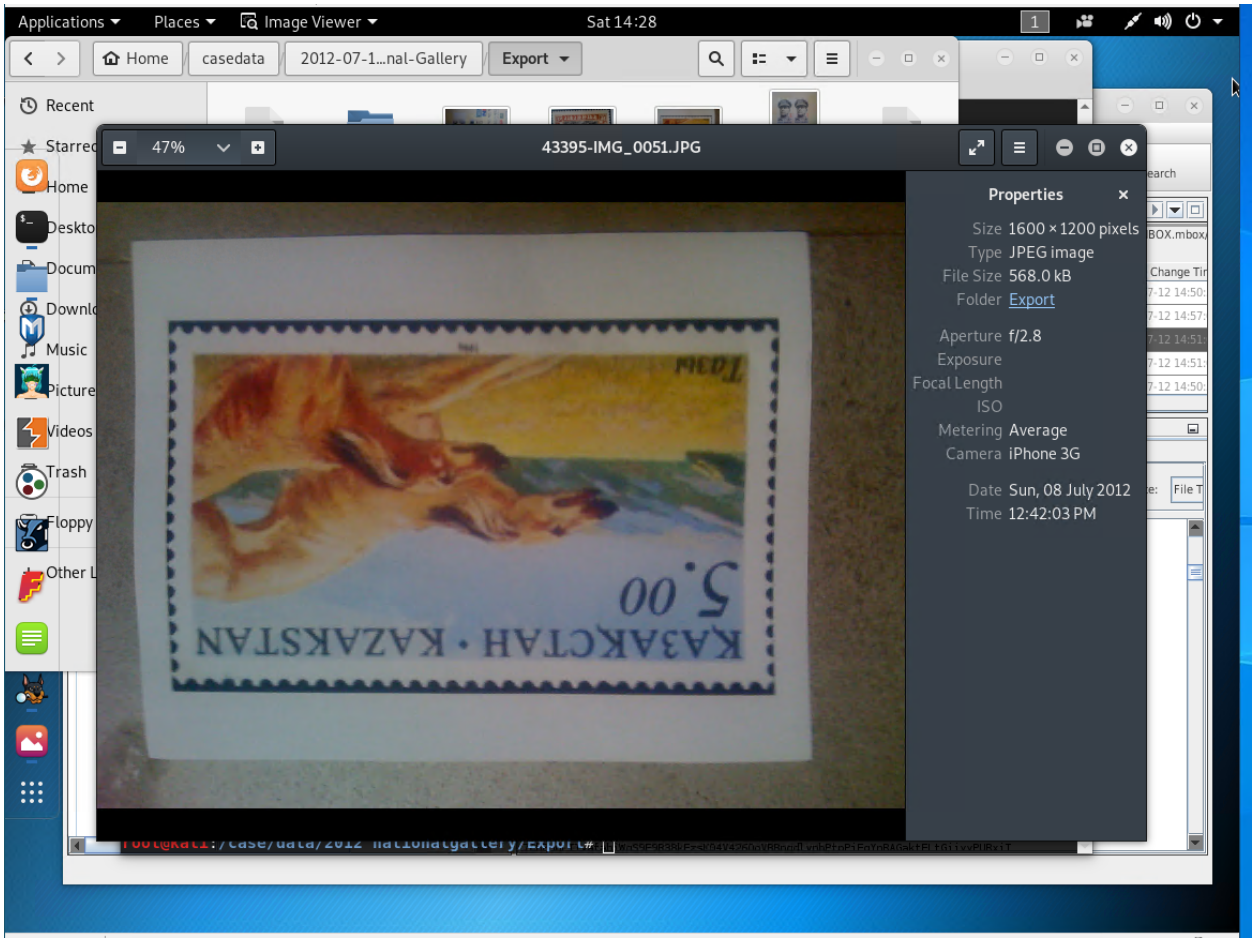


Photos of rare stamps discovered on Tracy's Iphone in: vol5/mobile/MEDIA/DCIM/100/APPLE

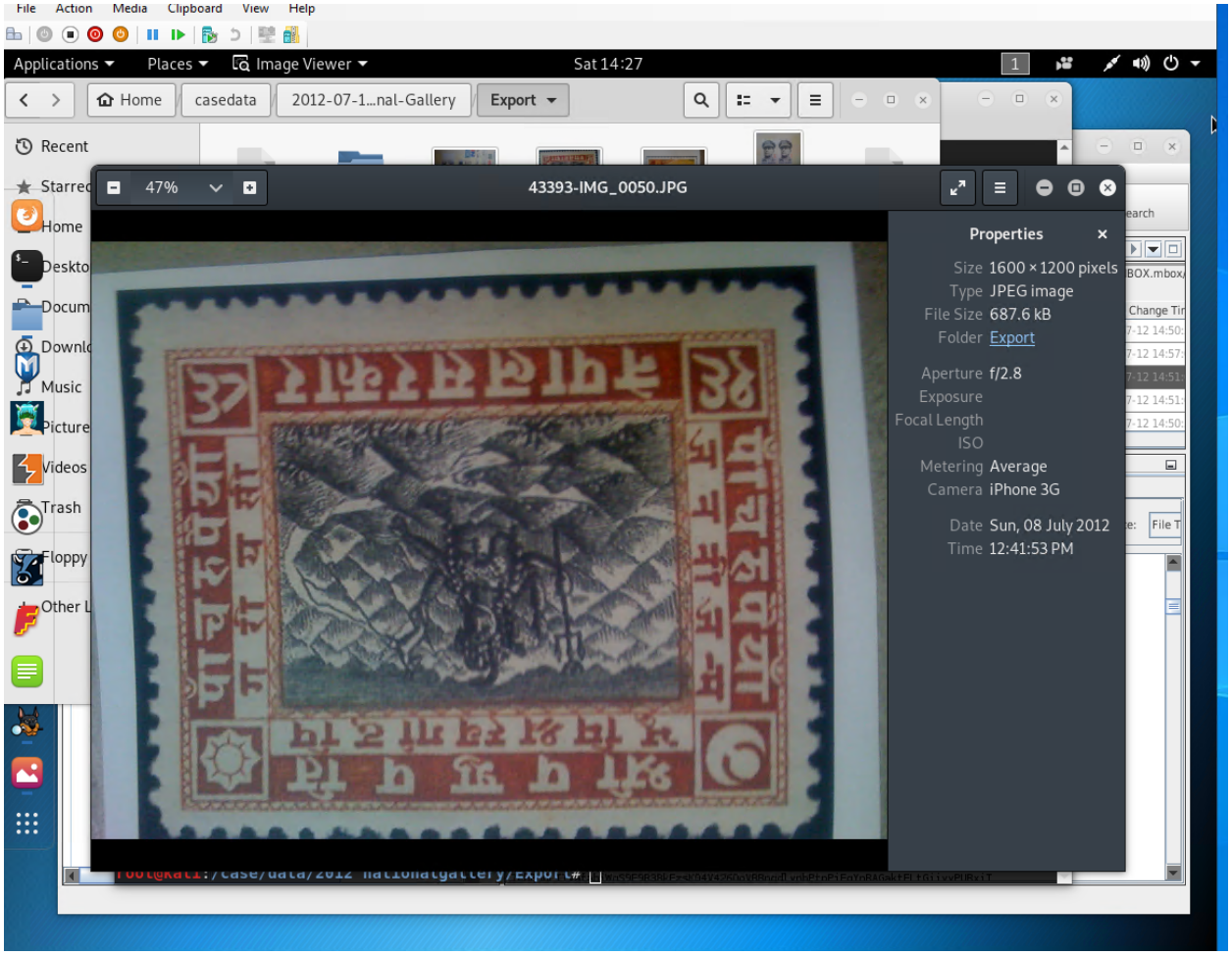
Artifact 4


47%
43391-IMG_0049.JPG
Properties
Size 1600 × 1200 pixels
Type JPEG image
File Size 533.1 kB
Folder Export
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 12:41:41 PM

Artifact 5


Applications
Places
Image Viewer
Sat 14:28
Home
casedata
2012-07-1...nal-Gallery
Export
Recent
Home
Music
Trash
47%
43395-IMG_0051.JPG
Properties
Size 1600 × 1200 pixels
Type JPEG image
File Size 568.0 kB
Folder Export
Aperture f/2.8
Exposure
Focal Length
ISO
Metering Average
Camera iPhone 3G
Date Sun, 08 July 2012
Time 12:42:03 PM
5.00
ҚАЗАҚСТАН · KAZAKSTAN

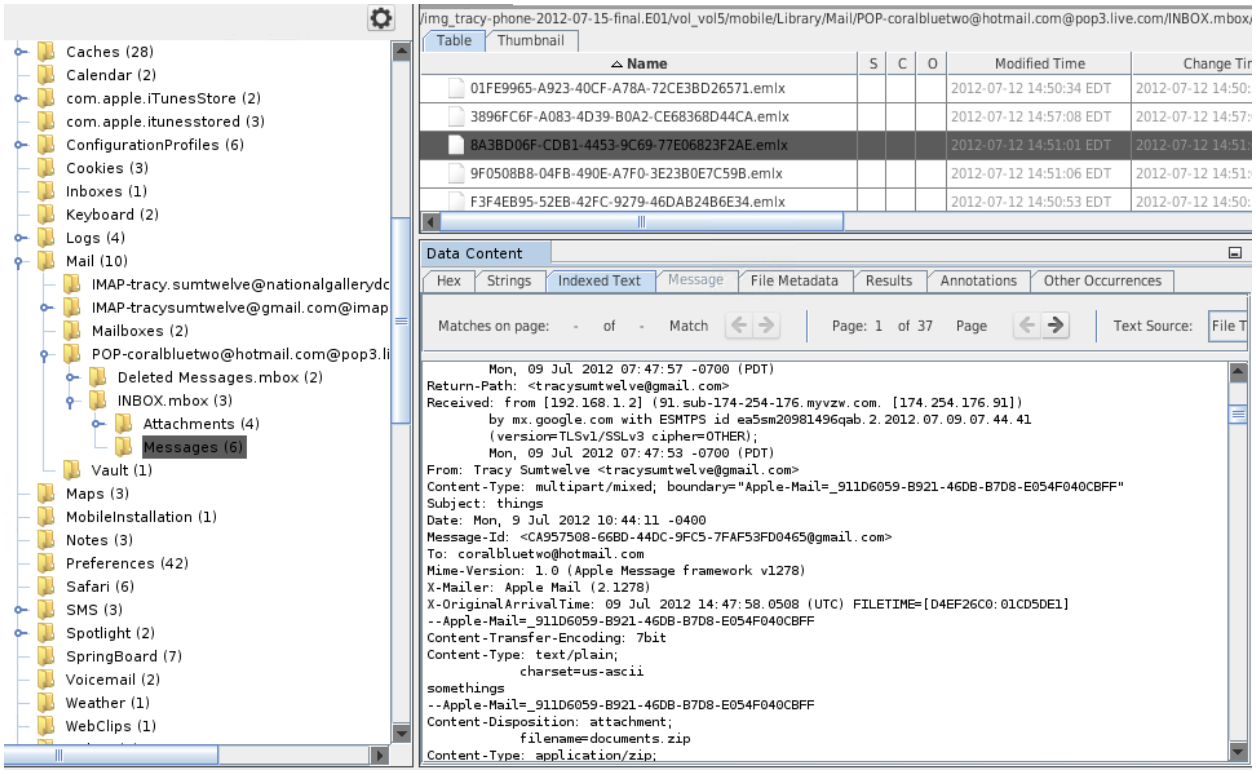
Artifact 6

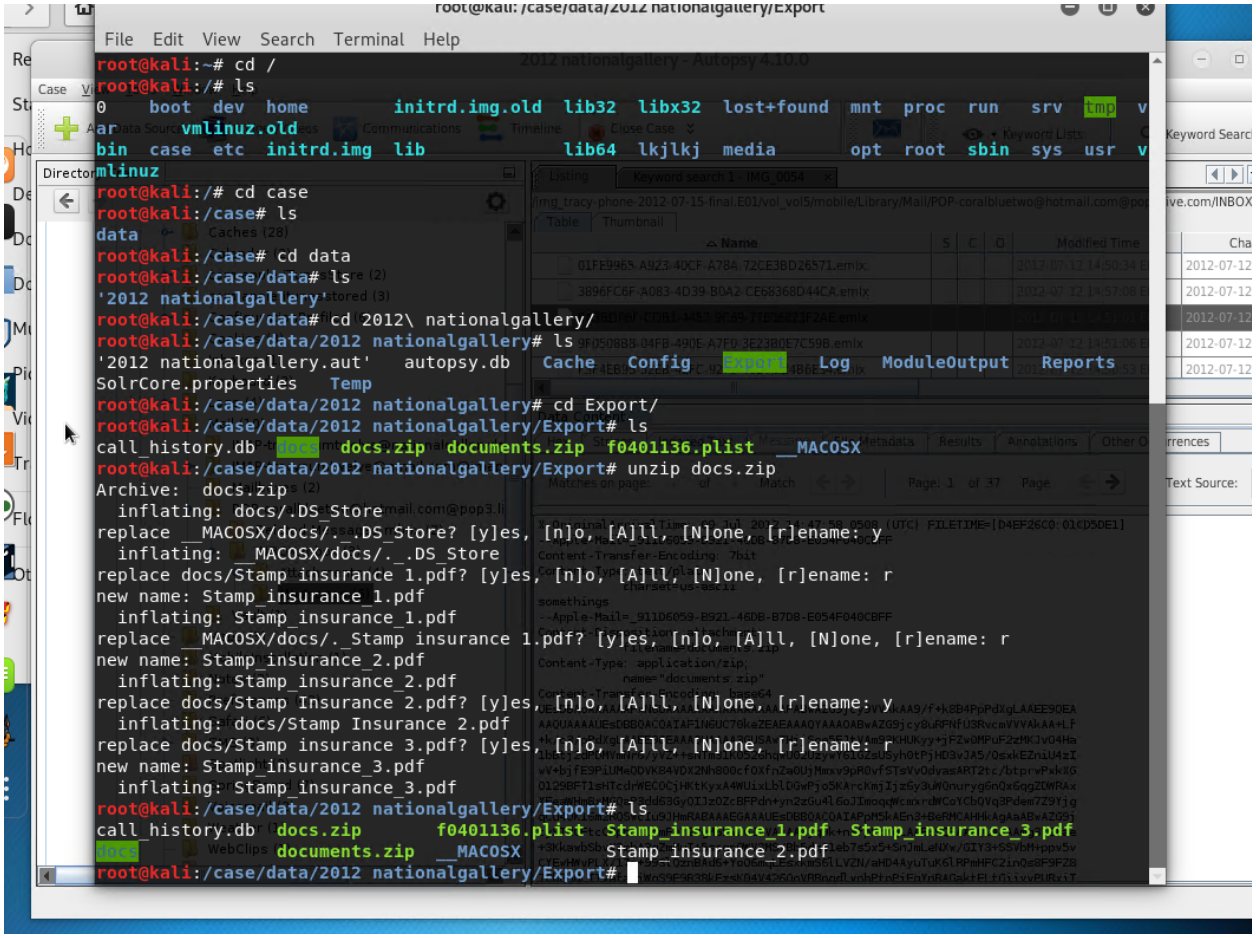


Evidence of Insurance policies found encrypted and zipped on Tracy's iphone located in:
/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/8ABD06FCDB1-4453-9C69-77E06823F2AE.emix

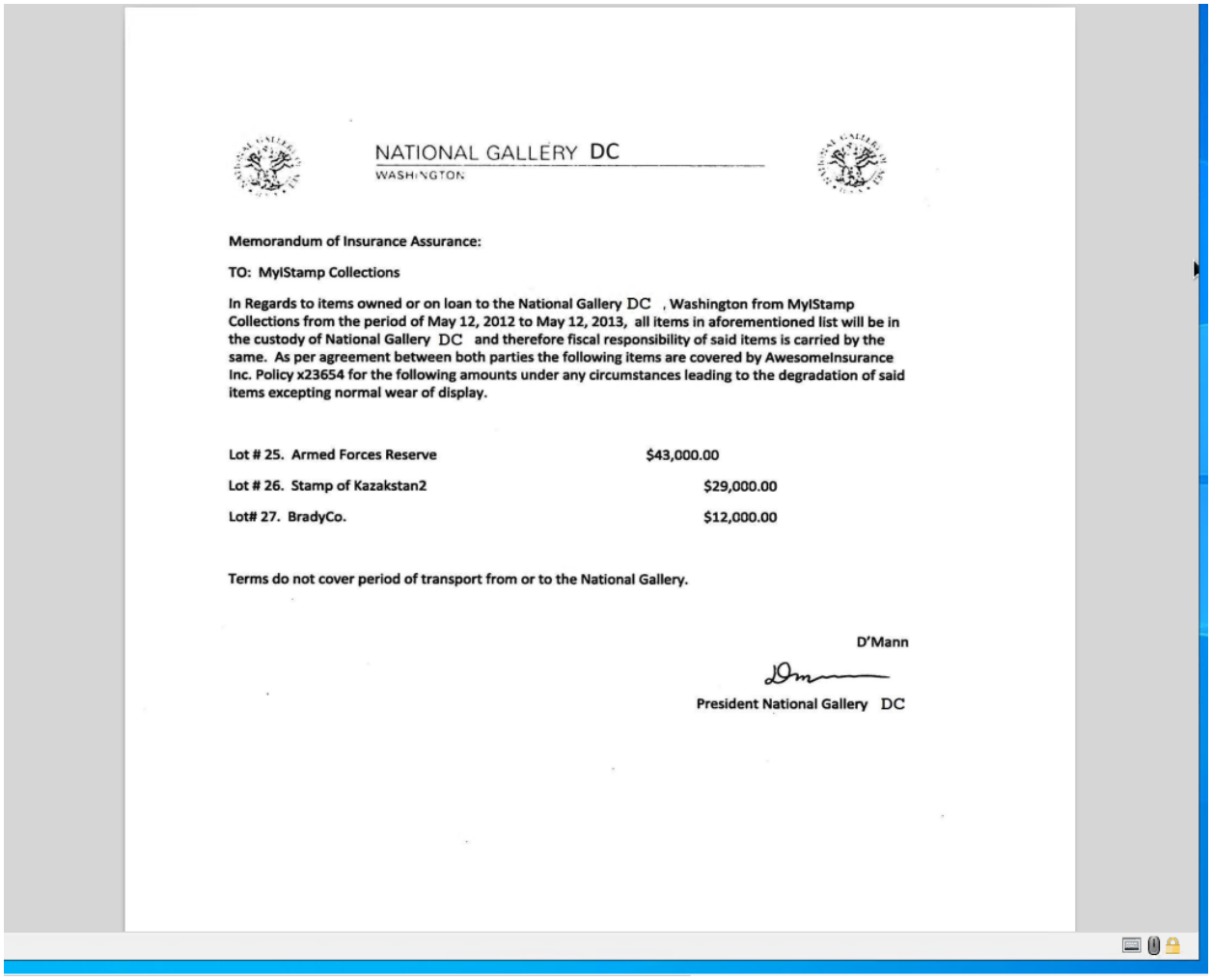
(These files were first unzipped and then discovered to be protected using a storage encryption tool known as ".DS/Store". In order to view them in their original format, a pdf viewer was installed to Kali Linux and the files were given admin privileges {chmod -R 777} and then renamed to prevent the .DS/Store from performing its function properly. This would typically be a breach of the chain of custody since Write privileges were used to rename the files, but it serves to illustrate the technical level of the accused and her accomplices.)

Artifact 7


Caches (28)
Calendar (2)
com.apple.iTunesStore (2)
com.apple.itunesstored (3)
ConfigurationProfiles (6)
Cookies (3)
Inboxes (1)
Keyboard (2)
Logs (4)
Mail (10)
IMAP-tracy.sumtwelve@nationalgallerydc
IMAP-tracysumtwelve@gmail.com@imap
Mailboxes (2)
POP-coralbluetwo@hotmail.com@pop3.li
Deleted Messages.mbox (2)
INBOX.mbox (3)
Attachments (4)
Messages (6)
Vault (1)
Maps (3)
MobileInstallation (1)
Notes (3)
Preferences (42)
Safari (6)
SMS (3)
Spotlight (2)
SpringBoard (7)
Voicemail (2)
Weather (1)
WebClips (1)
/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/
Table
Thumbnail
Name
S
C
O
Modified Time
Change Tir
01FE9965-A923-40CF-A78A-72CE3BD26571.emlx
2012-07-12 14:50:34 EDT
3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
2012-07-12 14:57:08 EDT
8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
2012-07-12 14:51:01 EDT
9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
2012-07-12 14:51:06 EDT
F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
2012-07-12 14:50:53 EDT
Data Content
Hex
Strings
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Matches on page: - of - Match
Page: 1 of 37 Page
Text Source:
Mon, 09 Jul 2012 07:47:57 -0700 (PDT)
Return-Path: <tracysumtwelve@gmail.com>
Received: from [192.168.1.2] (91.sub-174-254-176.myvzw.com. [174.254.176.91])
by mx.google.com with ESMTPS id ea5sm20981496qab.2.2012.07.09.07.44.41
(version=TLSv1/SSLv3 cipher=OTHER);
Mon, 09 Jul 2012 07:47:53 -0700 (PDT)
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]
--Apple-Mail=_911D6059-B921-46DB-B7D8-E054F040CBFF
Content-Transfer-Encoding: 7bit
Content-Type: text/plain;
charset=us-ascii
somethings
--Apple-Mail=_911D6059-B921-46DB-B7D8-E054F040CBFF
Content-Disposition: attachment;
filename=documents.zip
Content-Type: application/zip;


root@kali: /case/data/2012 nationalgallery/Export
File Edit View Search Terminal Help
root@kali:~# cd /
root@kali:/# ls
0 boot dev home initrd.img.old lib32 libx32 lost+found mnt proc run srv tmp v
ar vmlinuz.old
bin case etc initrd.img lib lib64 lkjlkj media opt root sbin sys usr v
mlinuz
root@kali:/# cd case
root@kali:/case# ls
data
root@kali:/case# cd data
root@kali:/case/data# ls
'2012 nationalgallery'
root@kali:/case/data# cd 2012\ nationalgallery/
root@kali:/case/data/2012 nationalgallery# ls
'2012 nationalgallery.aut' autopsy.db Cache Config Export Log ModuleOutput Reports
SolrCore.properties Temp
root@kali:/case/data/2012 nationalgallery# cd Export/
root@kali:/case/data/2012 nationalgallery/Export# ls
call_history.db docs docs.zip documents.zip f0401136.plist __MACOSX
root@kali:/case/data/2012 nationalgallery/Export# unzip docs.zip
Archive: docs.zip
inflating: docs/.DS_Store
replace __MACOSX/docs/._.DS_Store? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: __MACOSX/docs/._.DS_Store
replace docs/Stamp insurance 1.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: Stamp_insurance_1.pdf
inflating: Stamp_insurance_1.pdf
replace __MACOSX/docs/._Stamp insurance 1.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: Stamp_insurance_2.pdf
inflating: Stamp_insurance_2.pdf
replace docs/Stamp Insurance 2.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: docs/Stamp Insurance 2.pdf
replace docs/Stamp insurance 3.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: Stamp_insurance_3.pdf
inflating: Stamp_insurance_3.pdf
root@kali:/case/data/2012 nationalgallery/Export# ls
call_history.db docs.zip f0401136.plist Stamp_insurance_1.pdf Stamp_insurance_3.pdf
docs documents.zip __MACOSX Stamp_insurance_2.pdf
root@kali:/case/data/2012 nationalgallery/Export#

Artifact 8



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.

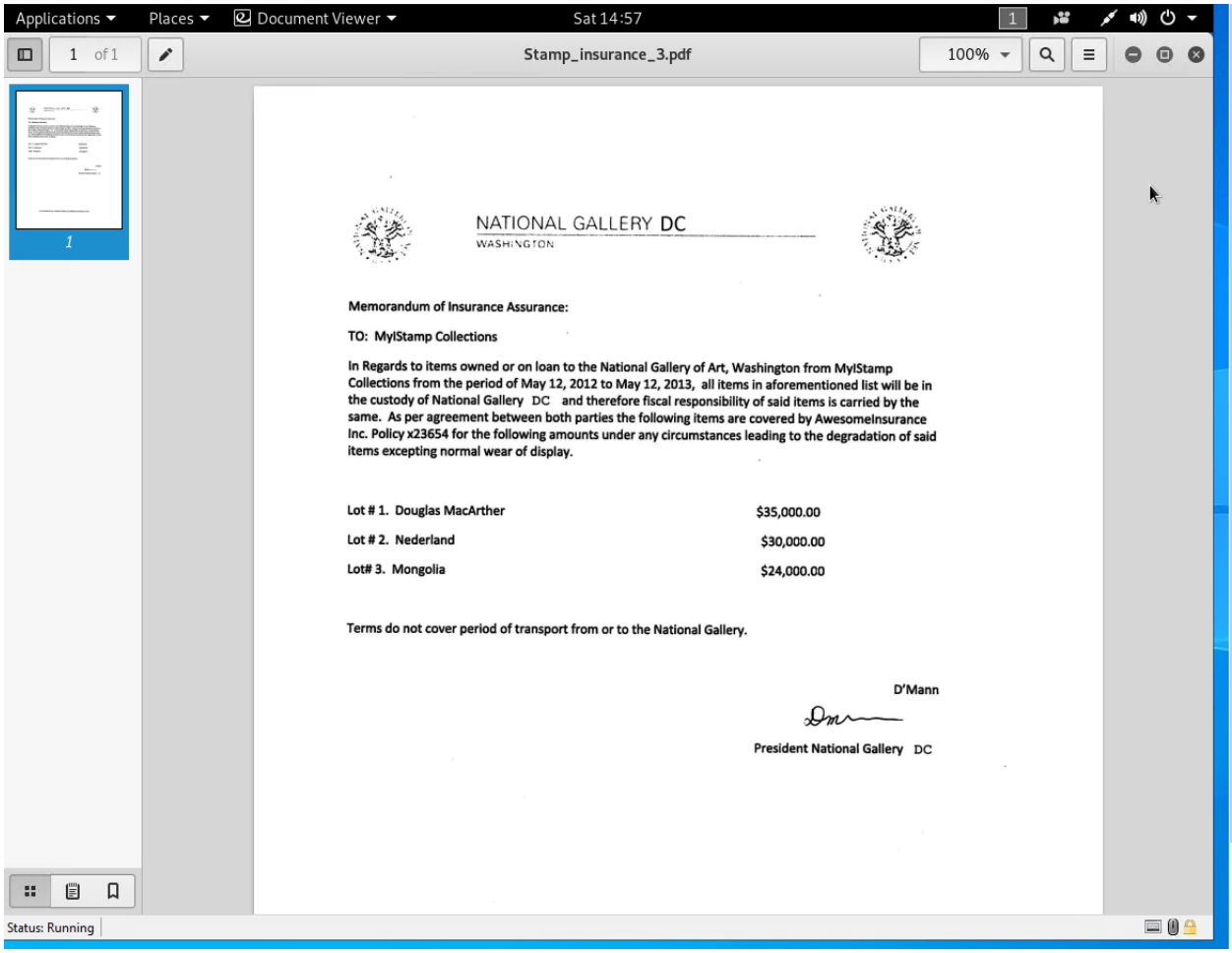
Lot # 25. Armed Forces Reserve	**$43,000.00**
Lot # 26. Stamp of Kazakstan2	**$29,000.00**
Lot# 27. BradyCo.	**$12,000.00**

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

D'Mann

President National Gallery DC

Artifact 9



Email Evidence was discovered within Tracy's iphone found at: /img_tracy-phone2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/Pop-coralbluetwo@hotmail.com@POP3live.com/INBOX.mbox/Messages/9f0508B8-04FBA7f0-3E23B0E7C59B.emix

Artifact 10

----------Forwarded message----------
Date: Fri, 6 Jul 2012 11:49:31 -0400
Subject: can't pass up
From: patsumtwelve@gmail.com

To: throne1966@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 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$ were dealing drugs and shooting dope in your veins every night, i feel he wouldn=92t be too happy. It=92s 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=92t 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

Artifact 11

---------- 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

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:

see attachment

--f46d0447963147823804c47b5550--
--f46d0447963147823c04c47b5552
Content-Type: text/plain; name="needs.txt"
Content-Disposition: attachment; filename="needs.txt"
Content-Transfer-Encoding: base64

X-Attachment-Id: 7e61cc54d96709df_0.1

--f46d0447963147823c04c47b5552
Content-Type: text/plain; name="needs.txt"
Content-Disposition: attachment; filename="needs.txt"
Content-Transfer-Encoding: base64
X-Attachment-Id: 7e61cc54d96709df_0.1

Received: from mail-ob0-f180.google.com ([209.85.214.180]) by
SNT0-MC2-F42.Snt0.hotmail.com with Microsoft SMTPSVC$
Tue, 10 Jul 2012 08:24:58 -0700
Received: by mail-ob0-f180.google.com with SMTP id uo19so132030obb.39
for <coralbluetwo@hotmail.com>; Tue, 10 Jul 2012 08:24:57 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:in-reply-to:references:date:message-id:subject:from:to
:content-type;
bh=C8wvCjoN9j+sLMzAIUkU+NUhCg/PfAOdPXdVBbCfMkc=;
b=UGeN6YehB4DWQc+bQ0o9RbTs/KPJ1I2aXdEtQI3omEDmyUOTspvADU+oprioF1nTtr
3DRZv3tY1iH9ZUEtrJkwJi1qsxO3WRE4STqdSHgRCgdErKnhOjac/H+GNKCffJfSpEqp
hxrX4n9fjMKQ56bJc0nskDYhnN6UwjGkqt6bOzTjWMV1VN5yYeJ+cumfQB1xixYnDX03
gj0GPIXxczfLA0PPR9GvUboCNILaUNBKdRt0IQflokLHaKSng42raMHeeRhW1DRLutKM
K7wjGIiqIHXObJg/CWMf8Gi2hadosCzaFXdYgLL60hQbdwTUzOom3nKZaHtfRN9NahX2
84Pw==
MIME-Version: 1.0
Received: by 10.182.53.103 with SMTP id a7mr40952369obp.3.1341933897613; Tue,
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.com>
<SNT134-W47FD1A09240D1D11C969CFCDD20@phx.gbl>

Attached file "needs.txt" was downloaded and contains the following message

Artifact 12

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)

Artifact 13

Date: Tue, 10 Jul 2012 11:24:57 -0400
Message-ID:
<CAA0mepmJ5+K6puFdL7GYC75pFyJ5HWDtJ3ANRW3d2dWP4Lo3dA@mail.gmail.com>
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=[2A69E350:01CD5EB0]

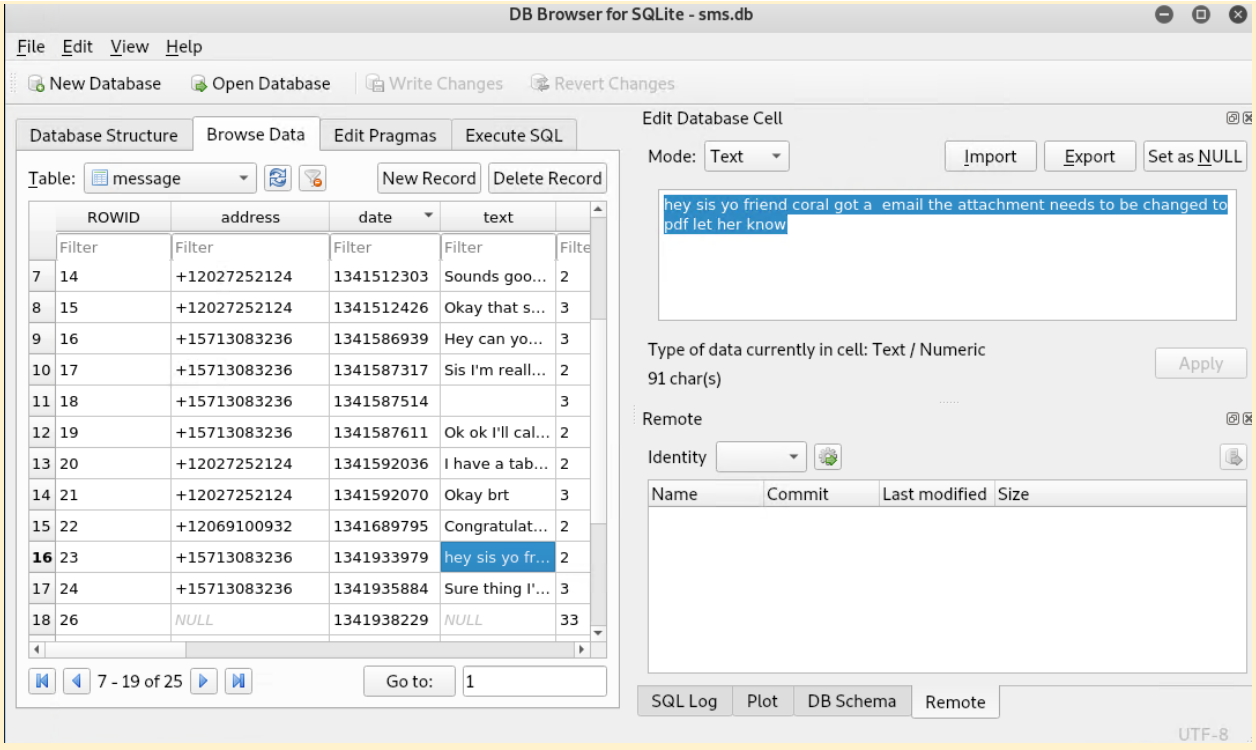
--f46d0447963147823c04c47b5552
Content-Type: multipart/alternative; boundary=f46d0447963147823804c47b5550

--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

Pat to Tracy:
An SMS reference to the email attachment (needs.txt) and for “Coral” (an alias for Tracy) to convert the file to PDF her response comes back 5 seconds later stating “sure thing, ill get on it”

Artifact 14

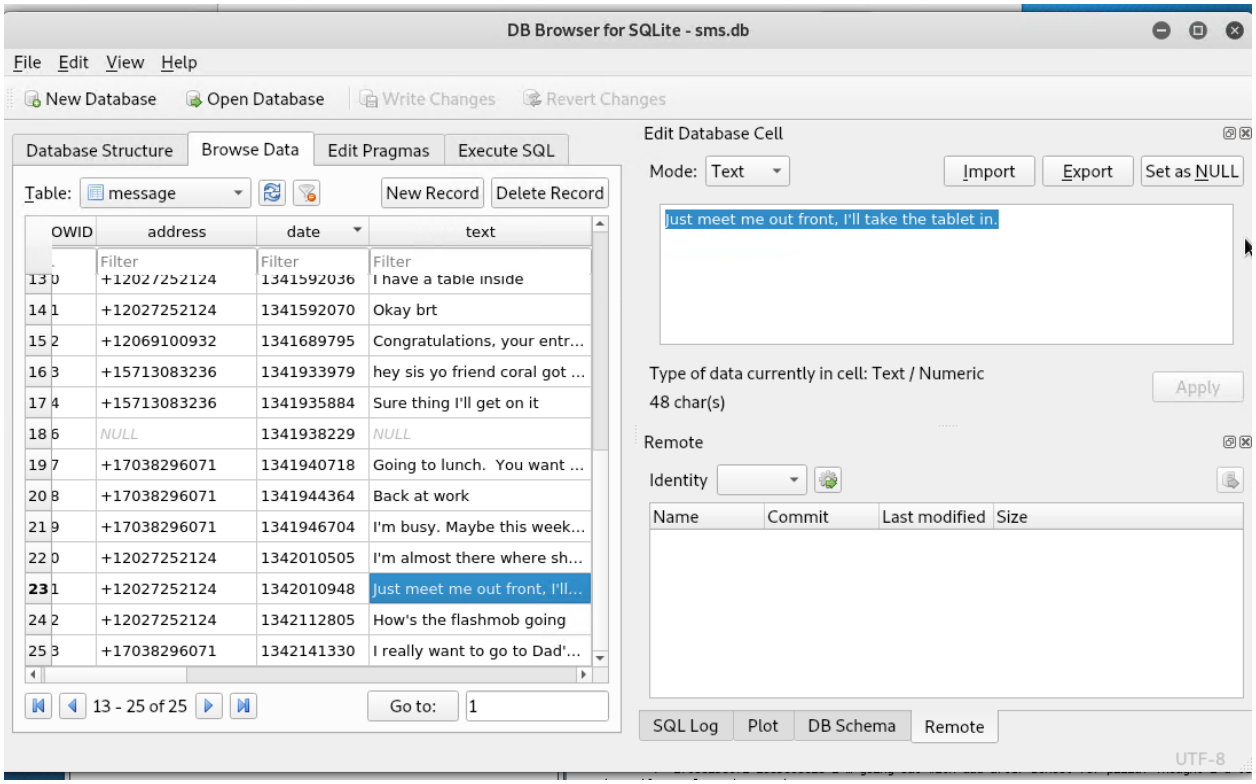


Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

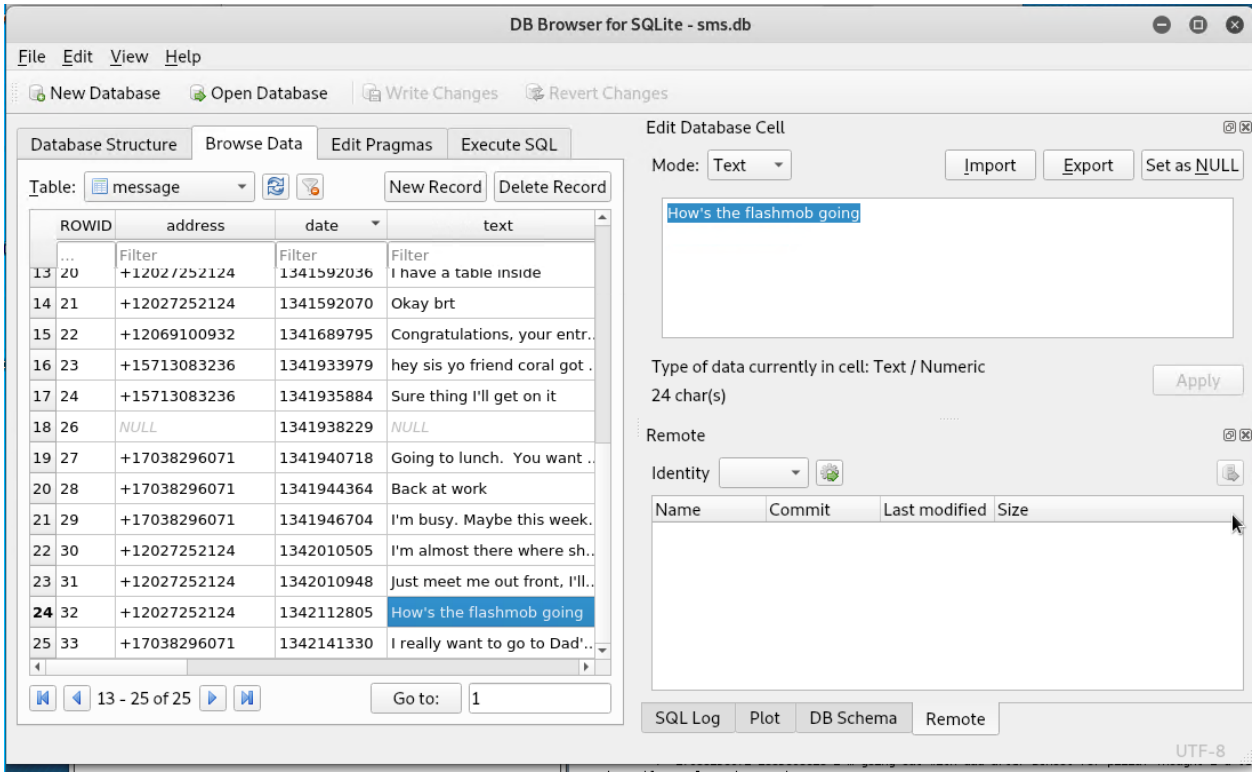
Below is an SMS message from Tracy to Carry stating she will meet her out front and smuggle the tablet in.

Artifact 15



This was followed by a message discussing the flashmob 5 seconds later

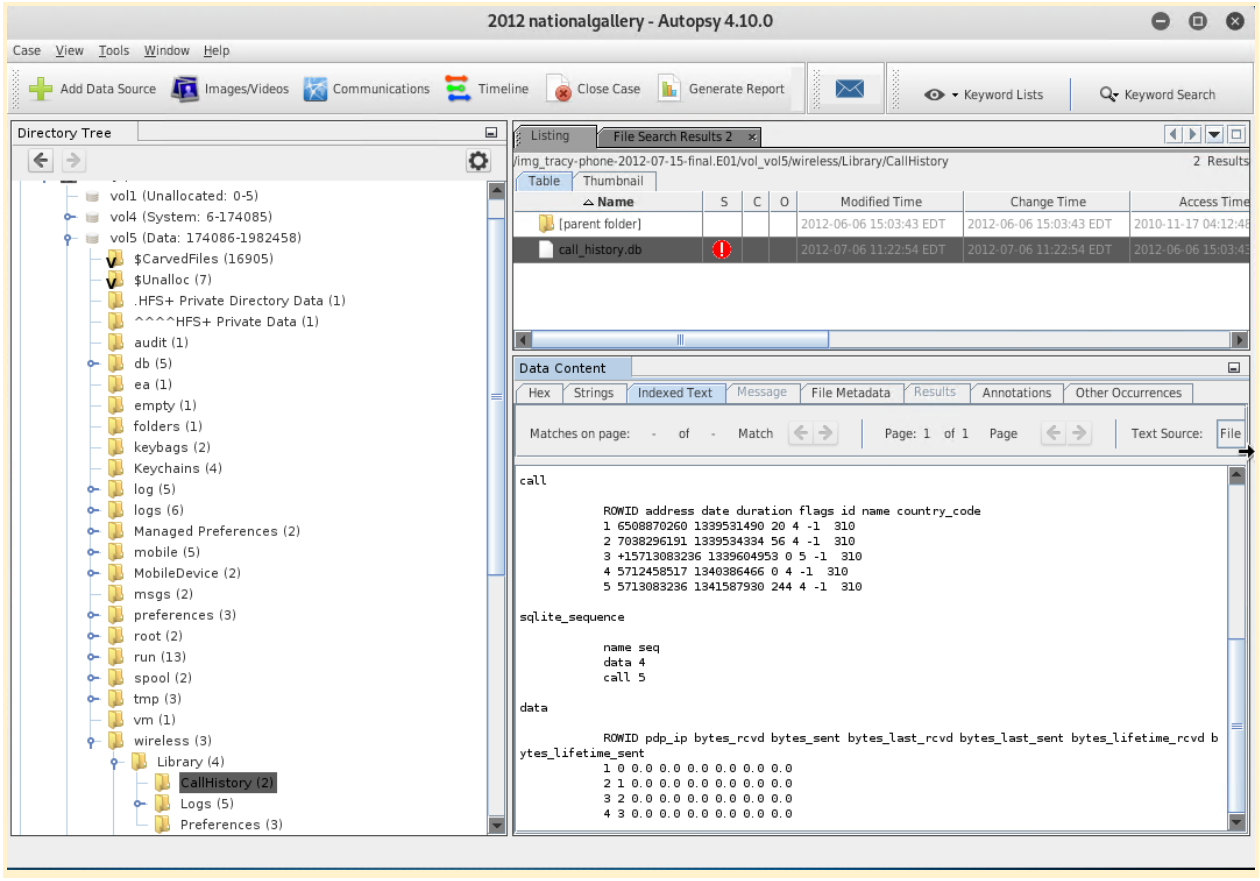
Artifact 16

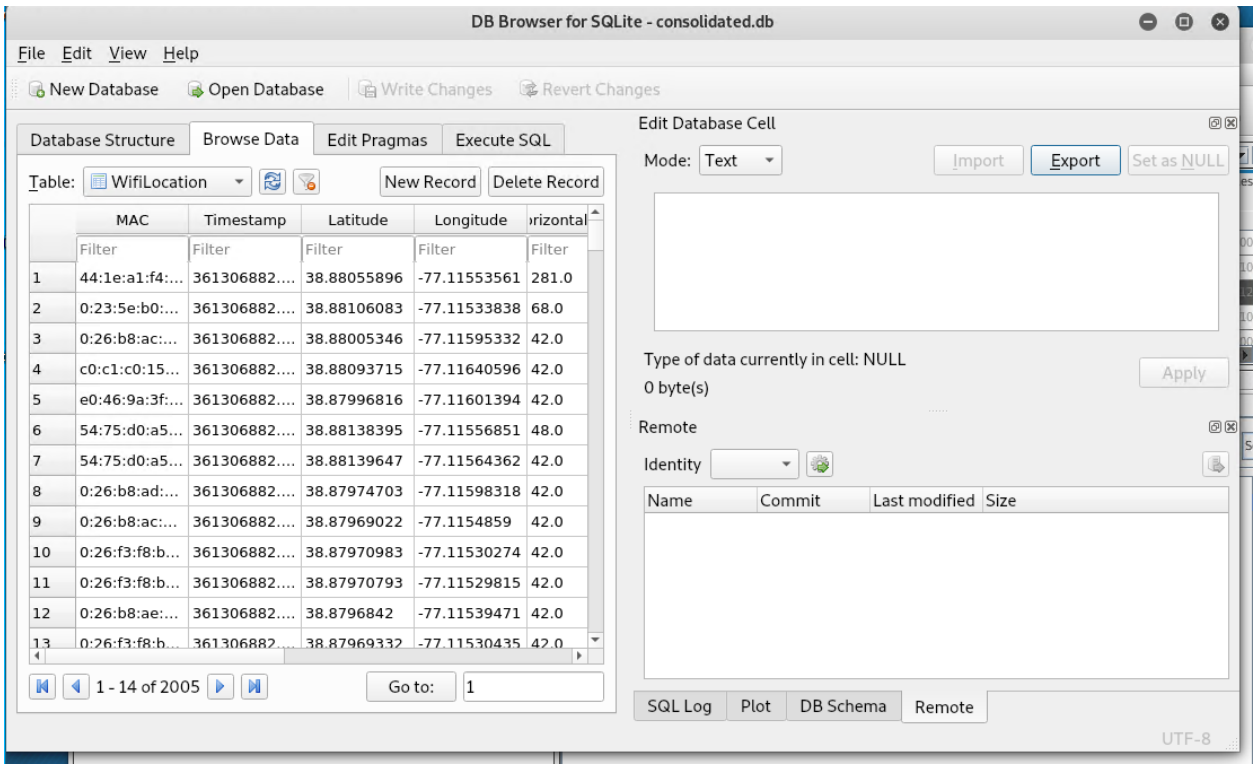


Plot Timeline

Call logs from Tracys iphone

Artifact 17


2012 nationalgallery - 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
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)
Library (4)
CallHistory (2)
Logs (5)
Preferences (3)
Listing
File Search Results 2
/img_tracy-phone-2012-07-15-final.E01/vol_vol5/wireless/Library/CallHistory
2 Results
Table
Thumbnail
Name
S
C
O
Modified Time
Change Time
Access Time
[parent folder]
2012-06-06 15:03:43 EDT
2012-06-06 15:03:43 EDT
2010-11-17 04:12:48
call_history.db
2012-07-06 11:22:54 EDT
2012-07-06 11:22:54 EDT
2012-06-06 15:03:43
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
call
ROWID address date duration flags id name country_code
1 6508870260 1339531490 20 4 -1 310
2 7038296191 1339534334 56 4 -1 310
3 +15713083236 1339604953 0 5 -1 310
4 5712458517 1340386466 0 4 -1 310
5 5713083236 1341587930 244 4 -1 310
sqlite_sequence
name seq
data 4
call 5
data
ROWID pdp_ip bytes_rcvd bytes_sent bytes_last_rcvd bytes_last_sent bytes_lifetime_rcvd b
ytes_lifetime_sent
1 0 0.0 0.0 0.0 0.0 0.0 0.0
2 1 0.0 0.0 0.0 0.0 0.0 0.0
3 2 0.0 0.0 0.0 0.0 0.0 0.0
4 3 0.0 0.0 0.0 0.0 0.0 0.0


DB Browser for SQLite - consolidated.db
File Edit View Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: WifiLocation
New Record
Delete Record
MAC
Timestamp
Latitude
Longitude
Filter
1 44:1e:a1:f4:... 361306882.... 38.88055896 -77.11553561 281.0
2 0:23:5e:b0:... 361306882.... 38.88106083 -77.11533838 68.0
3 0:26:b8:ac:... 361306882.... 38.88005346 -77.11595332 42.0
4 c0:c1:c0:15... 361306882.... 38.88093715 -77.11640596 42.0
5 e0:46:9a:3f:... 361306882.... 38.87996816 -77.11601394 42.0
6 54:75:d0:a5... 361306882.... 38.88138395 -77.11556851 48.0
7 54:75:d0:a5... 361306882.... 38.88139647 -77.11564362 42.0
8 0:26:b8:ad:... 361306882.... 38.87974703 -77.11598318 42.0
9 0:26:b8:ac:... 361306882.... 38.87969022 -77.1154859 42.0
10 0:26:f3:f8:b... 361306882.... 38.87970983 -77.11530274 42.0
11 0:26:f3:f8:b... 361306882.... 38.87970793 -77.11529815 42.0
12 0:26:b8:ae:... 361306882.... 38.8796842 -77.11539471 42.0
1 - 14 of 2005
Go to: 1
Edit Database Cell
Mode: Text
Import
Export
Set as NULL
Type of data currently in cell: NULL
0 byte(s)
Apply
Remote
Identity
Name
Commit
Last modified
Size
SQL Log
Plot
DB Schema
Remote
UTF-8

Conclusion

Evidence found on Tracy's iPhone indicated the following:

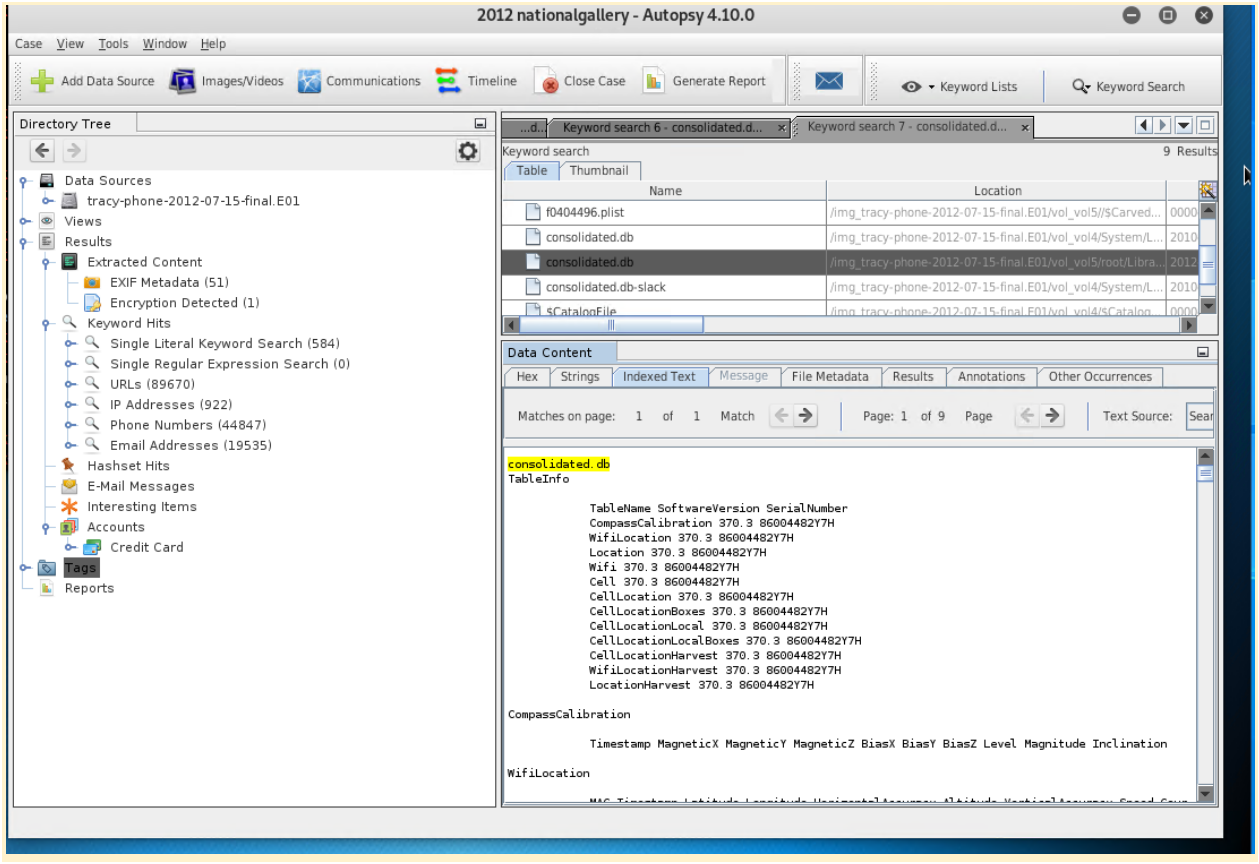
Stamps theft:
Tracy was motivated to earn additional money to help with financial hardships due to her divorce and custody issues with her daughter Terry. Pat presented her with Insurance documents proving the value of the stamps within the National Gallery. Pat also insisted they begin using aliases and alternate means of communicating once he started formulating a plot for a heist of the stamps. Email between these aliases and a man named King revealed a plot to steal the stamps and a list of the materials needed to do so. King is blackmailed with an email threatening to report his other parole violations if he does not cooperate in the theft.
Art defacement:
Tracy has been in contact with Carry who have met and phoned each other. Carry asked Tracy to smuggle in a tablet which Tracy agreed to do by meeting out front of the building. A "flash mob" was arranged by Carry as a form of diversion to offset security.

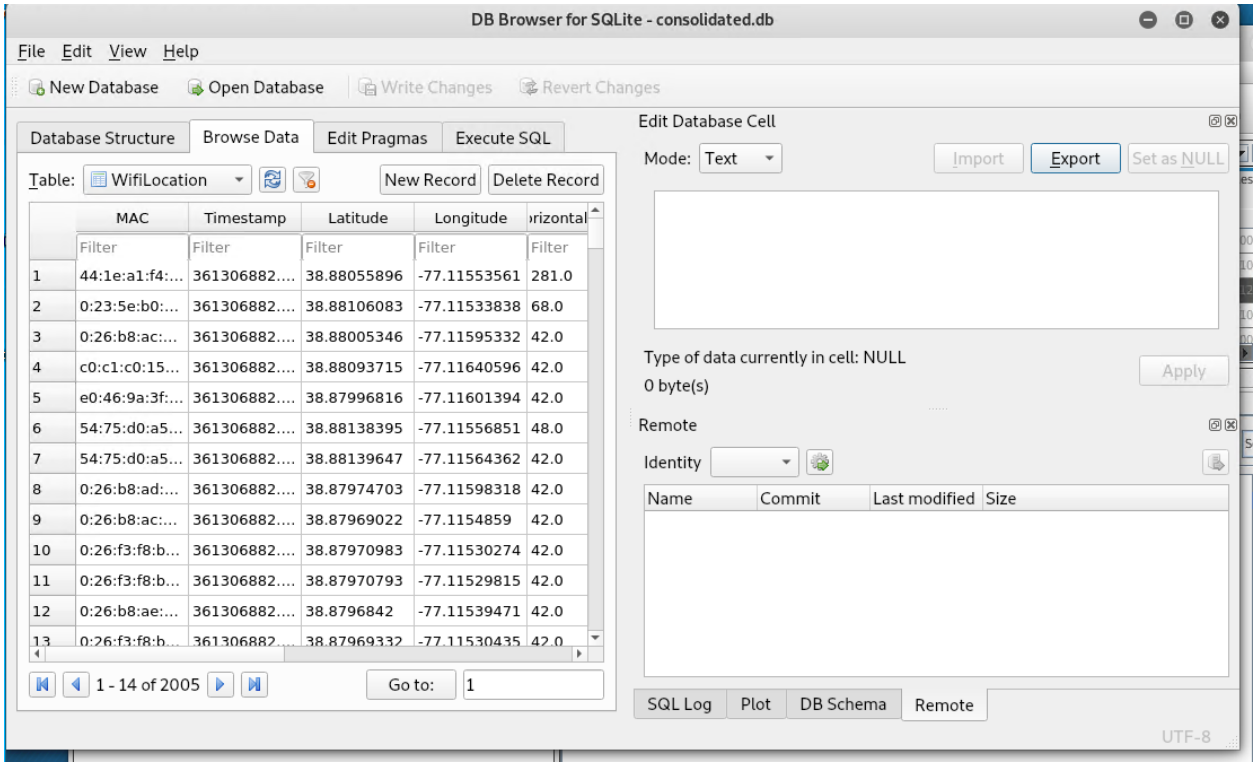
Appendix WiFi and GPS Location Information

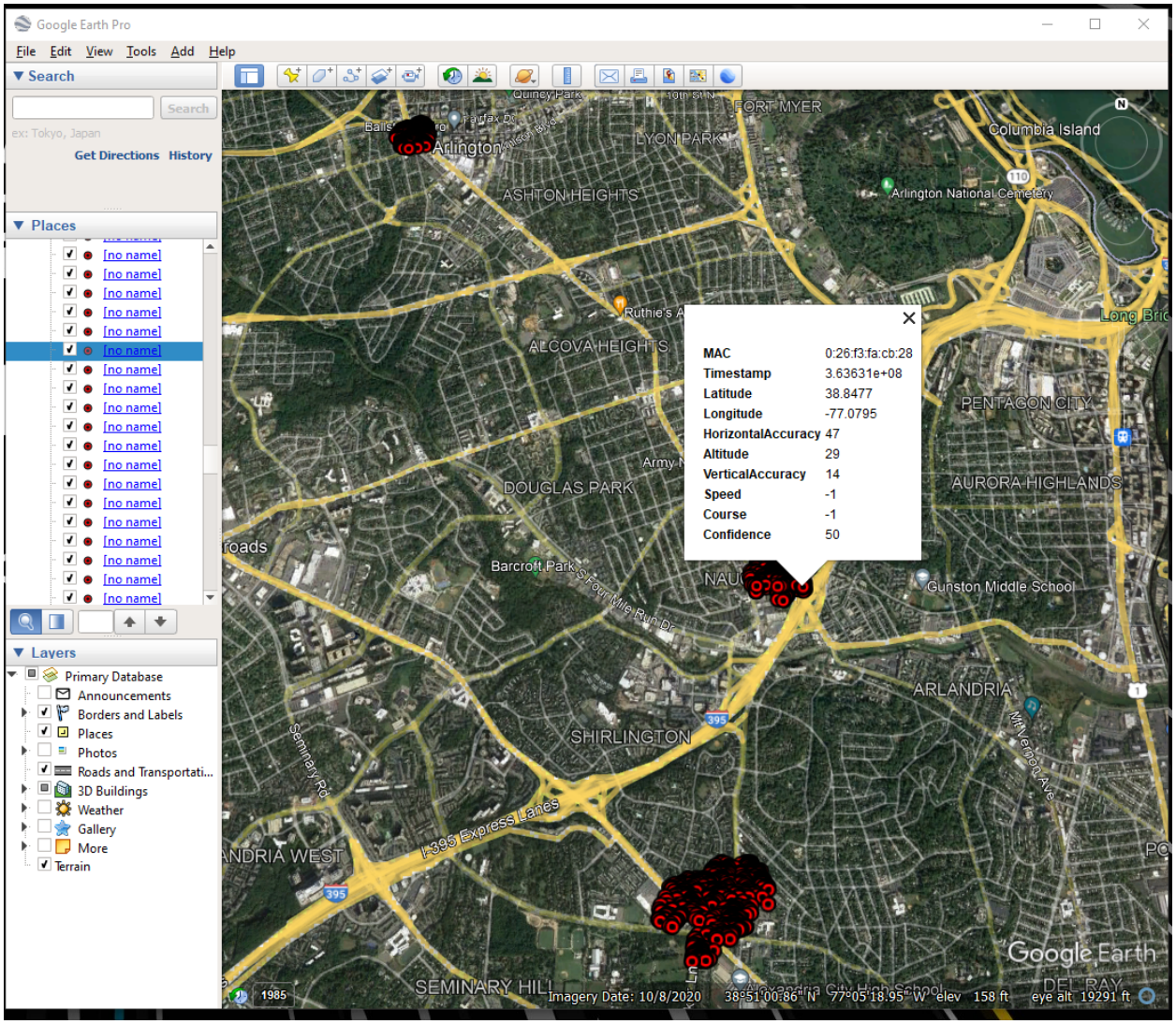
WIFI GPS data from Tracy's iphone

The following information was gathered from Tracy's phone as a file called "consolidated.db". This data was then exported into SQLitebrowser and converted to a csv. file for viewing in Google Earth (pictured below)

Artifact 18


2012 nationalgallery - 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
tracy-phone-2012-07-15-final.E01
Views
Results
Extracted Content
EXIF Metadata (51)
Encryption Detected (1)
Keyword Hits
Single Literal Keyword Search (584)
Single Regular Expression Search (0)
URLs (89670)
IP Addresses (922)
Phone Numbers (44847)
Email Addresses (19535)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Credit Card
Tags
Reports
Keyword search 6 - consolidated.d...
Keyword search 7 - consolidated.d...
Keyword search
9 Results
Table
Thumbnail
Name
Location
f0404496.plist
consolidated.db
consolidated.db
consolidated.db-slack
Data Content
Hex
Strings
Indexed Text
Message
File Metadata
Results
Annotations
Other Occurrences
Matches on page: 1 of 1 Match
Page: 1 of 9 Page
Text Source:
consolidated.db
TableInfo
TableName SoftwareVersion SerialNumber
CompassCalibration 370.3 86004482Y7H
WifiLocation 370.3 86004482Y7H
Location 370.3 86004482Y7H
Wifi 370.3 86004482Y7H
Cell 370.3 86004482Y7H
CellLocation 370.3 86004482Y7H
CellLocationBoxes 370.3 86004482Y7H
CellLocationLocal 370.3 86004482Y7H
CellLocationLocalBoxes 370.3 86004482Y7H
CellLocationHarvest 370.3 86004482Y7H
WifiLocationHarvest 370.3 86004482Y7H
LocationHarvest 370.3 86004482Y7H
CompassCalibration
Timestamp MagneticX MagneticY MagneticZ BiasX BiasY BiasZ Level Magnitude Inclination
WifiLocation


DB Browser for SQLite - consolidated.db
File Edit View Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: WifiLocation
New Record
Delete Record
MAC
Timestamp
Latitude
Longitude
Filter
1 44:1e:a1:f4:... 361306882.... 38.88055896 -77.11553561 281.0
2 0:23:5e:b0:... 361306882.... 38.88106083 -77.11533838 68.0
3 0:26:b8:ac:... 361306882.... 38.88005346 -77.11595332 42.0
4 c0:c1:c0:15... 361306882.... 38.88093715 -77.11640596 42.0
5 e0:46:9a:3f:... 361306882.... 38.87996816 -77.11601394 42.0
6 54:75:d0:a5... 361306882.... 38.88138395 -77.11556851 48.0
7 54:75:d0:a5... 361306882.... 38.88139647 -77.11564362 42.0
8 0:26:b8:ad:... 361306882.... 38.87974703 -77.11598318 42.0
9 0:26:b8:ac:... 361306882.... 38.87969022 -77.1154859 42.0
10 0:26:f3:f8:b... 361306882.... 38.87970983 -77.11530274 42.0
11 0:26:f3:f8:b... 361306882.... 38.87970793 -77.11529815 42.0
12 0:26:b8:ae:... 361306882.... 38.8796842 -77.11539471 42.0
13 0:26:f3:f8:b... 361306882.... 38.87969332 -77.11530435 42.0
1 - 14 of 2005
Go to: 1
Edit Database Cell
Mode: Text
Import
Export
Set as NULL
Type of data currently in cell: NULL
0 byte(s)
Apply
Remote
Identity
Name
Commit
Last modified
Size
SQL Log
Plot
DB Schema
Remote
UTF-8



In order to correlate GPS coordinates to individual communications found on Tracys phone, the timestamp number could be looked up to match with each SMS message or email or phone call. This match up will provide an estimated location of the phone at the given time.